الإرهاب في العصر الرقمي (الإرهاب الإلكتروني): صوره، مخاطره، آليات مواجهته

أ.د/ جمال علي الدهشان

http://dx.doi.org/10.29009/ijres.1.3.3

الإرهاب في العصر الرقمي (الإرهاب الإلكتروني): صوره، مخاطره، إليات مواجهته

أ. د/ جمال علي الدهشان

أستاذ أصول التربية، وعميد كلية جامعة المنوفية، مصر. g_eldahshan@yahoo.com

قدمت للنشر في ١ / ٥ / ٢٠١٨م قبلت في ٢٠/ ٥ / ٢٠١٨م

الملخص: تهدف الورقة الحالية إلى دراسة ظاهرة الإرهاب الذي يستخدم الوسائل الإلكترونية والرقمية، وأصبح يسمي الإرهاب الرقمي، أو الإرهاب الإلكتروني، بما يؤدي إلى توعية المجتمع عن هذه الظاهرة من كافة جوانبها، وصورها ومخاطرها وأساليب مواجهتها، وتتناول الورقة الحالية النقاط التالية: (المقصود بالإرهاب الإلكتروني وخصائصه وأسبابه، صور الإرهاب الإلكتروني ومخاطره، وإليات وخطط مواجهة الإرهاب الإلكتروني).

الكلمات الدلالية: الإرهاب، العصر الرقمي، الإرهاب الإلكتروني.

http://dx.doi.org/10.29009/ijres.1.3.3

Terrorism in the Digital Era (Cyber Terrorism): Types، Risks & Mechanisms of Encountering

El-Dahshan، Gamal Ali

Professor of "Foundation of Education", and Dean, College of Education, Menoufia University, Egypt. g_eldahshan@yahoo.com

Received 1 May 2018 Accepted 20 May 2018

Abstract: The present paper aims to study the phenomenon of terrorism, which uses electronic and digital means, that called digital terrorism, or Cyber terrorism, which leads to raising the awareness of society about this phenomenon in all its aspects, forms, dangers and methods of confronting them. The present paper deals with the following points: Electronic properties and its dangers, mechanisms and plans to confront electronic terrorism).

Keywords: Terrorism، Digital Era، Cyber Terrorism.

http://dx.doi.org/10.29009/ijres.1.3.3

مقدمة

تعاني المجتمعات المعاصرة من ظاهرة خطيرة تتمثل في ظهور مجموعة من الأفعال الإجرامية الموجهة ضد الدول والافراد، والتي يكون هدفها أو من شأنها إثارة الفزع أو الرعب لدي شخصيات معينة أو جماعات من الناس أو لدي العامة، وترويعهم بإيذائهم أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر أو إلحاق الضرر بالبيئة أو بأحد المرافق أو الأملاك العامة أو الخاصة، أو احتلالها والاستيلاء عليها، أو تعريض الموارد الوطنية للخطر بغير حق، وبشتي صنوف العدوان وصور الإفساد في الأرض، تلك الظاهرة التي يطلق عليها الإرهاب.

واذا كانت تلك الظاهرة قد اتخذت صورة واشكال متعددة، وارتبطت تلك الاشكال بظروف كل عصر وتحدياته، فأنه في ظل ما يشهده العالم اليوم من تطوراً هائلا في تكنولوجيا الاتصالات والمعلومات؛ حتي أصبح يطلق علي هذا العصر- عصر الثورة المعلوماتية – والتي شملت معظم جوانب الحياة، وكانت أشبه ما تكون بالثورة في حياة البشرية وأسلوب حياتهم، فهي ثورة ولكنها من نوع جديد، ثورة تعتمد علي تكنولوجيا الحواسب والاجهزة المحمولة وشبكات المعلومات والانترنت، تلك الثورة لم يتم استخدامها والاستفادة من إيجابياتها، ولكن في المقابل وللأسف تم استخدامها من قبل البعض بشكل سلبي يضر بالبشرية بأكملها.

ففي ظل تلك الثورة وذلك الاستخدام السلبي لها ظهرت صورة واشكال جديدة لتلك الظاهرة اطلق عليها الإرهاب الإلكتروني، الذي ظهر وشاع استخدامه عقب الطفرة الكبيرة التي حققتها تكنولوجيا المعلومات واستخدامات الحواسب الآلية والإنترنت تحديداً في إدارة معظم الأنشطة الحياتية. وهو الأمر الذي دعا ٣٠ دولة إلى التوقيع على "الاتفاقية الدولية الأولي لمكافحة الإجرام عبر الإنترنت"، في بودابست، عام ٢٠٠١، والذي يعد وبحق من أخطر أنواع الجرائم التي ترتكب عبر شبكة الإنترنت ويتضح هذا جليا من خلال النظر إلى فداحة الخسائر التي يمكن أن تسببها عملية ناجحة واحدة تندرج تحت مفهومه.

http://dx.doi.org/10.29009/ijres.1.3.3

فالإرهاب الإلكتروني يعتمد على استخدام الإمكانيات العلمية والتقنية، واستغلال وسائل الاتصال والشبكات المعلوماتية، من أجل تخويف وترويع الآخرين، وإلحاق الضرر بهم، أو تهديدهم، مثل ما حصل في العام ٢٠٠٠، حينما أدي انتشار فيروس الحاسوب "I love you" إلى إتلاف معلومات قدرت قيمتها بنحو ١٠ مليارات دولار أمريكي، وفي العام 2003، أشاع فيروس "بلاستر" الدمار في نصف مليون جهاز من أجهزة الحاسوب، وقدّر "مجلس أوروبا في الاتفاقية الدولية لمكافحة الإجرام عبر الإنترنت "كلفة إصلاح الأضرار التي تسببها فيروسات المعلوماتية بنحو ١٢ مليار دولار.

والاخطر ان الإرهاب الإلكتروني لم يقتصر خطره فقط على ممارسة الأعمال التخريبية لشبكات الحاسوب والإنترنت، بل امتد ايضا ليشمل أنشطة أكثر خطورة تمثلت، – وكما يشر أحد الباحثين المتخصصين– في الاستخدام اليومي للإنترنت من قبل المنظمات الإرهابية لتنظيم وتنسيق عملياتهم المتفرقة والمنتشرة حول العالم، حيث اشار احد الخبراء إلى الأمنيين أنه يوجد ٩٠ ألف صفحة باللغة العربية و٤٠ ألفًا أخري بلغات مختلفة تستخدمها داعش على الإنترنت.

كما ان خطورة الوجود الإرهابي النشط على الشبكة العنكبوتية لاتقف عند حد عدد الصفحات والمواقع بل انه اضافة إلى ذلك هو متفرق ومتنوع ومراوغ بصورة كبيرة، فإذا ظهر موقع إرهابي اليوم، فسرعان ما يغير نمطه الإلكتروني، ثم يختفي ليظهر مرة بشكل جديد، وبعنوان إلكتروني جديد بعد فترة قصيرة، والمواقع الإلكترونية لتلك المنظمات لا تخاطب أعوانها وممولها فحسب بل توجه رسالاتها أيضاً للإعلام والجمهور الخاص بالمجتمعات التي تقوم بترويعها وإرهابها، وذلك بهدف شن حملات نفسية ضد الدول المستهدفة، فهي –مثلاً– تعرض أفلاما مرعبة للرهائن والأسري أثناء إعدامهم، في نفس الوقت يدعي الإرهابيون أنهم أصحاب قضايا نبيلة، ويشتكون من سوء المعاملة من قبل الآخرين.

فالإرهاب الإلكتروني نوع جديد من أنواع القوة، حيث لم تعد القوة مقتصرة على القوة الصلبة والتي تتمثل في القوة العسكرية والاقتصادية، والتي تحتكرها الدول بشكل عام، وليس كل الدول

http://dx.doi.org/10.29009/ijres.1.3.3

وإنما الدول الكبرى، كما ان هذا النوع لم يعد يقتصر على الدول فقط، وانما امتد إلى كل من له القدرة على امتلاك المعرفة التكنولوجية والقدرة على استخدامها وتوظيفها لتحقيق أهدافه، سواء أكان دولة أو أفراد أو فاعلين من غير الدول، ومن ثم انتهي عصر احتكار القوة واقتصارها على الجوانب العسكرية والاقتصادية.

وانطلاقا من ان الإرهاب الإلكتروني اصبح من أخطر أنواع الإرهاب في العصر الحاضر، نظرًا لاتساع نطاق استخدام التكنولوجيا الحديثة في العالم، لذا فمن الأهمية بمكان مدارسة أسبابه، وطرق مكافحته، ولذلك فقد عقدت العديد من المؤتمرات والندوات واجريت العديد من الدراسات والبحوث حول تلك الظاهرة، من ابرزها على المستوي العربي، ندوة المركز الدولي للدراسات المُستقبلية والاستراتيجية في ١١ أبريل ٢٠١٢ بعنوان "مستقبل الإرهاب الإلكتروني.. تحديات وأساليب المُواجهة"، الملتقي العلمي الدولي والذي نظمه مركز الملك عبدالله بن عبدالعزيز للدراسات الإسلامية المعاصرة وحوار الحضارات تحت عنوان "الإرهاب الإلكتروني: خطره وطرق مكافحته" وذلك يوم الثلاثاء ٢٥/ ١/ ١٤٣٦هـ الموافق ١٨/ ١١/ ٢٠١٤م، وندوة " الإرهاب الإلكتروني " المخاطر.. والمواجهة الأمنية " والتي نظمتها اكاديمية الشرطة بوزارة الداخلية المصرية في ٢٧ ديسمبر ٢٠١٥، كل ذلك بهدف إبراز مخاطر الإرهاب الإلكتروني ووضع استراتيجية فاعلة للمواجهة الأمنية له، وكذلك مؤتمر ليبيا الدولي لمكافحة الإرهاب الإلكتروني والذي عقد في مدينة بنغازي خلال الفترة من ٩- ١١فبراير ٢٠١٦، ومؤتمر جامعة الامام محمد بن سعود الاسلامية في ١٧ نوفمبر ٢٠١٦ الذي عقد تحت عنوان "الإرهاب الإلكتروني: خططه ووسائل مكافحته"، ومؤتمر "الإرهاب الإلكتروني" والذي عقد في العاصمة اللبنانية بيروت ونظمه معهد التنمية الادارية خلال الفترة من ١٢ – ١٥ فبراير ٢٠١٧، واخيرا المؤتمر الدولي لتجريم الإرهاب الإلكتروني والذي عقد في أبوظبي خلال الفترة من ١٥ – ١٦ مايو ٢٠١٧ بهدف إيجاد أرضية مشتركة، لصياغة منظومة من القوانين الدولية، للتصدي لجذور وامتدادات ظاهرة الإرهاب في الفضاء الرقمي، والذي شارك في فيه على

http://dx.doi.org/10.29009/ijres.1.3.3

مدي يومين، نخبة من أصحاب القرار والخبراء في القانون والجرائم الإلكترونية ومكافحة الإرهاب، من مختلف دول العالم.

كما تعددت الدراسات التي تناولت مفهوم الإرهاب الإلكتروني وتم تناوله من أبعاد متعددة منها على سبيل المثال: دراسات تهتم بالإرهاب الإلكتروني ضمن دراسات الأمن الدولي والتعامل معه باعتباره مشابه للأسلحة النووية مثل دراسة جعجع (٢٠١٦)، وهناك دراسات اخري تركز على الجانب القانوني وعلاقة ذلك بالقانون الدولي وحقوق الانسان اللواتي (٢٠١٧)، ودراسات اهتمت بالإرهاب الإلكتروني كقضية عسكرية مثل دراسة الالفي (٢٠١٤)، ودراسات اخري تنظر للإرهاب الإلكتروني باعتباره شكل من أشكال الحرب الغير تقليدية وهي حروب المعلومات، حروب الشبكات والاتصالات والحروب التكنولوجية مثل دراسة حسنين (٢٠١٠)، اضافة إلى الدراسات التي ركزت على استخدام الجماعات الإرهابية للإرهاب الإلكتروني مثل دراسة عادل صادق (٢٠١٦)، والدراسات التي ركزت على اثر الإرهاب الإلكتروني على تغير القوة في العلاقات الدولية وتأثير الإرهاب الإلكتروني على النظام الدولي والتي منها على سبيل المثال لا الحصر الجخة (٢٠٠٩)، ودراسة نوال قيسي، ودراسة الزنط (٢٠١٠) ودراسة بشير (٢٠١٤)، ودراسة عطية (٢٠١٤)، دراسة نوران شفيق علي (٢٠١٤)، دراسة عبدالعال،(٢٠١٥)، ودراسة جمال نصار (٢٠١٥).

وفي اطار دراسة كيفية استخدام الجماعات الإرهابية للإرهاب الإلكتروني لفرض سيطرتها ونشر أفكارها، قامت الباحثة ريهام العباسي بدراسة حالة لتنظيم الدولة الاسلامية في العراق والشام (داعش)، والذي اتضحت قدرتها على تطويع الاعلام والاستفادة من ثورة التكنولوجيا والاتصالات، وتوظيف الفضاء الإلكتروني على النحو الذي يحقق أهدافها، تقوم داعش باستخدام وسائل التواصل الاجتماعي لتجنيد أعضاء جدد والترويج لأفكارها وبالتالي تضمن استمرار دعم المؤيدين لها، والمتعاطفين مع فكرة دولة الخلافة، ومن ناحية آخري شن حرب نفسية شرسة ضد خصومها عن طريق نشر صور وفيديوهات الضحايا والأسري والتي تتعامل معهم بأبشع الطرق، مما يسهل لها الاجتياح السريع للأراضي والسيطرة عليها.

http://dx.doi.org/10.29009/ijres.1.3.3

وكان من نتائج زيادة والتوسع في انشطة الإرهاب الإلكتروني ان الاهتمام به ودراسته لم تقتصر على المؤتمرات والندوات والدراسات والبحوث، بل أنها اصبحت قضية راي عام تتناولها التحقيقات الصحفية والبرامج الاذاعية والتلفزيونية، ولعل ذلك تبرزه العناوين التالية: الإرهاب الإلكتروني هو إرهاب المستقبل، الشباب صيد ثمين للإرهابيين والشبكة الإلكترونية في دائرة الاتهام، (الإنترنت) سلاح الإرهاب الجديد..!، – التهديدات الإرهابية الأكثر خطورة مصدرها الإنترنت، شبكات التواصل والإنترنت في قوائم جماعات العنف، ٤٦ ألف حساب تويتر استخدمها (داعش)، في الفترة بين إعلان خلافتها وخليفتها المزعوم أبو بكر البغدادي في ٢٩ يونيو (حزيران) سنة ٢٠١٤ – بخمس لغات – وحتي ديسمبر (كانون الأول) من نفس العام.

لقد اصبح للجماعات الإرهابية انتشار كبير على الانترنت، لها الاف الصفحات والمواقع والتي تستخدمها في استقطاب الشباب من مختلف دول العالم، كما تستخدمها في الترويج لأهدافها وللدعاية الخاصة بها، فتنظيم القاعدة على سبيل المثال له العديد من المواقع الإلكترونية والصحف الإلكترونية والتي تصدر بلغات مختلفة، ومؤخراً ظهور تنظيم الدولة الاسلامية (داعش) والذي يستخدم الفضاء الإلكتروني بشكل واسع، له العديد من المواقع الإلكترونية والصحف والتي تصدر بلغات مختلفة ويستخدمها للترويج له، حيث يقوم بنشر الأعمال الإرهابية التي يرتكبها والمصورة بتقنية عالية الجودة تشبه أفلام هوليود، كذلك الترويج لنمط حياة الأفراد في المناطق التي يسيطر عليها التنظيم، وترويج وتضخيم لقوتهم لتشكيل صورة ذهنية عنهم بأنهم الأقوى والأخطر عالمياً.

وتتمثل خطورة الإرهاب الإلكتروني بشكل كبير في سهولته بمعني القدرة على القيام بالهجمات الإرهابية من المنزل، وتعدد أشكاله وتنوع أساليبه وأدواته وقدرته الهائلة على التخريب والتدمير وتوفير قدر كبير من الأمان والسلامة للإرهابيين.

إن نجاح التنظيمات الإرهابية في الإبقاء على قوتها الإعلامية على الإنترنت والاستمرار في تنفيذ هجماتها الإرهابية هو بسبب استخدام (الاتصالات المشفرة) بالإنترنت والتي تمثل طبقة عميقة يصعب اختراقها أو الوصول إلى المعلومات فيها إلا عن طريق رابط يرسله مستخدم إلى آخر. وتوضح

http://dx.doi.org/10.29009/ijres.1.3.3

الدراسات أنه من المستحيل تتبع الخطاب لمتطرف على تلك الشبكة أو اختراق المواقع بسبب الزخم المعلوماتي.

لقد بات الإرهاب الإلكتروني (Cyber Terrorism) يُمثل تهديداً واضحاً للأمن القومي للدول، حيثُ أصبحت البنية التحتية لأغلب المُجتمعات الحديثة تُدار عن طريق أجهزة الحاسب الآلي والإنترنت، وهو ما يُعرّضها لهجمات مُتعددة من (الهاكرز) و (المُخترقين) بشكل عام، ومن أجهزة المخابرات والمنظمات الإرهابية بشكل خاص.

إن مخاطر ظاهرة الإرهاب الإلكتروني وانتشارها، تتطلب ضرورة دراستها وبحثها من كافة جوانبها وتوعية افراد المجتمع ومستخدمي شبكات الانترنت والمعلومات بتلك الظاهرة وصورها ومخاطرها وأساليب مواجهتها، وتوجيه البحوث والدراسات إلى بحث ودراسة كافة جوانبها بطريقة علمية وتقديم المقترحات المناسبة لمواجهتها، وهو ما تسعي الورقة الحالية إلى تقديمه من خلال تناول النقاط التالية:

- المقصود بالإرهاب الإلكتروني وخصائصه وأسبابه.
- صور الإرهاب الإلكتروني ومخاطره.
- آليات وخطط مواجهة الإرهاب الإلكتروني.

أولا: المقصود بالإرهاب الإلكتروني وخصائصه وأسبابه

لقد تعددت تعاريف الإرهاب واختلفت وتباينت في شأنه الاجتهادات، ولم يصل المجتمع الدولي حتي الآن إلى تعريف جامع مانع متفق عليه للإرهاب؛ ويرجع ذلك إلى تنوع أشكاله ومظاهره، وتعدد أساليبه وأنماطه، واختلاف وجهات النظر الدولية والاتجاهات السياسية حوله، وتباين العقائد والأيديولوجيات التي تعتنقها الدول تجاهه، فما يراه البعض إرهاباً يراه الآخر عملاً مشروعاً. كما بذلت في هذا الشأن جهود مشكورة من أهل العلم والإنصاف، ومن بعض المجامع الإسلامية والعربية، وكذلك حاولت بعض الاتفاقيات الدولية أو الإقليمية تحديد المراد من هذا المصطلح، كما قامت بعض القوانين الجنائية الوطنية بتعريف الإرهاب، وقد اتفق معظمها على أنه:

http://dx.doi.org/10.29009/ijres.1.3.3

" كل استخدام للقوة أو العنف أو الترويع أو التخويف أو التهديد مادياً أو معنوياً الصادر من الدول أو الجماعات أو الأفراد على الإنسان، في دينه أو نفسه أو عرضه أو عقله أو ماله بغير حق، بشتي صنوف العدوان وصور الإفساد في الأرض، تنفيذاً لمشروع إجرامي فردي أو جماعي بهدف الإخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر، وإيذاء الأشخاص أو إلقاء الرعب بينهم أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر أو إلحاق الضرر بالبيئة أو بالاتصالات أو المواصلات أو بالأموال أو المباني أو بالأملاك العامة أو الخاصة أو احتلالها أو الاستيلاء عليها أو منع أو عرقلة ممارسة السلطات العامة أو دور العبادة أو معاهد العلم لأعمالها أو تعطيل تطبيق الدستور أو القوانين أو اللوائح".

للإرهاب في الغالب شكلين كما ان له ركنان فمن من أشكال الإرهاب : ارهاب الأفراد والجماعات، وارهاب الدولة وهو الشكل الأكثر تنظيماً من أشكال الإرهاب، وأكثرها تناقض مع مبادئ القانون الدولي ويعد ارهاب الدولة واضحاً في الإرهاب الذي تمارسه اسرائيل بحق الشعب الفلسطيني، اما الركنين فهما : الركن المادي ويتمثل في العنف الموجه لشخص أو مجموعة أشخاص أو ممتلكات أو منشآت، والركن المعنوي ويتمثل في توافر قصد العنف والتخويف للمستهدفين بذلك العنف وترويعهم.

اما الإرهاب الإلكتروني فعلى الرغم من عدم تمكن الباحثين من التوصل إلى تعريف محدد ودقيق له الا ان الجميع يعتبره نوع جديد من أنواع القوة الناعمة الجديدة حيث لم تعد القوة قاصرة على القوة الصلبة سواء العسكرية أو الاقتصادية والتي كانت محتكرة من قبل الدول ليس كل الدول وانما الدول الكبرى فقط، حيث ادي ظهور القوة الافتراضية إلى انهاء احتكار القوي التقليدية للقوة فأصبح كل من لديه معرفة تكنولوجية ولديه قدرة على استخدامها يمتلك القوة والقدرة على التأثير في النظام العالمي.

يعتبر العصر الحالي هو عصر الفضاء الإلكتروني Cyber Space بامتياز، فقد أصبح العمود الفقري لمعظم التفاعلات اليومية، واتجهت معظم الدول والحكومات إلى تبني نماذج الحكومات

http://dx.doi.org/10.29009/ijres.1.3.3

الذكية، وتعدي الأمر بناء مدن ذكية. ومع سهولة الاستخدام ورخص التكلفة وعظم العائد، زاد عدد مستخدمي الإنترنت، فمن المتوقع أن يصل إلى ٣,٦ مليار مستخدم بحلول عام ٢٠١٨، أي ما يُعادل نصف سكان العالم، ومع تزايد الاعتماد عليه في مجالات الحياة كافة، سواء كانت سياسية أو اقتصادية أو عسكرية أو غيرها، ومع تحوّل بعض مواقع التواصل الاجتماعي لتكون فاعلاً غير تقليدي في العلاقات الدولية، أصبحت الإنترنت سلاحاً ذا حدين، فكما هي وسيلة لتحقيق الرخاء والتقدم البشري، هناك جانب آخر مظلم، يتمثل في تزايد التهديدات والمخاطر الناجمة عن الاعتماد المتزايد عليه، في ظل عالم مفتوح تحكمه تفاعلات غير مرئية وغياب سلطة قانونية عليا تسيطر عليه.

هذا التطور الكبير في مجال الإنترنت، كماً من حيث عدد المستخدمين والخدمات التي يمكن الحصول عليها، وكيفاً من حيث تطور خصائص شبكة الويب، بالإضافة إلى تزايد الاعتماد على تطبيقات الهاتف المحمول في الحصول على خدمات الإنترنت، أوجب على الدول والحكومات أن تغير من مفاهيمها التقليدية، وأن تتبني مفاهيم تتلاءم مع عصر جديد يمكن تسميته بالعصر السيبري Cyber Age، وأن تضع سياسات تُمكنها من تعظيم الاستفادة من الإنترنت وتفادي مخاطرها، فتضخم المحتوي المعلوماتي العسكري والأمني والفكري والسياسي والاجتماعي والاقتصادي والخدمي والعلمي والبحثي، أوجد علاقة بين الإنترنت والأمن القومي، فضلاً عن ارتباط معظم الخدمات وقواعد البيانات والبني التحتية والأنظمة المالية والمصرفية بشبكة الإنترنت.

فالإرهاب الإلكتروني نتج من التزاوج بين ظاهرة الإرهاب والثورة التكنولوجية والمعلوماتية والاتصالية، وشاع استخدامه عقب الطفرة الكبيرة التي حققتها تكنولوجيا المعلومات واستخدامات الحواسب الآلية والإنترنت تحديداً في إدارة معظم الأنشطة الحياتية، حيث بات الفضاء الإلكتروني يشكل بيئة استراتيجية جديدة لنمو وبروز أشكال جديدة من الصراع ولظهور فاعلين جدد على الساحة الدولية.

http://dx.doi.org/10.29009/ijres.1.3.3

وينطلق تعريف الإرهاب الإلكتروني من تعريف الإرهاب فهو يعرف على أنه نوع من الإرهاب يعتمد على استخدام الإمكانيات العلمية والتقنية، واستغلال وسائل الاتصال والشبكات المعلوماتية، من أجل تخويف وترويع الآخرين، وإلحاق الضرر بهم، أو تهديدهم.

يعرف كذلك على أنه: العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدول، أو الجماعات أو الأفراد على الإنسان، في دينه، أو نفسه، أو عرضه، أو عقله، أو ماله بغير حق، باستخدام الموارد المعلوماتية والوسائل الإلكترونية، بشتي صنوف العدوان وصور الإفساد.

وفي ضوء ذلك تعرف تلك الدراسة الإرهاب الإلكتروني على أنه " عمل اجرامي يتم التحضير له عن طريق استخدام أجهزة الكمبيوتر والاتصالات السلكية واللاسلكية، ينتج عنه تدمير أو تعطيل الخدمات لبث الخوف بهدف ارباك وزرع الشك لدي الافراد وذلك بهدف التأثير على الحكومة أو الافراد لخدمة أجندة سياسية أو اجتماعية أو ايدلوجية، من خلال هجمات غير مشروعة أو تهديدات بهجمات ضد الحاسبات أو الشبكات أو المعلومات المخزنة إلكترونياً من أجل الانتقام أو ابتزاز أو اجبار الحكومات أو الشعوب أو المجتمع الدولي بأسره لتحقيق أهداف سياسية أو دينية".

خصائص الإرهاب الإلكتروني

يتسم الإرهاب الإلكتروني بمجموعة من السمات والخصائص تزيد من خطورته، والتي يعد معرفتها ودراستها مدخلا مناسبا لمواجهته وتجنب مخاطره، وتتمثل أبرز خصائص الإرهاب الإلكتروني فيما يلي:

١- عصري يعتمد على التقنيات الحديثة

من خلال الاعتماد على استخدام الموارد المعلوماتية والوسائل الإلكترونية التي جلبتها حضارة التقنية في عصر المعلومات، حيث يختلف الإرهاب الإلكتروني عن الإرهاب التقليدي في أنه يعتمد على التقنيات الحديثة في مجال المعلوماتية والاتصالات، وكل ما هو جديد في هذا المجال، واستغلال الإمكانات العلمية والتقنية، واستخدام وسائل الاتصال والإنترنت، في ارتكاب وتنفيذ جرائمه. فعلى سبيل المثال أجهزة ونظام تحديد المواقع عبر الأقمار الصناعية (Global Positioning System)

http://dx.doi.org/10.29009/ijres.1.3.3

المعروفة بـ (GPS)، والهواتف الجوالة المتصلة بالأقمار الصناعية، وبرامج الكمبيوتر للتعرف على الأصوات باللغات المختلفة، إلى غير ذلك، ما هي إلا أساليب تكنولوجية حديثة في العصر الرقمي، تحمل مع غيرها آفاقا واعدة في الحاضر والمستقبل، ومع ذلك قد يساء استخدامها من قبل البعض في تحقيق أهداف واعتداءات إجرامية وإرهابية، الإرهاب الصوتي Vocal Terror.

فالتكنولوجيا الرقمية الحديثة ـ وبخاصة في مجالي المعلومات والاتصالات ـ في تقدم مذهل ومتسارع يومياً، وقد يساء استخدامها في اعتداءات إجرامية أو إرهابية، تتطلب من المجتمع الدولي كله اقتراح واتخاذ كافة أساليب وإجراءات العلاج العاجلة والفعالة لمكافحة الإرهاب في العصر الرقمي.

٢- تعدد أشكاله وتنوع أساليبه

فالإرهاب الإلكتروني لا يتخذ شكلا واحدا او اسلوب واحد وانما تتعدد اشكاله وتتنوع صوره وأساليبه، تتمثل اشكاله في التجسُس الإلكتروني، والاختراقات، أو القرصنة على المواقع الحيوية للمُنشآت، والمؤسسات الرسمية في المُجتمعات المُختلفة، والتجنيد الإلكتروني من خلال ما يُطلق عليه التلقين الإلكتروني، وأخيراً التهديد والترويع الإلكتروني، كما ان ادواته متعددة متمثلة في الفيروسات اختراق البيانات وتدميرها والتجسس وتجنيد الإرهابين وجمع الاموال وتمويل العمليات الإرهابية وحروب الدعاية للأفكار المتطرفة والهدامة وغيرها.

٣- اثاره خطيره وعواقبه مدمره

حيث اشار تقرير The Norton Cybercrime Report 2011 الصادر عن شركة سيمانتك العالمية المتخصصة في أمن المعلومات – وهيي احد اشكال الإرهاب الإلكتروني - حول أوضاع جرائم المعلومات في عام ٢٠١١، والذي حمل عنوان "صورة إجمالية لأوضاع أمن المعلومات حول العالم"، إن "الفاتورة" الإجمالية لجرائم أمن المعلومات عالميا وعربيا في ٢٠١١ وحده تقدر بحوالي ٣٨٨ مليار دولار أميركي، أما التكلفة النقدية المباشرة لهذه الجرائم والمتمثلة في الأموال المسروقة ونفقات إزالة آثار الهجمات فتقدر بحوالي ١١٤ مليار دولار. ومعني ذلك أن القيمة المالية لجرائم المعلومات أكبر من السوق السوداء لمخدرات الماريجوانا والكوكايين والهيروين مجتمعين، والتي تقدر

http://dx.doi.org/10.29009/ijres.1.3.3

بحوالي ٢٨٨ مليار دولار، وتقترب من قيمة السوق العالمية للمخدرات عموما والتي تصل إلى ٤١١ مليار دولار، وأعلى من الإنفاق السنوي لمنظمة الأمم المتحدة للأمومة والطفولة (اليونيسيف) بحوالي ١٠٠ ضعف، حيث تصل ميزانيتها إلى ٣,٦٥ مليار دولار، كما تعادل هذه الخسائر ما تم إنفاقه خلال ٩٠ عاما على مكافحة الملاريا وضعف ما تم إنفاقه على التعليم في ٣٨ عاما، بل صل الامر إلى حد ما يعرف بالتدمير الإلكتروني اي تدمير المواقع والبيانات والنظم الإلكترونية، وإلحاق الضرر بالبنية المعلوماتية التحتية وتدميرها، وهو يتم إذا تمكن الإرهابيون من الدخول غير المشروع على نقطة ارتباط أساسية أو فرعية متصلة بالشبكة المعلوماتية من خلال نظام إلى (Server-PC)، أو مجموعة نظم مترابطة شبكياً (Intranet) بهدف تخريب نقطة الاتصال أو النظام، خاصة وأنه ليس هناك وسيلة تقنية أو تنظيمية يمكن تطبيقها وتحول تماما دون تدمير المواقع أو اختراقها بشكل دائم.

٤- سهولة استخدامه مع شدة أثره وضرره

حيث يمكن لمن لديه بعض المعارف والمعلومات البسيطة عن التعامل مع شبكة المعلومات الدولية الانترنت وادواتها وعلوم الحاسب ان يقوم بالعديد من جرائم الإرهاب الإلكتروني بسهولة ويؤدي إلى احداث خسائر عديدة تتجاوز حدود الدول وقد تمت إلى العالم اجمع، ومما زاد من سهوله استخدامه توفر خدمات الانترنت من خلال الاجهزة النقالة وحاسبات الجيب التي اصبحت في متناول الجميع في اي مكان وفي اي وقت، حيث يعتمد الإرهاب الإلكتروني على استغلال الإمكانات العلمية والتقنية، واستخدام وسائل الاتصال والإنترنت، من أجل تخويف وترويع الآخرين، وإلحاق الضرر بهم، أو تهديدهم وتدمير مرتكزات التنمية في البلاد ونشر الفوضى والدمار والدماء لأهداف فاسدة ومنحرفة ونشر الإشاعات الكاذبة بين الناس مما يؤدي لنشر الخوف والهلع بين الجمهور، حيث يقوم مستخدمه بعمله الإرهابي وهو مسترخ في منزله أو في مكتبه أو في غرفته الفندقية، وبعيداً عن أنظار السلطة والمجتمع، فبدلاً من استخدام المتفجرات تستطيع الجماعات والمنظمات الإرهابية من خلال الضغط على لوحة المفاتيح تدمير البنية المعلوماتية، وتحقيق آثار تدميرية تفوق مثيلتها المستخدم فيها المتفجرات، فكل ما يحتاجه الإرهابي المحترف في هذا المجال الحيوي والمعقد هو جهاز حاسب إلى

http://dx.doi.org/10.29009/ijres.1.3.3

واتصال بشبكة الإنترنت مما يتيح لهذا الإرهابي القيام بأعمال تخريبية وهو آمن في مقره بواسطة نقرات بسيطة على لوحة المفاتيح ودون أن يترك لنفسه أثراً. هذه النقرات على لوحة المفاتيح قد تنطوي على أوامر موجهة لبعض الخلايا للقيام بأعمال إرهابية معينة. ويجب أن نعترف أن الإنترنت لها مجال مفتوح وواسع وبلا حدود ويتوسع في كل يوم، ويمكنك من موقعك من أي بلد الوصول لأي مكان دون أوراق أو تفتيش أو قيود، وكل ما تحتاجه هو بعض المعلومات لتستطيع اقتحام الحوائط الإلكترونية. كما أن تكاليف القيام بمثل هذه الهجمات الإلكترونية لا يتجاوز أكثر من حاسب إلى واتصال بشبكة الإنترنت.

٥- تزايد خطورته في الدول التي تدار بنيتها التحتية بالحواسب الآلية والشبكات

ففي ظل اعتماد انشطة الحياة في المجتمعات المعاصرة على المعلوماتية وشبكة الانترنت، لك ان تتصور النتائج المترتبة على وقوع هجوم إلكتروني على أحد المواقع الإلكترونية بقصد تدميرها وشلها عن العمل، من خلال شن هجوم مدمر لإغلاق المواقع الحيوية على الشبكات المعلوماتية، وإلحاق الشلل بأنظمة القيادة والسيطرة والاتصالات، ومحطات توليد الطاقة والماء، ومواقع الأسواق المالية، بحيث يؤدي توقفها عن العمل إلى تحقيق آثار تدميرية تفوق ما تحدثه المتفجرات من كوارث، وربما يقوم أحد التنظيمات الإرهابية بهجوم إرهابي عن طريق الإنترنت على أحد البنوك والمصارف المالية بقصد السرقة والاستيلاء على الأموال، من أجل تمويل ذلك التنظيم الإرهابي، وهكذا.

٦- تخطيه للحدود وقدرته على التأثير على الجميع

فالهجوم الإلكتروني نشاط عابر للحدود ومن ثم فهو نشاط عالمي، حيث يستخدم الإرهابيون الفضاء الإلكتروني في التأثير على الرأي العام وتجنيد أعضاء جدد من مختلف أنحاء العالم والتمويل، ونشر رسالتهم والوصول إلى أكبر عدد ممكن من الجمهور وشن حرب نفسية ضد الأعداء والدعاية للتنظيم.

٧- القدرة على التخفي وتجهيل مصادر المعلومات

تتميز جرائم الإرهاب الإلكتروني بأنها صعبة الاثبات لا توجد أدلة مادية واضحة كما هو الحال في الهجمات التقليدية ويرجع صعوبة اثباتها إلى العديد من الأسباب: من يقوم بارتكابها شخص ذو درجة كفاءة عالية، وارتفع درجة الخداع والتضليل، واختلاف الزمان والمكان والقانون المطبق في الدولة التي

http://dx.doi.org/10.29009/ijres.1.3.3

ارتكبت فيها. فإذا قامت جهة ما بنسب هجمة او ارهاب إلكتروني إلى جهة معينة، ستصطدم بتحدي "الإنكار المقبول"، إذ يمكن رفض هذه التهم بكل بساطة. وبسبب إمكانية إخفاء الهوية التي يتيحها الفضاء السيبراني، ولذلك تستغله الحكومات للتجسس وجمع المعلومات الاستخبارية. ولا توجد حتي الآن أية آليات فعالة لردع الجهات الحكومية عن القيام بهجمات سيبرانية.

٨- **عدم توافر درجة عالية من اليقين في نتائج هجمات الإرهاب الإلكتروني**

ففي الهجمات التقليدية يكون الموقع المستهدف محدد والأضرار من الممكن توقعها كما أنه يمكن اصلاح تلك الأضرار بشكل سريع لأنه يسهل اكتشاف مصادر الخلل على عكس الهجمات الإلكترونية.

٩- **رخص التكلفة**

وهو ما يجعله عنصر جاذب للجماعات الإرهابية، ففي حين يحتاج الإرهاب الفعلي إلى أسلحة ومدرعات وقنابل وتحركات سرية جداً قد تصيب أو تخفق ناهيك عن التكاليف المادية لإنجاح هذه العمليات، يحتاج الإرهاب الإلكتروني إلى بعض المعلومات ليستطيع اقتحام الحواجز الإلكترونية، كما أن تكاليف القيام بهذه الهجمات لا تتجاوز جهاز حاسوب والدخول إلى الشبكة العنكبوتية.

١٠- **الصبغة الدينية للإرهاب الإلكتروني**

فالإرهاب الإلكتروني غالبا ما يكون مغطي بطبقة دينية كثيفة من الصعب إزالتها عنه إلا بقاشط حاد، ومن قبل جراحين متخصصين. فنقرأ أن اسم الموقع الإلكتروني اسم ديني. ونري أن معظم المواد المنشورة عليه تتضمن بين ثناياها - إذ لم يكن في كل سطر من سطورها – حديثاً نبوياً شريفاً، أو آية قرآنية كريمة، قد تمَّ حشرها قسراً، وتفسيرها تفسيراً قسرياً، وتمَّ لي عنقها ليّاً شديداً، لكي تناسب واقع الحال، وتُعبِّر عن المآل.

http://dx.doi.org/10.29009/ijres.1.3.3

أسباب الإرهاب الإلكتروني ودوافع انتشاره

تتعدد أسباب الإرهاب الإلكتروني ودوافع انتشاره، وهي عينها أسباب ظاهرة الإرهاب عموماً؛ لكن يجدر التنبيه إلى أن هناك العديد من العوامل والبواعث الخاصة التي تجعل من ظاهرة الإرهاب الإلكتروني موضوعاً مناسباً وسلاحاً سهلاً للجماعات والمنظمات الإرهابية، ويمكننا بيان أبرز دوافع انتشار الإرهاب الإلكتروني بوجه خاص فيما يلي:

- ضعف بنية الشبكات المعلوماتية وقابليتها للاختراق.
- غياب الحدود الجغرافية وتدني مستوي المخاطرة.
- سهولة الاستخدام وقلة التكلفة.
- صعوبة اكتشاف وإثبات الجريمة الإرهابية.
- الفراغ التنظيمي والقانوني وغياب جهة السيطرة والرقابة على الشبكات المعلوماتية.

ويوضح الشكل التالي أهم أسباب انتشار الإرهاب الإلكتروني وأهدافه.

شكل (١) يوضح أهم أسباب وأهداف الإرهاب الإلكتروني

(المصدر: شبكة الانترنت)

http://dx.doi.org/10.29009/ijres.1.3.3

ثانيا: صور الإرهاب الإلكتروني ومخاطره

يتخذ الإرهاب الإلكتروني صور واشكال متعددة، وتتمثل تلك الصور بصفة عامة في أربعة مجالات أساسية تتمثل فيما يلي:

١- استخدام الإرهابين لشبكة الانترنت في إدارة عملياتها

فالجماعات الإرهابية أصبح لها انتشار كبير على الانترنت، لها الاف الصفحات والمواقع والتي تستخدمها في استقطاب الشباب من مختلف دول العالم، كما تستخدمها في الترويج لأهدافها وللدعاية الخاصة بها، ومن خلال ما اطلق عليه الحضانات الإلكترونية أو الجماعات الإرهابية الإلكترونية، فتنظيم القاعدة على سبيل المثال له العديد من المواقع الإلكترونية والصحف الإلكترونية والتي تصدر بلغات مختلفة، ومؤخراً ظهور تنظيم الدولة الاسلامية (داعش) والذي يستخدم الفضاء الإلكتروني بشكل واسع، له العديد من المواقع الإلكترونية والصحف والتي تصدر بلغات مختلفة ويستخدمها للترويج له، حيث يقوم بنشر الأعمال الإرهابية التي يرتكبها والمصورة بتقنية عالية الجودة تشبه أفلام هوليود، كذلك الترويج لنمط حياة الأفراد في المناطق التي يسيطر عليها التنظيم، وترويج وتضخيم لقوتهم لتشكيل صورة ذهنية عنهم بأنهم الأقوى والأخطر عالمياً. وتتمثل خطورة الإرهاب الإلكتروني بشكل كبير في سهولته بمعني القدرة على القيام بالهجمات الإرهابية من المنزل، وتعدد أشكاله وتنوع أساليبه وأدواته وقدرته الهائلة على التخريب والتدمير وتوفير قدر كبير من الأمان والسلامة للإرهابيين.

وقد رصدت إحدى الدراسات أشهر المواقع والنوافذ التي تطلُّ من خلالها التنظيمات الإرهابية على العالم، وأشهرها ١٦ شبكة إعلام بعدة لغات، من بينها مؤسسة السحاب ومؤسسة الملاحم، ومؤسسة الأندلس، ومؤسسة المنارة البيضاء، ووكالة أعماق الإخبارية، ومؤسسة الفرقان، ومؤسسة الحياة، ومؤسسة أجنا.

ويوضح الشكل التالي تطور العلاقة بين الإرهاب الانترنت بالسعودية.

http://dx.doi.org/10.29009/ijres.1.3.3

شكل (٢) يوضح تطور العلاقة بين الإرهاب والانترنت

(المصدر شبكة الانترنت)

٢- تدمير المواقع والبيانات الإلكترونية والنظم المعلوماتية

ويتمثل فيما تتعرض له المجتمعات المعلوماتية الحديثة والدمار الذي قد يلحقه الهجوم الإرهابي بمنظومة المعلومات التي تتحكم في حياة هذه المجتمعات التي تعتمد على الكمبيوتر والانترنت اعتماداً مطلقا والخسائر التي قد تنجم عن مثل المعلوماتية الحديثة والدمار الذي قد يلحقه الهجوم الإرهابي، فإرهاب القضاء المعلوماتي أو إرهاب الانترنت يعتمد على القدرة على اختراق شبكات الانترنت لتحقيق أهداف عدوانية ذات طابع سياسي في الأغلب وإن كان يحلق وراءه وآثار سلمية تنال كثير من جوانب الحياة، كمُهَاجمة نُظم التحكُّم الوطني في الطيران لإحداث تصادم بين الطائرات، ومُهَاجمة نُظم التحكُّم الوطني في قطارات السككِ الحديديَّة لإحداث تصادم بين القطارات، وتعطيلُ البنوك وعمليَّات التحويل المالي، مما يُلْحِقُ الأذى بالاستثمار الأجنبي وبالثقة بالاستثمار عامةً، وإلحاق الأذى بالاقتصاد الوطني، وتعديلُ كُل من ضغط الغاز عن بُعد في أنابيب الغاز لتفجيرها، ونُظم السلامة في المصانع الكيماوية لإحداث أضرار بالناس، وأيضاً الدخولُ عن بُعد

http://dx.doi.org/10.29009/ijres.1.3.3

لنظامِ التحكُّم في علاج المرضي في المستشفيات بهدفِ قتل المرضي، وفي مصانع غذاء الأطفال لتغيير مُستويات نسب المواد الغذائيَّة بهدف قتل الأطفال.

فما يتاح للإرهاب الإلكتروني سقفا لا يمكن تصور ارتفاعه في تنفيذ عمليات إرهابية، كميا ونوعيا، فقد تشن التنظيمات الإرهابية هجمات إلكترونية، بقصد تدمير المواقع والبيانات والنظم الإلكترونية، وإلحاق الضرر بالبنية المعلوماتية التحتية وتدميرها، وتستهدف ثلاثة أهداف أساسية غالباً، وهي الأهداف: العسكرية، والسياسية، والاقتصادية، وفي عصر ثورة المعلومات تجد الأهداف الثلاثة نفسها، وعلى رأسها مراكز القيادة والتحكم العسكرية، ثم مؤسسات المنافع كمؤسسات الكهرباء والمياه، ومن ثم تأتي المصارف والأسواق المالية، وذلك لإخضاع إرادة الشعوب والمجتمعات الدولية.

٣- تبادل المعلومات الإرهابية ونشرها من خلال الشبكة المعلوماتية

حيث تساعد شبكة الانترنت المنظمات الإرهابية المتفرقة في الاتصال ببعضها البعض والتنسيق فيما بينها، وذلك نظراً لقلة تكاليف الاتصال باستخدام الانترنت، مقارنة بالوسائل الأخرى، كما أنها تمتاز بوفرة المعلومات التي يمكن تبادلها، وقد أصبح عدم وجود زعيم ظاهر للجماعة الإرهابية سمة جوهرية للتنظيم الإرهابي الحديث، مختلفاً بذلك عن النمط الهرمي القديم للجماعات الإرهابية، وكل هذا بسبب سهولة الاتصال والتنسيق عبر الشبكة العالمية.

٤- التهديد والترويع واخافة الآخرين

من خلال بث عدد من النشرات والفيديوهات التي ظهر قوة وقسوة الجماعات الإرهابية، وصور تعذيب وقتل من يخالف اوامره وتعليماتها، واستخدام وسائل الاتصال والإنترنت، من أجل تخويف وترويع الآخرين، وإلحاق الضرر بهم، أو تهديدهم وتدمير مرتكزات التنمية في البلاد ونشر الفوضى والدمار والدماء لأهداف فاسدة ومنحرفة ونشر الإشاعات الكاذبة بين الناس مما يؤدي لنشر الخوف والهلع بين الجمهور، كما حصل في إحدى العواصم العربية عندما نشر بوسائل التواصل الاجتماعي عن وجود شاب سفاح يقتل النساء فأثار الرعب في تلك العاصمة ولمدة طويلة.

http://dx.doi.org/10.29009/ijres.1.3.3

وكذلك دعوتهم إلى التمرد والثورة ومهاجمة الدولة ومرافقها، وإظهار وحشيتها في التعامل مع الشعب خاصة الفئات الفقيرة والمهمشة التي تعتبر في بعض الأحيان حاجات عند بعض الشباب خاصة الذين يعانون من الشعور بالتهميش سواء كان حقيقيا او وهميا، حيث يجدون في التنظيم وسيلة للانتقام والثأر، الوحشية هي أبرز سمات هذه الجماعات التي فاقت كل تصور بوحشيتها الدموية.

وقد لخصت إحدى الدراسات صور وأشكال الإرهاب الإلكتروني والتي يتم استخدام الفضاء الإلكتروني فيها بصورة غير مباشرة عن طريق تسهيل عملية تنفيذ العمل الإرهابي من خلال عدة ادوات، هذه الأدوات يصعب الفصل بينها بمعني أنه قد يتم استخدام كل هذه الأدوات في عملية واحده ويصعب الفصل بين الأدوات المستخدمة فيها كما يلي:

٥- **اختراق المواقع الإلكترونية**

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

٦- **الفيروسات**

فيروسات الحاسب الآلي والتي تنتشر بسرعة كبيره عن طريق شبكة الانترنت، وذلك يرجع إلى عدد الملفات الهائل التي يتم تبادلها بين مستخدمي الشبكة العنكبوتية، وهذه الفيروسات هي عبارة عن برامج تستنسخ نفسها في الجهاز وعندما تنشط هذه الفيروسات تحدث تغييرات في البرامج أو في البيئة التي تعمل فيها، ولها أضرار مختلفة تتمثل في فقد الملفات المخزنة وقد تصل تلك الأضرار إلى تحطم نظام التشغيل في الجهاز.

٧- **الحرب الإعلامية**

الفضاء الإلكتروني له تأثير هائل على الرأي العام العالمي لأنه يخاطب ملايين المستخدمين للشبكة العنكبوتية من شتي أنحاء العالم بوسائل مختلفة "الصوت- الصورة- النص"، وبالتالي أي جماعة أو منظمة يمكن لها انشاء مواقع إلكترونية تروج أفكارها وتنشرها في مختلف أنحاء العالم.

http://dx.doi.org/10.29009/ijres.1.3.3

٨- **التجسس الإلكتروني**

لقد نجحت العديد من الحكومات في استخدام تقنيات متطورة للتجسس من خلال الشبكة العنكبوتية على الدول أو المنظمات وكذلك الافراد ومراقبة المعلومات التي يتم تداولها حول العالم.

٩- **التهديد الإلكتروني**

يوجد العديد من الأساليب التي تستخدم في التهديد عبر الشبكة العنكبوتية، وتتنوع تلك الأساليب بين تهديدات باغتيال شخصيات سياسية، تهديدات بتفجيرات في مراكز سياسية أو هيئات حكومية، أو التهديد بإطلاق الفيروسات التي من شأنها تدمير أنظمة معلومات بالكامل.

١٠- ٦- **القصف الإلكتروني**

يشير إلى الهجوم على شبكة المعلومات عن طريق توجيه مئات الآلاف من الرسائل الإلكترونية إلى مواقع هذه الشبكات، وبالتالي تسبب ضغط كبير على هذه المواقع، وتفقدها قدرتها على استقبال الرسائل من العملاء، ويؤدي ذلك إلى التوقف عن العمل تماماً.

١١- **تدمير أنظمة المعلومات**

تشير إلى محاولة اختراق شبكة المعلومات الخاصة بالشركات العالمية أو بالأفراد بهدف تخريب نقطة الاتصال، وتخليق أنواع جديده من الفيروسات التي تسبب الدمار لأجهزة الكمبيوتر وللمعلومات.

مخاطر الإرهاب الإلكتروني

إن خطر الإرهاب الإلكتروني يتمثل في سهولة استخدام هذا السلاح بالإضافة إلى أثاره المدمرة، فالإرهاب الإلكتروني أصبح وحش يخيف العالم الذي بات مهدداً ومعرضاً لهجمات الإرهاب الإلكتروني، ونظراً لأن التقنية الحديثة في تطور مستمر فإن هذه المخاطر تزداد يوماً بعد يوم، أي يمكننا القول أن خطورة الإرهاب الإلكتروني تزداد بشكل كبير في الدول المتقدمة والتي تعتمد على الحواسب الآلية والشبكات المعلوماتية في إدارة بنيتها التحتية، وبالتالي قدرة الجماعات الإرهابية على تدمير البني المعلوماتية واحداث أضرار فائقة.

http://dx.doi.org/10.29009/ijres.1.3.3

وتتمثل هذه الأضرار على سبيل المثال في شل أنظمة القيادة والسيطرة والاتصالات، قطع شبكة الاتصال بين الوحدات والقيادات المركزية، تعطيل أنظمة الدفاع الجوي، التحكم في خطوط الملاحة الجوية والبحرية والخطوط البرية، اختراق النظام المصرفي والحاق الأضرار بأعمال البنوك وأسواق المال العالمية، ويتم استخدام تقنية المعلومات لإصابة المرافق الحيوية ومن ثم فان الأهداف التي تتعرض للتهديد: تخزين المعلومات، عمليات ادخال المعلومات، ارسال واستقبال الرسائل، استهداف البنية التحتية للمعلومات وخاصة في قطاعات الكهرباء والاتصالات والكمبيوتر والتي تعد وبحق ركائز الأمن القومي الجديد.

وكذلك تقديم الوصفات الجاهزة لصناعة القنابل والمُفرقعات، ومُهَاجمة نُظم التحكُّم الوطني في الطيران لإحداث تصادم بين الطائرات، ومُهَاجمة نُظم التحكُّم الوطني في قطارات السككِ الحديديَّة لإحداث تصادم بين القطارات، وتعطيلُ البنوك وعمليَّات التحويل المالي، مما يُلْحِقُ الأذىٰ بالاستثمار الأجنبي وبالثقة بالاستثمار عامةً، وإلحاق الأذىٰ بالاقتصاد الوطني، وتعديلُ كُل من ضغط الغاز عن بُعد في أنابيب الغاز لتفجيرها، ونُظم السلامة في المصانع الكيماوية لإحداث أضرار بالناس، وأيضاً الدخولُ عن بُعد لنظامِ التحكُّم في علاج المرضي في المستشفيات بهدفِ قتل المرضي، وفي مصانع غذاء الأطفال لتغيير مُستويات نسب المواد الغذائيَّة بهدف قتل الأطفال.

حيث تمكُن بعض القراصنة من اختراق مجموعة (سيتي جروب) الأمريكية، وسرقة عشرات الملايين من الدولارات، مما أصاب النظام الاقتصادي الأمريكي بخسائر فادحة، وهذا الفعل تبين بعد ذلك أنه تم بالتنسيق بين مجموعة من القراصنة الأمريكيين بعصابة روسية من خلال شبكة الإنترنت. أيضاً في عام ٢٠١٠ عقب ما عُرف بإعصار ويكيليكس (Wikileaks Storm) والذي تضمن أخطر قضايا القرصنة المعلوماتية في القرن الحالي، حيثُ تم استغلال شبكة الإنترنت العالمية في تسريب وثائق تحوي معلومات سرية للغاية مُتداولة بين الإدارة الأمريكية وقُنصلياتها الخارجية بدول العالم.

ففي دراسة حديثة لمركز "سمت" للدراسات، كشف عن حجم التغلغل الكبير للتنظيمات الإرهابية والجماعات المتطرفة عبر المنصات الإعلامية ومواقع التواصل الاجتماعي، إذ قفز

http://dx.doi.org/10.29009/ijres.1.3.3

عدد المواقع المحسوبة على هذه الجماعات من ١٢ موقعًا إلكترونيا عام ١٩٩٧ إلى ١٥٠ ألف موقع هذا العام.

كما أشارت دراسة اخري إلى ان الجماعات المسلحة قد استعانت بشبكات التواصل لتوظيفها عدة مهام تمثلت في عدة امور من ابرزها، التنسيق فيما بينها، واستخدامها كأداة عابرة لقيود المكان، وذلك من أجل مهام عدة، منها التدريب على تكوين خلايا تنظيمية، واستقطاب مزيد من الكوادر وتدريبهم على استخدام الأسلحة، والتنسيق للعمليات المسلحة وتوقيتها، والتدريب على صنع القنابل البدائية، تجنيد أتباع جدد ونشر الأفكار والمعتقدات، وغالباً ما تقوم الجماعات الإرهابية بإنشاء "مجموعة" (Group) على "تلك الشبكات" لاجتذاب المتوافقين فكرياً معها، ثم يتم بعد ذلك توجيه أعضاء المجموعة مباشرة إلى المواقع أو المنتديات المرتبطة بالجماعة الإرهابية. ويُمكِّن " بهذه الطريقة من تجنيد الأعضاء من أنحاء العالم كافة من دون أن يمثل ذلك تهديداً لهم.

اضافة إلى استخدام تلك الشبكات كساحة افتراضية للتدريب حيث يتم استضافة الفيديوهات التي يقوم المشتركون بتحميلها على الموقع (Upload) وبعد ذلك تصبح متاحة للرؤية من قبل الجميع، من أجل شرح كيفية القيام بهجمات أو استخدام الأسلحة مثل الكلاشينكوف، او تصنيع العبوات الناسفة وغيرها، وكذلك الحصول على الدعم المادي والمعنوي، حيث استخدمت الجماعات الإرهابية مواقع التواصل الاجتماعي لتسهيل التحويلات المالية فيما بينها، بجانب الحصول على التبرعات المالية، في ظل سهولة استخدام تلك المواقع لتحويل التبرعات والدعم المالي، مع عدم إمكانية التحقق من هوية متلقي تلك التبرعات في بعض الأحيان.

لقد أصبح اليوم وفي عصر الإرهاب الرقمي الحاسب الآلي وكاميرا الفيديو المحمولتين باليد، بأهمية وخطورة الكلاشينكوف وقذيفة (الآر بي ج)، من خلال استخدام الحاسب الآلي والكاميرا إلى أقصي حد ممكن، فأصبحت تقدم أدلة عسكرية ودورات تدريبية على شكل كتب وأفلام وسلايدات (بوربوينت) تتضمن معلومات شتي عن الأسلحة والتكتيكات والاغتيالات وصنع المتفجرات والسموم.

http://dx.doi.org/10.29009/ijres.1.3.3

لقد أصبحت شبكة الإنترنت الواسعة وكأنها معسكر تدريب افتراضي للإرهابيين، ومن المحزن ان لغة الغالبية العظمي من هذه المواقع هي العربية، وهي تدعو للجهاد وفي الوقت نفسه تعلم أصول صنع المواد المتفجرة والأحزمة الناسفة وغيرها. هذه المواقع الإرهابية والمتطرفة من الصعب جداً تعقبها لأنها تظهر على الشبكة الإلكترونية ثم تختفي سريعاً، والأصعب من ذلك معرفة وتتبع الأشخاص خلفها والمسؤولين عنها، وذلك لأن إمكانية إخفاء الهوية على الإنترنت تزداد سهول، ولقد نشرت صحيفة النيويورك تايمز تقريراً يؤكد أن ٩٠٪ من الهجمات الإرهابية استخدم فيها متفجرات صناعة يدوية من تلك التي توجد وصفاتها بكثرة على شبكة الإنترنت. ولقد لعب البريد الإلكتروني دوراً مهماً في التواصل بين الإرهابيين وتبادل المعلومات بينهم، حتي إن كثيراً من الحوادث الإرهابية التي حدثت في الآونة الأخيرة كان البريد الإلكتروني فيها وسيلة من وسائل تبادل المعلومات وتناقلها بين القائمين بالعمليات الإرهابية والمخططين لها.

ثالثا: آليات وخطط مواجهة الإرهاب الإلكتروني

في ضوء ما تم عرضه عن خصائص الإرهاب الإلكتروني واتساع وتعدد صوره واشكاله ومخاطره، فان الامر يتطلب ضرورة البحث عن آليات وخطط لمواجهته، حيث أصبحت هناك ضرورة عاجلة للمجتمع الدولي كله، ممثلاً في الأمم المتحدة، لاتخاذ كافة الأساليب العلاجية والإجراءات العاجلة الفعالة لمكافحة الجريمة والإرهاب في العصر الرقمي، ويمكن تلخيص ما توصلت إليه الدراسات والبحوث وتجارب الدول المختلفة فيما يلي:

١- وضعِ مفهومٍ دولي مُوحَّد للإرهاب بصفةٍ عامة، والإرهاب الإلكتروني بصفةٍ خاصة، وضرورةُ تأكيد أهمية دور وسائل الإعلام في بلورة استراتيجيات للتصدي لمزاعم الإرهابيين، وأهمية أنْ تعملَ الدولُ على ضرورة توحيد جهودها نحو وضع تشريعات داخلية صارمة لِمُكَافحة الجرائم التي تتعلَّق بالإرهاب الإلكتروني.

٢- ضرورة تثقيف المواطنين حول مخاطر الإرهاب الإلكتروني، من خلال التوعية بمخاطر الاستخدام غير الرشيد لشبكة الانترنت وبرامج محو الامية المعلوماتية Literacy

http://dx.doi.org/10.29009/ijres.1.3.3

Information وتنمية قيم ما يسمى بالمواطنة الرقمية Digital Citizenship ، فاليقظة تعتبر العامل الرئيسي في التصدي لأية تهديدات مُحتملة.

٣- السعي نحو وضع عدد من القوانين والتشريعات الجديدة لتتناسب مع طبيعة الجرائم الإلكترونية والإرهاب الإلكتروني، لتجريم أي استخدام غير آمن لتكنولوجيا المعلومات والاتصالات، مثل اصدار مصر لبعض القانين في هذا المجال من بينها (قانون التوقيع الإلكتروني رقم 15/2004، وقانون تنظيم الاتصالات رقم ١٠/ ٢٠٠٣، وقانون حماية حقوق الملكية الفكرية رقم ٨٢/ ٢٠٠٢)، قانون مكافحة الإرهاب، بتاريخ ١٦ أغسطس ٢٠١٥، والذي سلط الضوء في العديد من مواده على الدور السلبي غير المشروع لشبكة الإنترنت فيما يتعلق بـ" الإرهاب الإلكتروني أو الرقمي بالإضافة إلى التعاون والتنسيق الدائم مع الإنتربول الدولي في مجال تبادُل المعلومات والخبرات الأمنية والفنية في رصد ومُتابعة كافة الأنشطة الإجرامية والإرهابية، خاصة فيما يتعلق بالنشاط الإرهابي التكنولوجي لتزايده المُستمر من خلال عناصرِه الإجرامية المُحترفة والمُنتشرة في جميع أنحاء العالم، وارتباط هذا النشاط بشبكة المعلومات الدولية. هذا إلى جانب إنشاء إدارة مُتخصصة بوزارة الداخلية عام ٢٠٠٢، وهي إدارة مكافحة جرائم الحاسبات وشبكات المعلومات لرصد وتتبُع كافة أنواع الاستخدام غير الآمن وغير المشروع لشبكة الإنترنت، وضبط مُرتكبيها، اضافة إلى مُبادرة وزارة الاتصالات وتكنولوجيا المعلومات عام ٢٠٠٨ بإنشاء أول جهاز فني مُتخصص في حماية وتأمين البلاد من أي هجمات إلكترونية مُحتلة عبر شبكة الإنترنت.

وهذا يتطلب ضرورة أن تسن كل الحكومات والدول قوانين وعقوبات لمرتكبي الإرهاب الإلكتروني، ودعم الجهود التشريعية والأمنية، مع ضرورة تخصيص دوائر قضائية مُعينة للنظر في الجريمة الإلكترونية، والاستفادة مما انتهي إليه الاتحاد الأوروبي والدول الأخرى في مجال التشريعات الجنائية، و أن تضمن الدول أن جميع تشريعاتها المتعلقة

http://dx.doi.org/10.29009/ijres.1.3.3

بالإرهاب عبر شبكة الإنترنت) بما في ذلك حماية النظم الإلكترونية)، تتفق مع المعايير الدولية لحقوق الإنسان.

أن المعركة ضد الانتشار الواسع للتطرف والإرهاب عبر شبكة الإنترنت، تعتمد في الأساس على ضرورة "تجريم" تلك الممارسات، من خلال قوانين يتم سنها خصيصا لتشمل السلوك على الانترنت، وتضمن إجراء التحقيقات وإقامة الدعاوي القضائية بشكل فعال، والتي في الغالب تقوم على التعاون الدولي ومواءمة التشريعات الوطنية، وفي هذا الإطار تم اعتماد نهجين على المستوي العالمي، الأول يتعلق بالجرائم الإلكترونية، والثاني بمكافحة الإرهاب.

٤- تحديث القدرات الدفاعية والهجومية، لمواجهة مخاطر الحرب السيبرانية، والاستثمار في البنية التحتية المعلوماتية، وتأمينها، وتحديث القدرات العسكرية، ورفع كفاءة الجاهزية لمثل هذه الحرب عن طريق التدريب، والمشاركة الدولية في حماية البنية المعلوماتية، والاستثمار في رفع القدرات البشرية داخل الأجهزة الوطنية المعنية، مع ضرورة تصميم الشركات لبرامج حماية ضد تلك الجرائم التي ترتكب وتُهدد أمن المُجتمعات، إلى جانب أهمية دور الأفراد وحثهم على استخدام أنظمة الحماية والوقاية لكل الأضرار التي يمكن أن تلحق بأجهزتهم ومؤسساتهم، بمعني دعم تنمية الوعي الإلكتروني، والتأكيد على أهمية تشفير البيانات، وإخفاء البيانات، والاهتمام ببروتوكولات الحماية، وجُدر الحماية، ونُظم منع المتطفلين..

٥- قيام مزودي خدمة الإنترنت بالإبلاغ عن النشاط الإرهابي الملموس إن شعر بأنه يتضمن التهديد أو الإصابة الجسدية الخطيرة لأي شخص أو مؤسسة، وكذلك استخدام الأجهزة الأمنية التي تفيد في عمليات التشويش أو التعطيل لأجهزة الحاسب الآلي لمواجهة أعمال القصف الإلكتروني.

٦- محاولة التنسيق مع محركات البحث أمثال جوجل، وياهو، ويوتيوب، ووندوز لايف، ومكتوب، والفيس بوك، وغيرها لمنع دخول الإرهابيين لهذه المواقع وعدم استخدام

http://dx.doi.org/10.29009/ijres.1.3.3

مواقعهم كوسيلة نشر للفكر الإرهابي. والحذر من أن تكون هذه المواقع حامية وحاملة للإرهاب.

٧- بذل جهود دولية عاجلة ومتكاتفة لمواجهة تهديدات أمن الفضاء الإلكتروني، بإمكانية العمل على حل الصراعات على أرض الواقع لمنع انتقالها إليه، والعمل على توافق القوانين المتعلقة بالصراع الإلكتروني مع القانون الدولي وأهمية المبادرات الدولية لحماية الفضاء الإلكتروني فضلا عن البحث والتطوير في مجال الدفاعات ضد الأخطار الإلكترونية، وتعزيز أشكال التعاون الدولي في سبيل مكافحتها من أجل تعزيز أمن الفضاء الإلكتروني باعتباره مرفقا دوليا وتراثا مشتركا للإنسانية.

٨- تنظيم عمل وأنشطة ما يسمي بـ "مقاهي الإنترنت"، نظرا لأنها تعتبر نقطة الدخول الأكثر شعبية لشبكة الإنترنت، مع دراسة إمكانية إدخال بعض التدابير اللازمة لتنقية شبكة الإنترنت، وذلك من أجل التحكم في الوصول إلى المواقع الإلكترونية أو الحسابات المشبوهة التي تشكل تهديدا للأمن القومي، وفي هذا الاطار نموذجين لدولتين تمارسان السيادة على الإنترنت وهما: الصين، إذ وضعت السلطات الصينية ومقدمي خدمات الإنترنت في هذا البلد أطر عمل لمراقبة التحركات على الإنترنت والتي تحمل اسم مشروع الدرع الذهبي، المعروف كذلك باسم "جدار الصين الناري العظيم"؛ ثم هناك إيران، التي أعلنت مؤخراً عن تدابير تفرض من خلالها على شركات المراسلات الأجنبية حفظ البيانات الخاصة بالمستخدمين الإيرانيين داخل البلاد.

٩- ضرورة عقد شراكات بين الدول وبعضها البعض مع مراعاة إزالة الفجوات المتباينة، لتقديم الدعم الفني والمادي، بالإضافة إلى تعزيز التعاون بين وكالات الاستخبارات المختلفة، لتسهيل تبادل المعلومات الحساسة اللازمة لمواجهة التهديدات الإرهابية السيبرانية، حيث نجد أن التعاون الدولي مهم جدا لضمان سلامة الإنترنت، فضلا عن

http://dx.doi.org/10.29009/ijres.1.3.3

حتمية وجود تعاون لتأمين الشبكات أيضا. رغم تزايد الوعي بأهمية الأمن السيبراني، فإن إمكانيات تطبيق القانون الدولي لتنظيم سلوك الدول في الفضاء السيبراني تظل محدودة.

١٠- ضرورة مواكبة التكنولوجيا المتطورة لمواجهة التهديدات الإرهابية المحتملة، فهناك حاجة إلى تطوير وتعزيز تقنيات جديدة، للتعامل الرشيد مع ضرورة تطوير الاستخبارات الإلكترونية، (كنظام حكومي جديد وأفضل تنسيقا)، للتنبؤ بالتهديدات الإلكترونية المحتملة والعمل على ردعها.

١١- تفعيل التعاون الدولي في العديد من دول العالم من خلال الاتفاقيات الدولية لضبط وتسليم المُجرمين،، بالإضافة إلى التعاون والتنسيق الدائم مع الإنتربول الدولي في مجال تبادُل المعلومات والخبرات الأمنية والفنية في رصد ومُتابعة كافة الأنشطة الإجرامية والإرهابية، خاصة فيما يتعلق بالنشاط الإرهابي التكنولوجي لتزايده المُستمر من خلال عناصرهِ الإجرامية المُحترفة والمُنتشرة في جميع أنحاء العالم، وارتباط هذا النشاط بشبكة المعلومات الدولية. وذلك لأن الفضاء الإلكتروني بات يشكل بيئة استراتيجية جديدة لنمو وبروز أشكال جديدة من الصراع، ولظهور فاعلين جدد على الساحة الدولية.

والواقع أنه على الرغم من الوعي المتزايد بالتداعيات السياسية والاقتصادية والاجتماعية للحوادث السيبرانية، وأهمية وضرورة وجود أعراف مشتركة تسهل الوصول إلى تفاهم بين الدول، فإنه لا يزال هناك الكثير مما ينبغي القيام به لوضع معايير دولية محددة وقانون دولي قابل للتطبيق وبدون ثغرات في الفضاء السيبراني، وبالنظر للتحديات المطروحة أعلاه، فإن وضع معايير ملزمة من الناحية السياسية هي الطريقة الأفضل لتحقيق اتفاق مبدئي مشترك بين الدول، وذلك قبل الشروع في بلورة مبادئ قانونية دولية واضحة حول العالم السيبراني.

إن وضع قوانين ومعايير قابلة للتطبيق على الفضاء السيبراني سيكون بدون شك عمليةً لا تخلو من بطء وتعثر من الناحية التنظيمية، فالموافقة عليها– أي فهم طريقة تطبيقها

http://dx.doi.org/10.29009/ijres.1.3.3

–وقبولها وتعزيزها كلها من طرف الدول ما تزال تسير بإيقاع بطيء. وهو ما يرجع إلى التحديات المرتبطة بتحديد المسؤوليات والتعاريف المتناقضة حول المعني الحقيقي للأنشطة "السيبرانية"، اضافة إلى إن التوجهات السيبرانية تتطور بوتيرة أسرع بكثير مقارنة بالسياسات المتخذة للتصدي لها، الأمر الذي يضع صناع القرار في جميع أنحاء العالم أمام مجموعة كبيرة من التحديات التي لم يعد من الممكن لهم تأجيل التعاطي معها.

خاتمـــة

حاولت الورقة الحالية دراسة ظاهرة الإرهاب الإلكتروني، وتحديد المقصود بالإرهاب الإلكتروني وخصائصه وأسبابه، وصور الإرهاب الإلكتروني ومخاطره، وآليات وخطط مواجهة الإرهاب الإلكتروني. ونتمنى أن تكون الورقة الحالية مصدراً لمزيد من النقاش والدراسة عن هذه الظاهرة المدمرة، بما يؤدي لاجتثاثها من جذورها.

http://dx.doi.org/10.29009/ijres.1.3.3

المراجع العربية

- الألفي، محمد محمد. (٢٠١٤). الإرهاب الإلكتروني من التدمير إلى المواجهة – مجلة لغة العصر، مجلة الاهرام للكمبيوتر والانترنت والاتصالات – عدد2014-12-4 – مؤسسة الاهرام – القاهرة – ٢٠١٤.
- بشير، هشام. (٢٠١٤). الإرهاب الإلكتروني في ظل الثورة التكنولوجية وتطبيقاته في العالم العربي، افاق سياسية، العدد السادس، يونيو ٢٠١٤.
- التتر، سامي، والحميداني، سعيد. (٢٠١٧). الإرهاب يغزو شبكات التواصل الاجتماعي: تحريض.. تجنيد.. ودعاية سوداء، متاح على http://www.alriyadh.com/alyamamah/article/955131
- الجحنة، عادل عبدالصادق. (٢٠٠٩). أثر الإرهاب الإلكتروني على مبدأ استخدام القوة في العلاقات الدولية(٢٠٠١– ٢٠٠٧)، رسالة ماجيستير غير منشورة، كلية الاقتصاد والعلوم السياسية، جامعة القاهرة،،٢٠٠٩.
- الجحنة، عادل عبدالصادق. (٢٠٠٩). الإرهاب الإلكتروني والقوة في العلاقات الدولية: نمط جديد وتحديات مختلفة، مركز الدراسات السياسية والاستراتيجية بالأهرام،، القاهرة، (٢٠٠٩).
- جعجع، عبد الوهاب. (٢٠١٧). الامن المعلوماتي وإدارة العلاقات الدولية متاح على https://www.politics-dz.com/threads/almn-almylumati-u-dar-alylaqat-alduli.10851
- حسنين، رجب عبد الحميد. (٢٠١٢). أمن شبكات المعلومات الإلكترونية: المخاطر والحلول.– Cybrarians Journal – ع ٣٠ (ديسمبر ٢٠١٢).
- خليفة، ايهاب خليفة: كيف تحمي الدول أمنها وتدير شؤونها في عصر الإنترنت؟ متاح على https://futureuae.com/ar-AE/FutureFile/Item/12/cyber-politics-%D9%83%D9%8A%D9%81-
- الدهشان، جمال علي. (٢٠١٦). "الإرهاب الإلكتروني احد صور الإرهاب في عصر المعلوماتية مظاهره، واساليب مواجهته"– ورقة عمل مقدمة إلى – المنتدي الجغرافي الأول بعنوان الإرهاب في مصر بين الواقع الجغرافي والمرتكزات الثقافية والنفسية والاجتماعية–

http://dx.doi.org/10.29009/ijres.1.3.3

الذي نظمه قسم الجغرافيا بكلية الاداب جامعة المنوفية يوم الاثنين الموافق ٥ ديسمبر٢٠١٦ بقاعة المؤتمرات بالكلية.

- الدهشان، جمال علي. (٢٠١٦). المواطنة الرقمية مدخلا للتربية العربية في العصر الرقمي"- نقد وتنوير- السنة الثانية – العدد الخامس- نيسان/إيار/حزيران (٢٠١٦).
- الدهشان، جمال علي. (٢٠١٧). توظيف شبكات التواصل الاجتماعي في خدمة العملية التربوية والتعليمية لماذا؟ في ماذا؟ وكيف؟ – ورقة عمل مقدمة إلى المؤتمر العلمي الدولي الثاني لمجتمع العربي وشبكات التواصل الاجتماعي في عالم متغير في الفترة من 31أكتوبر - 2نوفمبر2017 م الإعلام- كلية الآداب والعلوم الاجتماعية – جامعة السلطان قابوس، مسقط، سلطنة عمان.
- الدهشان، جمال علي. (٢٠١٧). جمال الدهشان يكتب: الإرهاب الإلكتروني اخطر اشكال الإرهاب في عصر المعلوماتية متاح على http://www.shbabalnil.com/%d8%a7%d9%84%d8%af%d9%83%d8%aa%d9%88%d8%b1-%d8%ac%d9%85%d8%a7%d9%84
- الدهشان، جمال علي. (٢٠١٧). محو الامية المعلوماتية للمراة العربية مدخل للتنمية المستدامة في العصر الرقمي- ورقة عمل مقدمة إلى مؤتمر الاتحاد العربي للمراة المتخصصة فرع القاهرة بعنوان "المراة وتكنولوجيا جودة الحياة " الذي عقد بالمركز الكشفي العربي العالمي بمدينة نصر بالقاهرة يوم السبت ٩ ديسمبر ٢٠١٧.
- الدهشان، جمال علي. (٢٠١٨). دور تكنولوجيا المعلومات في دعم التحولات الديمقراطية: الديمقراطية الرقمية نموذجا، المجلة الدولية للبحوث في العلوم التربوية، المجلد الاول العدد الثاني، مارس ٢٠١٨.
- الدهشان، جمال علي. (٢٠١٨). محو الامية المعلوماتية الدوائية Pharmaceutical Information Literacy احد مجالات تعليم الكبار في العصر الرقمي – المؤتمر السنوي السادس عشر لمركز تعليم الكبار بجامعة عين شمس تعليم الكبار في العصر الرقمي « التحدي العربي الكبير « لال الفترة من ١٦ إلى ١٨ ابريل ٢٠١٨ بدار الضيافة بجامعة عين شمس.

http://dx.doi.org/10.29009/ijres.1.3.3

- الدهشان، جمال علي.(٢٠١٤). الدور السياسي لتكنولوجيا المعلومات والاتصالات في العصر الحديث – مجلة الجامعة الاسلامية ع٤٨ - رابطة الجامعات الاسلامية – ٢٠١٤.
- الدهشان، جمال علي.. (٢٠١٨). الإرهاب الإلكتروني في عصر المعلوماتية، مظاهره، وإليات مواجهته –ورقة عمل مقدمة إلى المؤتمر الدولي الثاني للجنة علوم الإدارة بالمجلس الاعلى للثقافة بالقاهرة – بعنوان "الإدارة المجتمعية لمحاربة الإرهاب"- بدار الاوبرا المصرية – السبت ٦ فبراير ٢٠١٨.
- الراشد، عبدالعزيز. (٢٠١٧). النت سلاح، الإرهاب الجديد، استغلوا التطور التقني للترويج لأجندتهم والتنسيق لعملياتهم عن بُعد متاح على http://www.alriyadh.com/1006999
- الرميح، يوسف بن أحمد. (٢٠١٧). الإرهاب الإلكتروني وشبكات التواصل الاجتماعي متاح على http://www.al-jazirah.com/2015/20150323/ar2.htm
- الزنط، سعد عطوة. (٢٠١٠). الإرهاب الإلكتروني واعادة صياغة استراتيجيات الأمن القومي، مؤتمر الجرائم المستحدثة- كيفية اثباتها ومواجهتها،(المركز القومي للبحوث الاجتماعية والجنائيةبالقاهرة في الفترة من ١٥-١٦/ ١٢/ ٢٠١٠.
- السند، عبد الرحمن بن عبد الله. (٢٠١٧). وسائل الإرهاب الإلكتروني حكمها في الإسلام وطرق مكافحتها متاح على http://shamela ws/browse.php/book-1244/page-9
- شمش الدين، فتحي. (٢٠١٧). الإرهاب الإلكتروني.. خطر المستقبل المتعاظم - مجلة لغة العصر مجلة الاهرام للكمبيوتر والانترنت والاتصالات عدد 4-9-2017 – مؤسسة الاهرام – القاهرة – ٢٠١٧.
- صادق، عادل. (٢٠١٧). الهجمات السيبرانية": انماط وتحديات جديدة للأمن العالمي – المركز العربي لابحاث الفضاء الإلكتروني متاح على http://accronline.com/article_detail.aspx?id=29088
- الصالح، مصلح. (٢٠٠٢). ظاهرة الإرهاب المعاصر، طبيعتها وعواملها واتجاهاتها - مركز الملك فيصل للدراسات والبحوث الإسلامية، الرياض، ٢٠٠٢.

http://dx.doi.org/10.29009/ijres.1.3.3

- العباسي، ريهام عبدالرحمن رشاد. (٢٠١٥). أثر الإرهاب الإلكتروني على تغير مفهوم القوة في العلاقات الدولية (2001-2015)دراسة حالة: تنظيم الدولة الاسلامية في العراق والشام (داعش) – المركز الديمقراطي العربي – 24يوليو ٢٠١٦.
- عبد الصبور، سماح. (٢٠١٤). الإرهاب الرقمي: أنماط استخدام الإرهاب الشبكي، مجلة (اتجاهات الأحداث) الصادرة عن مركز المستقبل، العدد الثاني، سبتمبر ٢٠١٤، متاح على https://futureuae.com/ar-AE/Mainpage/Item/227/%D8%A7%D9%84%D8%A5%D8%B1%D9%87%D
- العجلان، عبدالله بن عبدالعزيز بن فهد. (٢٠٠٨). الإرهاب الإلكتروني في عصر المعلومات، بحث مقدم إلى المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الإنترنت"، والمنعقد بالقاهرة في المدة من ٢ – ٤ يونيو ٢٠٠٨م.
- العربي، محمد مسعد العربي:. (٢٠١٤). العصر الرقمي الجديد.. إعادة تشكيل مستقبل الأفراد والأمم والأعمال – السياسة الدولية – مؤسسة الاهرام القاهرية – عدد 2014-12-7.
- عطية، ايسر محمد. (٢٠١٤). دور الآليات الحديثة للحد من الجرائم المستحدثة: الإرهاب الإلكتروني وطرق مواجهته، مؤتمر الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية المنعقد بكلية العلوم الاستراتيجية بعمان، في الفترة من (٢-٤/ ٩/ ٢٠١٤).
- غباره، عبدالباسط. (٢٠١٧). الإنترنت.. الذراع الأخطر للتنظيمات الإرهابية متاح على http://www.afrigatenews.net/content/%D8%A7%D9%84%D8%A5%D9%86%D8%AA%D8%B1%D9%86%D8%AA-
- قيسي، نوال. (٢٠١١). بعض جرائم الانترنت الموجهة ضد مستخدمي الانترنت، رسالة ماجستير غير منشورة، كلية العلوم الاجتماعية جامعة الامام محمد بن سعود الاسلامية.
- الكردي، احمد السيد: امن المعلومات ماهيتها وعناصرها واستراتيجياتها متاح على http://kenanaonline.com/users/ahmedkordy/posts/323552

http://dx.doi.org/10.29009/ijres.1.3.3

- اللواتي، نسرين فوزي. (٢٠١٧). تجريم الانفلات الإلكتروني..خطوة في الاتجاه الصحيح – مجلة لغة العصر، مجلة الاهرام للكمبيوتر والانترنت والاتصالات – عدد 13-10-2015 – مؤسسة الاهرام – القاهرة – ٢٠١٧.
- المنيري، شيريهان نشأت. (٢٠١٢). الإرهاب الإلكتروني: " ندوة" مخاطر جرائم الإنترنت على استقرار النظام الدولي– المركز الدولي للدراسات المُستقبلية والاستراتيجية – القاهرة – ابريل ٢٠١٢.
- النابلسي، شاكر. (٢٠١٨). من الإرهاب المسلح إلى الإرهاب الآليكتروني متاح على http://www.ahl-alquran.com/arabic/show_article.php?main_id=7350
- ناعوس، بن يحيي الطاهر. (٢٠١٥). مكافحة الإرهاب الإلكتروني ضرورة بشرية وفريضة شرعية – مكتبة الالوكة – ٢٠١٥.

http://dx.doi.org/10.29009/ijres.1.3.3

References

- Abbasi, Reham Abdul Rahman Rashad. (2015). The Impact of Electronic Terrorism on the Change of the Concept of Power in International Relations (2001-2015) Case Study: Organization of the Islamic State in Iraq and Syria (Da'ash) - Arab Democratic Center - July 24, 2016.

- Abdel-Sabour, Samah. (2014). Digital Terrorism: Patterns of Use of Network Terrorism, Journal of Events Trends, Center for the Future, Issue 2, September 2014, available at https://futureuae.com/en-US/Mainpage/Item/227/%D8%A7%D9 % 84% D8% A5% D8% B1% D9% 87% D

- AL- Arab, Mohamed Massad Arab:. (2014). The New Digital Age: Re - shaping the Future of Individuals, Nations and Business - International Policy - Al - Ahram Foundation - 7-12-2014.

- Al-Ajlan, Abdullah bin Abdulaziz bin Fahad. (2008). Electronic Terrorism in the Information Age, presented to the First International Conference on "Protection of Information Security and Privacy in Internet Law", held in Cairo from 2 to 4 June 2008.

- Al-Alfi, Muhammad Muhammad. (2014). Electronic terrorism from destruction to confrontation - Journal of the language of the age, Journal of Al-Ahram for computer and the Internet and communications - Number 4-12-2014 - Al-Ahram - Al-Fayha - 2014.

- Aljajah, Adel Abdel Sadik. (2009). The Impact of Electronic Terrorism on the Use of Force in International Relations (2001-2007), Unpublished MA Thesis, Faculty of Economics and Political Science, Cairo University, 2009.

- Aljajah, Adel Abdul Sadig. (2009). Electronic Terrorism and Power in International Relations: A New Pattern and Different Challenges, Center for Political and Strategic Studies, Cairo, Egypt (2009).

- ALlawaty, Nasreen Fawzi. (2017). Al - Ahram Journal of Computer, Internet and Communications - No. 13-10-2015 - Al - Ahram Foundation - Al - Fayha - 2017.

- Al-Muniri, Shirihan Nashat. (2012). E-terrorism: Seminar on the risks of cybercrime on the stability of the international system - International Center for Future and Strategic Studies - Cairo - April 2012.

- Al-Rashed, Abdulaziz. (2017). The new weapon, the new terrorism, exploited the technical development to promote their agenda and coordinate their operations remotely is available at http://www.alriyadh.com/1006999

- Alsaleh, Mosleh.. (2002). The phenomenon of contemporary terrorism, nature, factors and trends - King Faisal Center for Islamic Studies and Research, Riyadh, 2002.

http://dx.doi.org/10.29009/ijres.1.3.3

- Alsanad, Abdul Rahman bin Abdullah. (2017). The means of electronic terrorism in Islam and its methods of combating it is available at http: // shamela ws / browse.php / book-1244 / page-9

- Altter, Sami, and Hamidani, Said. (2017). Terrorism invades social networks: incitement.. recruitment.. and black propaganda, available at http://www.alriyadh.com/alyamamah/article/955131

- Al-Zant, Saad Atwa. (2010). Electronic terrorism and redrafting of national security strategies, the conference of new crimes - how to prove and confront them, (National Center for Social and Criminal Research in Cairo from 15-16/12/2010.

- Attia, Iser Mohammed. (2014). The role of modern mechanisms to reduce the new crimes: electronic terrorism and ways to confront it, the conference of crimes created under the changes and regional and international changes held in the Faculty of Strategic Sciences in Amman, from (2-4 / 9/2014).

- Bashir, Hisham. (2014). Electronic Terrorism in the Shadow of the Technological Revolution and its Applications in the Arab World, Political Outlook, Issue 6, June 2014.

- Dust, Abdel Basset. (2017). The Internet: the most dangerous arm of terrorist organizations is available at :

http://www.afrigatenews.net/content/%D8%A7%D9%84%D8%A5%D9%86%D8%AA %D8%B1%D9%86% D8% AA-

- EL-Dahshan, Jamal Ali (2014). The Political Role of Information and Communication Technologies in Modern Times - Islamic University Magazine, p. 48 - Association of Islamic Universities - 2014.

- EL-Dahshan, Jamal Ali.. (2018). - Electronic terrorism in the era of informatics, its manifestations, and mechanisms to face it - A working paper submitted to the second international conference of the Science Committee of the Supreme Council of Culture in Cairo - entitled "Community Management to Fight Terrorism" - at the Egyptian Opera House - Saturday 6 February 2018.

- El-Dahshan, Jamal Ali. (2016). "Electronic terrorism is one of the forms of terrorism in the era of informatics, its manifestations and methods of confronting it." - Working paper presented to the first geographical forum entitled "Terrorism in Egypt between geographical reality and the cultural, psychological and social foundations" organized by the Department of Geography, Faculty of Arts, Monofiya University, Monday, December 5, 2016 College.

- El-Dahshan, Jamal Ali. (2016). Digital Citizenship is an Introduction to Arabic Education in the Digital Age "- Criticism and Enlightenment - Second Year - Issue No. 5 - April (2016).

http://dx.doi.org/10.29009/ijres.1.3.3

- EL-Dahshan, Jamal Ali. (2017). Employment of social networks in the service of the educational process Why? In what? And how? - Working paper presented to the Second International Scientific Conference of the Arab Society and Social Networking in a Changing World in the period from 31 October to 2 November 2017. Media - Faculty of Arts and Social Sciences - Sultan Qaboos University, Muscat, Sultanate of Oman.

- El-Dahshan, Jamal Ali. (2017). Jamal al-Dahshan writes: Electronic terrorism is the most dangerous form of terrorism in the age of information is available on http://www.shbabalnil.com/%d8%a7%d9%84%d8%af%d9%83%d8%aa%d9%88 % d8% b1-% d8% ac% d9% 85% d8% a7% d9% 84%

- El-Dahshan, Jamal Ali. (2017). The Arab Women's Women's Center in Cairo, entitled "Women and Quality of Life Technology" held at the Arab International Scout Center in Nasr City, Cairo, on Saturday, December 9, 2017.

- EL-Dahshan, Jamal Ali. (2018). Literacy Information Literacy One of the areas of Adult Education in the Digital Age - 16th Annual Conference of the Center for Adult Education at Ain Shams University Adult Education in the Digital Age "The Great Arab Challenge" for the period from 16 to 18 April 2018 at the Hospitality House at Ain Shams University.

- El-Dahshan, Jamal Ali. (2018). The Role of Information Technology in Support of Democratic Transitions: Digital Democracy as a Model, International Journal of Research in Educational Sciences, vol. I Issue 2, March 2018.

- Garrett، R. K.، "Protest in an Information Society: A Review of Literature on Social Movements and New ICTs Information"، Communication and Society، Vol. 9، No. 2، 2006، pp 5 – 8.

- Geagea, Abdel Wahab. (2017). Information security and international relations management are available at https://www.politics-dz.com/threads/almn-almylumati-u-dar-alylaqat-alduli.10851

- Geoff Dean، Peter Bell، Jack Newan، The Dark Side of Social Media :Review of Online Terrorism، Pakistan Journal of Criminology، Vol. 3، No. ،٤ April – July 2012، pp 194 – 195.

- Hassanein, Rajab Abdel Hamid. (2012). Security of Electronic Information Networks: Risks and Solutions. - Cybrarians Journal - p. 30 (December 2012).

http://dx.doi.org/10.29009/ijres.1.3.3

- James A. lewis، Assessing the Risks of Cyber Terrorism، Cyber War and Threats، Center for Strategic and International Studies ،December 2002، available at : http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf
- Joseph Nye، "Smart Power and The War on Terror"، Asia Pacific Review، Vol. 15، no. 1، 2008، p 11.
- Joseph Nye، The Paradox of American Power: Why the World's Only Super Power Cannot Go It Alone، (Oxford University Press، 2002) pp 85-86.
- Khalifa, Ihab Khalifa: How do States protect their security and manage their affairs in the age of the Internet? Available at https://futureuae.com/en-US/FutureFile/Item/12/cyber-politics-%D9%83%D9%8A%D9%81-
- Kurdiy, Ahmed Al-Sayed: Information security, its elements and strategies available at http://kenanaonline.com/users/ahmedkordy/posts/323552
- Nabulsi, Shaker. (2018). From armed terrorism to cyber terrorism is available at http://www.ahl-alquran.com/arabic/show_article.php?main_id=7350
- Naous, son of Yahya al-Tahir. (2015). Combating Electronic Terrorism - Human Needs and Legitimacy - Al - Wakah Bookshop - 2015.
- Philip Seib and Dana M. Janbek، Global Terrorism and New Media: The Post-Al Qaeda Generation، (New York: Routledge، 2011)، p. 44
- Qaisi, Nawal. (2011). Some Internet Crimes Against Internet Users, Unpublished Thesis, Faculty of Social Sciences, Imam Muhammad Bin Saud Islamic University.
- Ramih, Yousef bin Ahmed. (2017). Electronic terrorism and social networks are available at http://www.al-jazirah.com/2015/20150323/en2.htm
- Sadiq, Adel. (2017). Cyber attacks ": new patterns and challenges for global security - The Arab Center for Space Research is available at http://accronline.com/article_detail.aspx?id=29088
- Shams al-Din, Fathi. (2017).. The danger of the future growing - Journal of the age of the Journal Journal of Al-Ahram for computer and Internet and communications No. 4-9-2017 - Al Ahram Foundation - Cairo - 2017.

http://dx.doi.org/10.29009/ijres.1.3.3