الجهاد الإلكتروني: دراسة لتنظيم داعش، واستراتيجية الولايات المتحدة لمواجهته

د. إنجـــي محمد مهدي *

مستخلص

تقدم الورقة دراسة عن حالة الصراع علي الفضاء الإلكترونى ما بين الخلافة الإلكترونية لتنظيم داعش، واستراتيجية الدفاع الإلكتروني للولايات المتحدة من خلال تناول الموضوعات التالية: سياسة الجهاد الإلكترونى لتنظيم داعش، وظاهرة الذئاب المنفردة فى إطارها، وأخيرا استراتيجية الولايات المتحدة لمواجهة مثل هذا النمط من الإرهاب.

يعكس استخدام تنظيم داعش للفضاء الإلكترونى تميزا واضحا على غيره من الجماعات الإرهابية الأخرى. وإن توظيف داعش للإنترنت يعكس قدرا كبيرا من الاحترافية والتعقيد فى الأداء، كما يبرز فهما عميقا عند قيادات التنظيم للروابط بين عالم الإعلام، وخاصة وسائل التواصل الاجتماعى، وعالم العمليات. لقد تمكن التنظيم الإرهابي من استخدام الإعلام لتعظيم آثار أنشطتهم العملياتية. وهناك أيضا استراتيجية داعش اللامركزية، وقوامها الإرهاب من خلال الذئاب المنفردة، للإشارة إلى تحريض مجموعة من الأفراد على تنفيذ أعمال إرهابية بصفة منفردة، فى مناطق بعيدة، بعد أن انحسرت انتصاراته فى المناطق المحدودة الخاضعة لسيطرته، عقب إحكام جهود مكافحته وملاحقة قياداته وأتباعه وتقديمهم للمساءلة. ويكون توجيه القيادات إلكترونيا لتصنيع قنابل شديدة الانفجار بأدوات بدائية لتنفيذ الأعمال الإرهابية الخطيرة.

ومن ناحية أخرى، تسعى جهود الولايات المتحدة لمكافحة داعش إلى التضييق عليه ومنع فرص انتشاره وتوغله. ولقد سعت وزارة الدفاع الأمريكية إلى دمج العمليات الإلكترونية مع قدراتها العسكرية التقليدية والتخطيط الاستراتيجى للعمليات العسكرية، ولديها فرق إلكترونية متكاملة ذات قيادة إقليمية، منتشرة خارج وداخل الولايات المتحدة.

لقد ألقت الحرب علي تنظيم داعش الضوء على ضغط البنتاجون من أجل إعداد قواته لما يسمى "العمليات متعددة المجالات" لدمج العمليات الإلكترونية فى كل مراحل التخطيط، فضلا عن زخم غير مسبوق علي مستوى التشريعات الأمريكية لمواجهة الجريمة الإرهابية وما يرتبط بالإرهاب الإلكترونى خاصة.

* أستاذ مساعد بقسم العلوم السياسية، كلية الاقتصاد والعلوم السياسية،جامعة القاهرة.
Email: engymm@feps.edu.eg

كلمات مفتاحية: الإرهاب الإلكترونى- الجهاد الإلكترونى- الذئاب المنفردة- الإرهاب الموجه عن بعد- العمليات متعددة المجالات.

Abstract:

The paper presents a study on the state of conflict in cyberspace between the cyber terrorism of ISIS and the cyber defense strategy of the United States.

ISIS's use of cyberspace reflects a clear distinction from other terrorist groups. ISIS's employment of the Internet reflects a great deal of professionalism and complexity in performance, as well as a deep understanding among the organization's leaders of the links between the media world, especially social media, and the world of operations. The terrorist organization has been able to use the media to maximize the effects of their operational activities. There is also ISIS's decentralization strategy, which is based on terrorism through lone wolves, to refer to inciting a group of individuals to carry out terrorist acts alone, in remote areas, after ISIS victories receded in the limited areas under its control, because of tightening efforts to combat it and prosecute its leaders and followers and bring them to justice.

On the other hand, the United States' efforts to combat ISIS seek to restrict it and prevent opportunities for its spread and penetration. The US Department of Defense has sought to integrate cyber operations with its conventional military capabilities and strategic planning for military operations, and has coherent regional-command electronic teams deployed outside and within the United States.

The war on ISIS has shed light on the Pentagon's pressure to prepare its forces for so-called "multi-domain operations" to integrate electronic operations in all stages of planning, as well as an unprecedented momentum at the level of US legislation to confront terrorist crime and what is related to cyber terrorism in particular.

Key words: ***Cyber Terrorism- Cyber Jihad- Lone wolves-Remote directed terrorism-Multi Domain Operations.***

مقدمة:

يستخدم تنظيم داعش الفضاء الإلكترونى بشكل مكثف وناجح على نحو غير مسبوق يتفوق فيه على كل الجماعات الإرهابية الأخرى، حيث يرى الخبراء أن توظيف داعش للإنترنت يعكس قدرا كبيرا من الاحترافية والتعقيد في الأداء. سواء فيما يتعلق بعدد المنصات الاعلامية التابعة له أو التقنيات التي يستخدمها أو الموضوعات التي يتناولها أو الجمهور الذي يستهدفه(١).

ومنذ نشأته الحديثة، يعتبر داعش الإعلام أداة قتال رئيسة في معركته مع الأعداء، ومن ثم يعمد منظروه لإيلاء أهمية خاصة للفضاء الالكتروني كوسيلة أساسية لنقل المخرجات الاعلامية للتنظيم والتي تتسع لتشمل المجلات، الأفلام الوثائقية، الإصدارات المرئية، وكالات الأنباء، المحطات الاذاعية.. وغيرها، تتم ترجمتها إلى لغات مختلفة. كما نجح التنظيم على نحو لافت في توظيف شبكات التواصل الاجتماعي، والتي لم تصبح فقط عنوان لهويته الالكترونية وإنما منصة للسلطة والقوة. ومن أبرز المنصات الالكترونية التي تبث أخبار التنظيم بانتظام: مؤسسة آفاق – الأشهاد- الفرقان – الفرات للإعلام النصرة الشامية – الوعد – البتار – الثبات -الحياة – الخيال – الصمود الغريب- جيش أبناء الخلافة – حفيدات عائشة – شهداء اليرموك – شرق أفريقيا- صناعة الرجال – عزة الجهاد اليقين- ابن تيمية للإعلام – أنصار الخلافة في غزة – ترجمان الأساورتى – جيش أبناء الخلافة الالكتروني.. وغيرها.

أولا: الجهاد الإلكترونى لتنظيم داعش:

عمد تنظيم داعش إلى إصدار مجلات دورية شهرية وأسبوعية عديدة تأتي على رأسها مجلة النبأ ودابق، وغيرها من المجلات التي تصدر باللغات الأجنبية مثل دار السلام والرومية الفرنسية، وعدد آخر من القنوات والمجلات التي تصدر بعدة لغات، منها مجلة الشباب الأسبوعية. ومن خلال استقراء المحتوى الذي تبثه هذه المنصات يمكن التأكد من احترافية القائمين على استراتيجية داعش الاعلامية، الأمر الذي يظهر جليا من خلال استخدام عناوين مؤثرة باقتباس بعض العناوين من القرآن الكريم، أو ربط هذه العناوين بتاريخ الاسلام وبطولاته ومنها على سبيل المثال: *"فتربصوا انا معكم متربصون"* وهي عنوان كلمة صوتية لأبو بكر البغدادى، *"هذا وعد الله"* وهو إصدار مرئى يوضح سير المعارك في جبل مكحول، وكذلك الاصدار المرئي *شفاء الصدور"* والذي يوضح حرق الطيار الأردني معاذ الكساسبة، واصدار *"صليل الصوارم"*، *"رسائل من أرض الملاحم"* وغيرها الكثير(٢).

ويعمل التنظيم على تجديد المحتوى المنشور له عبر قنواته الافتراضية، بالتركيز على الأخبار العاجلة التي لا يتعدى مداها الزمني ٤٨ ساعة، لإعلام أفراده بتحركاته، وكذلك لتشتيت القوات الأمنية، وتثبيط نجاحاتهم ضده، وتوصيل رسالة مفادها أن التنظيم مازال موجودا. علاوة على ذلك، نشر المعلومات عن العمليات التي يقوم بها باقي الذئاب المنفردة، وتبني العمليات الإرهابية حتى ولو كانت خارج أعضائه(٣).

كما تعكس متابعة المحتوى الإعلامي لداعش في الفضاء الافتراضي أن لدي التنظيم نوعين من الرسائل حسب الجمهور المستهدف، وهما(٤):

١. الرسائل الإيجابية التطمينية.
٢. رسائل عنيفة أو ترهيبية.

- الرسائل الإيجابية التطمينية، التي تستهدف السكان في المناطق الخاضعة لسيطرتها التامة مثل مدينة الرقة علي سبيل المثال، وتتضمن نجاحات داعش في تكوين مؤسسات وتوفير الخدمات الأساسية للمواطنين من الغذاء والسكن، وكيف أن نظام الحكم يطبق العدل في القضاء، ويوفر الأمن، ما يمثل حوالي ٢٥% من إجمالي الدعاية، كما تتضمن تلك الدعاية فيديوهات لشباب حسن المظهر مهندمين الثياب شكلهم كشكل أي شاب وسيم في بلاد العالم أجمع ويتكلمون عن ضرورة وأسباب انضمام الفرد لداعش، ما يظهر داعش كحركة اجتماعية إنسانية عالمية تطالب بالعدل، والحق وليست منظمة إرهابية.
- رسائل عنيفة أو ترهيبية، تتضمن الأعمال الوحشية ذات الإطار العنيف المصاغ بشكل مسرحي استعراضي مناسب للاتجاهات السائدة كشئ شائع، ومحبوب بشكل مألوف للأفراد من كل أنحاء العالم، يعمل على تسهيل تقبلهم الأحداث العنيفة التي يستهلكونها سواء في ألعاب الفيديو أو في الأفلام والمسلسلات أو يشاهدونها في الأخبار، ويتم التركيز على المشاهد التي ينتصر فيها مقاتلو التنظيم والمشاهد التي يقاتلون فيها بشجاعة.

أما فيما يتعلق بالجمهور المستهدف لداعش على الانترنت، فيمكن القول أن التنظيم تمكن من تحقيق عدد من النجاحات حيث تنوعت الأدوات التي يعتمد عليها التنظيم في استراتيجياته الاتصالية بحسب الفئات المستهدفة، ولغاتها والتوقيت والطرق المتبعة. ومما يحسب للتنظيم في هذا السياق حرص داعش على مخاطبة المتلقي الأجنبي لاسيما الأوروبي، ولم يرتكز على خطاب الشعب العربي كما فعل "القاعدة"، وهو ما مكنه من استقطاب عدد كبير من المتعاطفين. فضلا عن سعيه التجنيد المبكر لمنتسبيه من خلال استقطاب المراهقين، المداومين على الألعاب بشكل كبير، عبر محاولة مخاطبة "اللاوعي" لديهم. إلى جانب التركيز على الهوية بشكل مكثف بحيث يصبح

علمهم "المزعوم" مألوفا للمستخدمين، وكذلك بعض مفرداتهم كمصطلح "الدولة الإسلامية"، وتصدير النماذج الإرهابية في التنظيم كرموز"، وحتى طريقتهم في اللباس والعيش، والتعامل مع المرأة ، والنظرة للحياة، وغير ذلك(٥).

إن الشئ الفريد في داعش هو حقيقة امتلاكهم فهما عميقا للروابط بين عالم الإعلام، وخاصة وسائل التواصل الاجتماعي وعالم العمليات، حيث تمكنوا بنجاح كبير من استخدام الإعلام لتعظيم آثار أنشطتهم العملياتية، لاسيما مع إدراك تنظيم داعش للمدى الواسع للتطبيقات التكنولوجية التجارية، فضلا عما تسمح به وسائل التواصل الاجتماعي للجماعة من شن عمليات على نطاق عالمي، كما تمكن الجماعة من إجراء المعاملات المالية وتسهيل الحركات اللوجيستية وتنظيم نفسها بطريقة موزعة عن بعد(٦).

ويمكن القول أن هناك حالة من الصراع على الفضاء الإلكتروني بين داعش وضحاياه لاسيما من الدول التي تتعرض لهجماته الإرهابية، حيث كان التنظيم يطور أنشطته عبر شبكات الإنترنت لجذب متعاطفين وجمع التمويل المالي إلى جانب ترويج آلاف الروايات لخلق انتشار ملحوظ يوحي ببقاء التنظيم على قيد الحياة أمام أنصاره. وفي مقابل ذلك تسعى جهود الدول المختلفة لمكافحة داعش إلى التضييق عليه ومنع فرص انتشاره وتوغله، بيد أنه من الملاحظ أن داعش يبدي قدرا كبيرا من التمكن والقدرة على الاستمرار في هذا السياق ، فنجد أنه في أغسطس ٢٠١٤ تمت إزالة هيكلها الاعلامي بالكامل من على موقع تويتر، وفي فترة وجيزة نقل التنظيم حساباته إلى موقع دياسبورا، وأنشأ التنظيم تواجده أكثر استقراره على موقع التواصل الاجتماعي الروسي "فكونتاكتى"(٧).

ومن الملاحظ فى هذا السياق أن معدلات نشاطات الجماعات الإرهابية على شبكة الانترنت قد تكثفت بشكل ممنهج منذ عام ٢٠١١، وقد أدى هذا التطور إلى ظهور مصطلح " الجهاد الإلكترونى، Cyber Jihad"" الذى أضحى كثيف الاستخدام حاليا(٨).

وفي الفترة بين عامي ٢٠١٥ و ٢٠١٧، وفي أعقاب النكسات العسكرية التي واجهها داعش، بدأ التنظيم يروج لعمليات وهمية عبر الانترنت؛ وتوازي مع ذلك جهود مكافحة دعاية التنظيم لاسيما عبر المنصات الرئيسية ووسائل التواصل الاجتماعي السائدة، إذ انتقل التنظيم لاستغلال مواقع الدارك ويب لموازنة مواجهته عبر مواقع التواصل الرئيسية. وعلى الرغم من الصعوبات المرتبطة بمواقع الدارك ويب أو المنصات الأخرى الأقل شهرة، على سبيل المثال التيليجرام، الذي أصبح ملاذ التنظيم عقب إزالة محتوياته على مواقع أخرى أكثر شهرة وتغلغلا داخل المجتمعات

مثل فيس بوك وتويتر. وبالمثل، يعرض التنظيم مرونة خاصة في الوجود عبر الإنترنت في سعي دؤوب منه للتمكين الإلكتروني؛ حيث ينشر المواد غالبا مع العديد من عناوين URL التي ترتبط بعدد من الأنظمة الأساسية، لتوقع إزالة بعض عناوين URL لضمان بقاء موادها على الإنترنت. ونظرا لزيادة مراقبة شركات الويب، يتم حذف نسبة معينة من هذا المحتوى في غضون بضع ساعات، أو بضعة أيام، أو بضعة أسابيع. نظرا لأن عناوين URL هذه من المتوقع أن يكون لها عمر افتراضي قصير، ولأنها تستخدم بشكل جماعي في أنواع مختلفة من المنصات، فإنها تسمى أحيانا "روابط انغماسية"، في إشارة إلى المقاتلين الانغماسيين. واستمر أعضاء التنظيم بنشر مواد جديدة، وتحميلها المنصات متعددة قبل مشاركة عناوين URL مع أنصارها ومتعاطفيها. يمكن ملاحظة أن منصات مشاركة الملفات الجهادية ومحركات التخزين الافتراضية يتم استغلالها بشكل كبير أكثر من سنوات مضت؛ حيث كانت المنصات الافتراضية مثل Archive وYouTube وDaily motion تستخدم بشكل أكثر شيوعا. يتم الآن مشاركة الوسائط الجهادية على نطاق أوسع من المنصات، بما في ذلك منصات بارزة مثل Amazon Drive، وخدمة Upstream، و Google Photo، إضافة إلى بوابات تخزين أقل رسوخا لا تتطلب أي تسجيل للمستخدم، مثل Gulf upload.لذلك، فإن هذا النوع الأخير من البوابات قابل للاستغلال بشكل خاص لمثل هذه البيانات. وقد واجه التنظيم مواجهات ضد منتدياته وحساباته على مواقع الإنترنت السائدة، ولذا توجه للمواقع الأكثر تحصينا وصعوبة في الملاحقة ليستمر محتواه الافتراضية موجودا على الإنترنت حتى ولو كانت مواقع أقل شهرة مثل الدارك ويب، بجانب تخزين محتوياته على المواقع الأرشيفية(٩).

وقد اخترقت الخلافة الإلكترونية لداعش في عام ٢٠١٥ وسائل التواصل الاجتماعي الخاصة بالقيادة المركزية للولايات المتحدة، وقامت بسرقة بيانات مهمة لعشرات المسئولين العسكريين الأمريكيين. كانت الرسالة التي تركها تنظيم داعش مدوية وواضحة:

"*أيها الجنود الأمريكيون نحن قادمون، انتبهوا لأنفسكم.. داعش*". ثم تبعتها رسالة أخرى: "*بسم الله الرحمن الرحيم، تواصل الخلافة الإلكترونية تحت رعاية تنظيم داعش جهادها الإلكتروني، بينما تقتل الولايات المتحدة وأقمارها الصناعية إخواننا في سوريا والعراق وأفغانستان، اخترقنا شبكاتكم وأجهزتكم الشخصية وعرفنا كل شئ عنكم. لن نرحمكم أيها الكفار. داعش هنا بالفعل، إننا على أجهزة الكمبيوتر الخاصة بكم، وفي كل قاعدة عسكرية. بإذن الله إننا في القيادة المركزية الآن. لن نتوقف! إننا نعرف كل شئ عنكم، وعن زوجاتكم وأطفالكم. أيها الجنود الأمريكيون.. إننا نراقبكم.. إليكم*

جزء من البيانات السرية من أجهزة المحمول الخاصة بكم: لا إله إلا الله محمد رسول الله. لا قانون إلا الشريعة!"(١٠).

على الرغم من حالة الفزع التي أحدثتها هذه الرسالة للشعب والقيادة الأمريكيين، إلا إن بعض الخبراء أمثال جيمس لويس، خبير الأمن الإلكتروني بمركز الدراسات الاستراتيجية والدولية، أوضحوا أنه على الرغم من خطورتها، إلا إنها لا تعكس القدرة الإلكترونية الفعلية للتنظيم الإرهابي، والذي بات يستخدم شبكة الإنترنت لتحقيق أغراض متباينة، تشمل التجنيد والدعاية والتمويل وبث الذعر والخوف في النفوس. كما عبر جون موليجان، نائب مدير المركز الوطني لمكافحة الإرهاب السابق، إنه لا ينبغي للولايات المتحدة أن تستهين بقدرة التنظيمات الإرهابية مثل داعش على شن هجمات إلكترونية ضد الوطن، في أثناء الانشغال بتقليص سيطرتها على الأراضي في العراق وسوريا، حيث تمد هذه التنظيمات جبهات قتالها ضد الولايات المتحدة الأمريكية إلى المجال الإلكترونى كاستخدامها للطائرات بدون طيار (الدرون)، وتسليحها أو استغلالها لوسائل التواصل الاجتماعي(١١).

لقد نجح تنظيم داعش الإرهابي وروع العالم بإنتاجه الإعلامي المتطور للغاية، وتقديمه في وقت حدوث العمل الإرهابي، حيث تم الاستبدال بأشرطة الفيديو منخفضة الجودة والتأثير التي كان ينتجها تنظيم القاعدة لتصوير ساحة المعركة والحوارات monologues المملة الطويلة التي كانت تمتد لساعتين، تم الاستبدال بها اللقطات عالية الوضوح Steadicam مع كتابتها بعناية وتحريرها روائيا، وإرسال الرسائل متعددة اللغات والتي تهدف، في جزء منها، إلى تطرف الشباب المسلمين، وتشجيعهم على الانضمام إلى التنظيم(١٢).

وبتحليل هذه الفيديوهات يمكن تقسيمها إلى نوعين يستهدفان مختلف الجماهير، الأول يتضمن "سلسلة قطع الرأس" (ملفات فيديو تصور قطع رؤوس الصحفيين الغربيين وعمال الإغاثة، جيمس فولي، وستيفن سوتلوف، وديفيد هاينز، وآلان هينينج)، وغيرها من تصوير الفظائع وانتهاكات حقوق الإنسان، مثل صور الجرحى أو قتلى جنود قوات الأمن العراقية، وتدمير الأضرحة الشيعية والصوفية، وإعدام السجناء وأفراد الأقليات الدينية، أما الفئة الثانية فتركز بشكل كبير على صور لبناء الدولة، وتوظف الدعاية التي تبرز أعمال العنف لدعم الأنشطة العسكرية لداعش وتخويف خصومه، كفيديو حرق جثة طيار سلاح الجو الملكي الأردني معاذ يوسف صافي الكساسبة.

ويمكن القول، في هذا السياق، إن تنظيم داعش قد استفاد كثيرا ولا شك من شبكة الإنترنت، على نحو لم يسبق له مثيل مع أي تنظيم إرهابي آخر. فقد ساعدت شبكات

التواصل الاجتماعي، مثل فيسبوك وتويتر وانستجرام ويوتيوب كثيرا في عملية تجنيد أعضاء جدد، وتشجيعهم على السفر والانضمام إلى صفوف أقرانهم من المقاتلين في الميدان من أعضاء التنظيم، أو الارتباط، على جانب آخر، بمجموعة إرهابية للقيام بدور داعم عن بعد.

لقد رصد تنظيم داعش مبالغ كبيرة لتمويل القنوات الفضائية والمحطات الإذاعية والمواقع الرقمية عبر شبكة الإنترنت، فأعلن عن إصدار أول صحيفة باسم دابق Dabiq، وستوديو أجناد، وقناة الفرقان وقناة الاعتصام وقناة الحياة[١٣]. ويعتمد التنظيم على الاستخدام المكثف لهذه القنوات للترويج لأفكاره ولعملياته على الأرض، فأصدر " النشرة الإخبارية للدولة الإسلامية "، وذلك للترويج للخدمات التي يقدمها التنظيم للجمهور في المناطق التي تخضع لسيطرته.

كما يستغل تنظيم داعش هذه الأدوات، كذلك، لتدريب أعضائه عبر مختلف أنحاء العالم على كيفية صناعة المتفجرات والقنابل وكيفية استخدامها، والتنسيق للعمليات الإرهابية وتحديد توقيتها، وللتحفيز من خلال استخدام الأناشيد الحماسية، وللتبشير بانتصارات التنظيم الدائمة وامتداده الحتمي وهزيمة الدول الغربية والعربية التي تكافحه[١٤].

وإضافة إلى ما سبق، فإن تنظيم داعش يستخدم مواقع التواصل الاجتماعي كأداة لتحديد أهدافه والتعرف عليها ومراقبة تحركاتها، خاصة في إطار عمليات الاغتيالات التي تطال بعض رموز الأجهزة الأمنية أو السياسية في الدول المستهدفة، وذلك إما بمراقبة من يمتلك حسابات على تلك المواقع، أو مراقبة دائرة أصدقائهم ومعارفهم للوصول إليهم، وجمع البيانات اللازمة عن تحركاتهم، وتوفير الوقت والجهد اللازمين للقيام بذلك على أرض الواقع، وأيضا ضمان سرية المراقبة[١٥]. وقد عبر موليجان عن حقيقة هذا التميز التقني لداعش، قائلا: "*إن الشئ الفريد في داعش هو حقيقة امتلاكهم فهما عميقا للروابط بين عالم الإعلام، وخاصة وسائل التواصل الاجتماعي، وعالم العمليات.. لقد تمكنوا بنجاح كبير من استخدام الإعلام التعظيم آثار أنشطتهم العملياتية*"[١٦].

يظل تنظيم داعش أكثر التنظيمات الإرهابية نجاحا في التعامل مع واستخدام آليات الإرهاب الالكتروني، حيث يرى كثيرون إن نقطه تفرده الأساسية تتمثل في امتلاكه فهما عميقا للروابط بين عالم الإعلام، وخاصة وسائل التواصل الاجتماعي، وعالم العمليات على أرض الواقع، كما تمكنوا بنجاح كبير من ينقلون المحادثات إلى منصات مراسلة أكثر أمانا. كما إنهم يعملون في بيئات غير منظمة إلى حد كبير، ويقومون

بتطوير أدوات غير منظمة ذات درجات واسعة من الكفاءة والإسهامات، مما يجعل الأمر أكثر صعوبة بالنسبة للحكومات في تحديد التدابير المضادة وتطويرها(١٧).

وتستثمر آلة الدعاية لداعش الجهد والموارد في مختلف وسائل الإعلام. حيث تقوم مؤسسة الحياة -ذراعها الإعلامي الرئيس- بإنتاج الأفلام التي تتراوح بين مقاطع الفيديو مدتها ٣ دقائق تصور علىات قطع رؤوس إلى وثائقيات تزيد مدتها عن ساعة. العديد منها عبارة عن منتجات عالية الجودة تتضمن تقنيات ومؤثرات خاصة على غرار المستخدمة في هوليوود. كما يلاحظ أن التقارير العسكرية والسياسية لداعش وكذلك مجلة دابق التي تعد هي النشرة الإخبارية الرئيسية لداعش والتي تجمع بين الأبعاد السياسية والعسكرية إضافة للتعليقات والتفسيرات الدينية. جميعها يتم ترويجها بشكل أساسي باللغة الإنجليزية بدلا من اللغة العربية. في بعض الأحيان لديهم أيضا ترجمات إلى اللغات الغربية الأخرى، مثل الفرنسية والألمانية والروسية، وحتى الألبانية. والمثل فإن مقاطع فيديو التي يبثها داعش والتي تم إنتاجها باللغة العربية تكون مصحوبة بترجمة باللغة الإنجليزية واضحة ومهنية، وهي ميزة لم يسبق لها مثيل في مقاطع الفيديو التي تم إصدارها رسميا من قبل مجموعات إسلامية أخرى(١٨).

وفي تطور هام، أصدر تنظيم داعش مصطلح " الذئاب المنفردة The Lone Wolves:"، في إشارة للعمليات الإرهابية التي تعتمد على تحريض مجموعة من الأفراد على تنفيذ أعمال إرهابية بصفة منفردة. والذئاب المنفردة التابعة لداعش هم الأشخاص المقيمون في مناطق لا تخضع لسيطرة التنظيم، ويستطيع هؤلاء، بتوجيه من قياداتهم تصنيع قنابل شديدة الانفجار بأدوات بدائية وتنفيذ عمليات إرهابية خطيرة(١٩).

ثانيا: دور الذئاب المنفردة في استراتيجية داعش الإلكترونية:

يقصد بالذئب المنفرد الشخص الذي يرتكب أعمال عنف دعما لجماعة أو حركة أو أيديولوجية ما، ولكنه يفعل ذلك بمفرده خارج أي هيكل قيادة. ومن ثم يعرف إرهاب الذئاب المنفردة بأنه الهجمات الإرهابية التي ينفذها أشخاص يعملون بشكل فردي، ولا ينتمون إلى جماعة أو شبكة إرهابية منظمة، كما تتم تلك العمليات بواسطة هؤلاء الأشخاص دون أي قيادة خارجية مباشرة أو تسلسل هرمي للسلطة. لا يوجد نمط موحد للذئاب المنفردة، وإن كان من الممكن التمييز بين فئاتهم المختلف استنادا إلى خلفياتهم الأيديولوجية أو الدينية(٢٠).

وتشير التقارير الرسمية إلى أن الذئاب المنفردة من منفذي الهجمات الإرهابية يأتون من خلفيات سياسية متنوعة تتنوع ما بين الإسلاميين المتطرفين والإرهابيين البيئيين ونشطاء تحرير الحيوانات والمتظاهرين العنيفين المناهضين للإجهاض والمتطرفين اليمينيين والفوضويين في مجموعة متنوعة من عمليات العنف بلا قيادة، بيد أن التهديد الأكبر في هذا الصدد يأتي من الإسلام الراديكالي لاسيما وأنه يعزز روح التضحية بالنفس (الاستشهاد) التي تعمل كقوة كبيرة مضاعفة للعنف السياسي، وذلك من خلال الاستعانة بشكل انتقائي بأجزاء من القرآن لتبرير العمليات الاستشهادية(٢١).

وفق هذا التعريف فهناك عدد من الذئاب المنفردة من الارهابيين الاسلاميين من أوائلهم وأبرزهم نضال حسن العسكري والطبيب النفسي السابق المدان بقتل ١٣ وجرح ٤٢ شخصا في إطلاق نار جماعي عام ٢٠٠٩ في قاعدة فورت هود العسكرية الأمريكية. وكذلك عبد الحكيم مجاهد محمد الذي فتح النار على مكتب تجنيد عسكري أمريكي في ولاية أركنساس، بالإضافة إلى عدد من الارهابيين المعادين للسامية مثل إيريك رودولف مفجر الحديقة الأولمبية الذي ارتكب سلسلة من التفجيرات في جميع أنحاء جنوب الولايات المتحدة بين عامي ١٩٩٦ و١٩٩٨ التي أودت بحياة شخصين وأصابت ما لا يقل عن ١٥٠ آخرين. رغم وفاته فإن العقيدة الاستراتيجية لمدير مخابرات داعش الأسبق ، أبو محمد العدناني، لا تزال حية من خلال دعواته لجميع عملاء داعش في الغرب لتنفيذ هجمات في الدول التي يعيشون فيها. يرى كثيرون أن رسالة العدناني التي تم بثها في ٢١ مايو ٢٠١٦ لدعوة الذئاب المنفردة لتنفيذ هجمات في أوروبا كانت نقطة تحول، فمنذ ذلك الحين تعمل داعش على إرسال عملاء إلى الغرب والتواصل معهم لإرشادهم(٢٢).

إن أغلب الأشخاص المنفذين لمثل هذه العمليات، يكونوا من الأشخاص الأسوياء الذين لا توجد شكوك حول سلوكهم وحركتهم اليومية. أغلب هذا النوع من الأشخاص يكونوا من الشباب من أصول عربية واسلامية، ومن الذين يقيمون في اوروبا ودول غربية. لتنتقل العمليات الإرهابية من العمليات الواسعة للتنظيم إلى أفراد، هذه العمليات ممكن اعتبارها بأنها محاولة من التنظيم لمواجهة مشكلة التمويل والنقص في القيادات الميدانية من الجيل الأول للقاعدة، الذين تقدم بهم السن وخرجوا من الخدمة. تقوم عمليات الذئب المنفرد عادة على مبدأ التمويل الذاتي المحدود والاستعانة بالمواد التي تدخل في صناعة المتفجرات والتي يمكن الحصول عليها في الاسواق دون أن تجلب الانتباه والمراقبة. أغلبهم لا يتردد إلى المساجد، ولا يرتدي السروال الأفغاني أو يطلق اللحي ويتقن أكثر من لغة مع اجادة علم الانترنت والتقنيات

الحديثة. العديد من "الذئاب المنفردة" يتلقون تشجيعا وتوجيها عبر الإنترنت من التنظيمات الارهابية لتنفيذ هجماتهم عبر توجيه من قبل "مدربين افتراضيين يعملون بصورة مستقلة للتخطيط لهجمات دون إشراف من الجماعات الإرهابية مستخدمين شبكات التواصل الاجتماعي ومواقع الرسائل المشفرة(٢٣).

وبعد سلسلة من الانتكاسات التي خسر خلالها داعش الأراضي في العراق وسوريا منذ أواخر عام ٢٠١٥، صعدت المنظمة من حملتها لنشر العنف خارج نطاق الشرق الأوسط. ومن ثم، حثت وسائل الإعلام الالكترونية التابعة لتنظيم داعش من أسمتهم "الذئاب أو الأسود المنفردة" على قتل أعدائها في بلدانهم الأصلية. وفي صيف عام ٢٠١٦، أصدر تنظيم داعش العدد الأول من مجلة الرمية التي تحث أتباع التنظيم في الغرب على تنفيذ هجمات منفردة ضد الأهداف السهلة، بما في ذلك ركاب المواصلات العامة والشباب الذين يلعبون في المتنزهات والمسنين... وغيرهم؛ ومن ثم فقد نجح التنظيم عبر الاستخدام الماهر والتخطيط الافتراضي في زيادة العنف السياسي في الغرب، كما يتضح من الهجمات الإرهابية في باريس وبروكسل وسان بيرناردينو وأورلاندو(٢٤).

وتعد نتائج تقرير المكتب الأوروبي للشرطة يوروبول حول الواقع الاجتماعي والديموجرافي لهجمات الذئاب المنفردة التي تعرضت لها دول الاتحاد الأوروبي في عام ٢٠١٦ من النقاط اللافتة في هذا السياق، إذ اتضح منها أن ٧٣% من مجموع منفذي هذه العمليات كانوا من مواطني البلد الذي تعرض لهذه العمليات الإرهابية، وتضاف إلى هؤلاء نسبة ١٤% ممن يتمتعون بإقامة دائمة في البلد الذي نفذت فيه العمليات، أو أنهم وفدوا إليه اعتياديا من بلد مجاور. ولم تتجاوز نسبة اللاجئين بين المنفذين ٥%، مع نسبة ٦% منهم تسللوا بشكل غير شرعي إلى البلد المعني(٢٥).

وبطبيعة الحال ساهم التطور التكنولوجي وتنوع منصات التواصل الاجتماعي في زيادة هجمات "الذئاب المنفردة"، إذ تتيح تلك الوسائط إمكانيات التواصل بين أشخاص لم تكن لتتاح لهم فرص التواصل دون هذه المنصات، كما تتيح لهؤلاء الأفراد التعبير عن آرائهم المتطرفة بسهولة إلى أشخاص يشبهونهم من خلال غرف الدردشة والمنتديات. من خلال هذه الاتصالات الافتراضية، يحصل الأفراد على ثقة كافية لتنفيذ أعمال العنف، فضلا عن أن مواقع التواصل الاجتماعي تجتذب أعدادا كبيرة من المستخدمين، ومن ثم فهي تعد وسيلة فعالة للإرهابيين للوصول إلى الجمهور المستهدف، بما في ذلك المؤيدين الذين ليس لديهم أي اتصال بالمنظمات الإرهابية(٢٦).

وهكذا، وحتى أواخر تسعينيات القرن الماضي، كانت شبكة الإنترنت بالنسبة للجهاديين مجرد مكتبة الكترونية مفتوحة، أما الآن ومع التطور المتلاحق لاسيما ظهور وسائل التواصل الاجتماعي وما تحمله من الطاقة التفاعلية، فقد أضحت شبكة الانترنت توفر للجهاديين النواة "الحية" لثقافة الإرهاب، إلى جانب البيئة الاجتماعية اللازمة لإقامة وتوثيق العلاقات بين الجهاديين عبر لغة جذابة، وأخيرا توفر بيئة مرنة تهدف إلى خلق وتعزيز هوية وتجارب الجمهور لأغراض تشغيلية. ومن ثم فقد أضحى للانترنت تأثير قوي على الشباب الذين يحتمل أن يمثلوا الجيل التالي من الذئاب المنفردة "المزروعين" بالفعل في مجتمعاتهم، وهم مقتنعون بروايات جهادية تحفز وتحرض على الهجوم على المدنيين الغربيين الذين يعدون أهدافا سهلة لهؤلاء الجهاديين(٢٧).

ويدلل المراقبون على ذلك بما أثبتته التحقيقيات من تبادل نضال حسن رسائل على الإنترنت مع أنور العولقي رجل الدين الراديكالي المولود في الولايات المتحدة والتابع لتنظيم القاعدة في شبه الجزيرة العربية، بما يعد فاعلا أساسيا في الجهاد المعاصر بسبب قدرته على إلهام وإرشاد مجموعات وأفراد تنظيم القاعدة في الغرب باستخدام وسائل التواصل الاجتماعي. وعلى الرغم من وفاته في هجوم بطائرة بدون طيار في عام ٢٠١١، فقد عمدت الجماعة إلى تخليد ذكراه عبر تطوير وإطلاق تطبيق إلكتروني لنشر الفكر الراديكالي في عام ٢٠١٤ تحت اسم "*جيل العولقى*" ***Generation Awlaki***"(٢٨).

ويمكن القول إن جميع حالات الذئاب المنفردة تقريبا في السنوات الأخيرة شهدت استخدام وسائل الإعلام الاجتماعية الإلكترونية، إذ يوفر الاتصال عبر الإنترنت لهؤلاء الذئاب الترابط الاجتماعي المطلوب، ومجتمع (افتراضي) ومصدرا للإرشاد والدعم الأخلاقي(٢٩).

وتجدر الإشارة إلى وجود عدة مراجعات مفاهيمية لفكرة الذئاب المنفردة ، ومن ثم برزت مفاهيم شبيهة مثل مفهوم "المجاهد المنفرد" ثم مفهوم "الذئب الجهادي" ومن مميزات مفهوم "الذئب الجهادي" كبديل عن الذئب المنفرد هو التخلص من كلمة "منفرد" أخذا بعين الاعتبار سلوك هؤلاء الذئاب الذين يعملون في حزم. مفهوم "الذئب المنفرد" يمكنه فقط توصيف بعض حالات الجيل الأقدم والأضعف من هؤلاء الإرهابيين. في حين إن الذئب الجهادي ليس ضعيفا ولا منعزلا؛ فهو متصل بالإنترنت طول الوقت ومن ثم فهو على علاقة دائمة بالمناخ الجهادي العالمي(٣٠).

في السياق ذاته رأي عدد من المتخصصين أنه وبعد عملية برشلونة التي أسفرت عن قتل ١٤ شخصا وإصابة أكثر من ١٢٠ آخرين، فقد أصبح مفهوم الذئاب المنفردة

مضللا، ومن ثم فمن الأفضل استخدام تعبير "الذئاب التي تعمل في حزم". حيث تشير التقارير إلى أنه منذ تلك العملية تعتمد استخبارات داعش في دعمها لهجمات الارهاب الالكتروني على القيام بخطوتين أساسيتين(٣١):

١. الخطوة الأولى إرسال المقاتلين الأجانب غير المعروفين إلى وكالات الاستخبارات إلى إحدى المنتجعات التركية المتوسطية لمدد تتراوح بين أسبوع إلى شهر واحد، حيث يظلون في تلك المنتجعات بضعة أيام فقط في فنادقهم ويحرصون على توثيق وجودهم بنشر الكثير من الصور لإثبات أنهم كانوا يقضون إجازاتهم في تركيا (إذا تم استجوابهم في وقت لاحق من قبل ضباط مكافحة الإرهاب في بلادهم)، بيد أنهم يتسللون من تركيا إلى سوريا لتلقي تدريبات عسكرية سريعة. بهذه الطريقة ، تمكنت داعش من تدريب العشرات من المقاتلين الأجانب بسرعة وإعادتهم إلى أوروبا.

٢. الخطوة الثانية، تطلب داعش بموجبها من المقاتلين الأجانب الموثوقين لديها التواصل مع أصدقائهم المقربين وأقاربهم في الغرب لتجنيدهم للهجوم. تحث داعش جهادييها على تجنيد الأصدقاء والعائلة لأن ذلك أسهل وأسرع وأكثر أمنا. وجدير بالذكر أن عملية برشلونة نفذتها مجموعة من الإرهابيين تربطهم علاقات قرابة وصداقة، وهو ما مكنهم من العمل سويا في سرية لمدة تزيد عن عام معتمدين على كتب توزع إلكترونيا لإرشادهم وتدريبهم(٣٢).

كما ظهر مفهوم "الإرهاب الموجه عن بعد" ويقصد به تلك الهجمات التي لم يسبق لمنفذيها أن سافروا إلى مناطق الصراعات، أو انضموا إلى تنظيم إرهابي، ولكنهم مع ذلك، كانوا على تواصل دائم مع عناصر الجماعات الإرهابية من خلال استخدام منصات وسائل الاتصال المشفرة، وذلك لتوفير الدعم والنصيحة للمهاجم في كل مرحلة من مراحل الإعداد، كما أنه لوحظ أنه في بعض يتم توفير الدعم المالي للقيام بعملية إرهابية، بل وفي انتقاء المناطق التي سيتم استهدافها. وفي ضوء التعريف السابق، يمكن القول إن الإرهاب الموجه عن بعد هو شكل هجين لنمطين سابقين من الإرهاب في الدول الغربية. وهما الإرهاب الشبكى وإرهاب الذئاب المنفردة. فهى تتشابه مع الأشكال الشبكية من الإرهاب فى وجود بعض الصلات بين منفذى الهجوم الإرهابي والتنظيم الإرهابي، غير أنه يختلف عنها فى محور واحد، وهو أن المنصات ليست تنظيمية، بل افتراضية، أى أن العنصر الإرهابي تم توجيهه من خلال الفضاء الإلكترونى. وبالمثل، فإن الإرهاب الموجه عن بعد يتشابه مع إرهاب الذئاب المنفردة في بعد وحيد، وهى أن أغلب الهجمات يقوم بها فرد واحد. غير أنه بخلاف إرهاب الفرد الواحد، فإنه يوجد اتصال مع جماعة إرهابية قائمة، وإن كان عبر الفضاء

الالكترونى، كما أن الجماعة الإرهابية تساعد منفذ الهجوم بداية من تجنيده، وانتهاء بتنفيذ هجمته(٣٣).

ويلاحظ في هذا الشأن، إن أسلوب تنظيم داعش لم يختلف كثيرا عن أسلوب تنظيم القاعدة، من حيث الاعتماد على الإرهاب المطلق، ففي تسجيل صوتي للناطق باسم التنظيم " أبو محمد العدناني" عام ٢٠١٤، دعا العدناني المتعاطفين مع التنظيم إلى قتل رعايا دول الائتلاف في أي مكان وبأي وسيلة متاحة، وهو أمر يمكن تنفيذه دون الرجوع إلى القيادة، بل ودون أن يكون هناك علاقة تنظيمية أصلا بين منفذ العمل الإرهابي والتنظيم(٣٤).

ومما هو جدير بالذكر، في هذا الخصوص، أن تنظيم داعش قد تحول إلى هذه استراتيجية اللامركزية، وقوامها الإرهاب من خلال الذئاب المنفردة، بعد أن انحسرت انتصاراته في المناطق الخاضعة لسيطرته، كمدينة الرقة السورية ومدينة سرت الليبية، ومدينتي الفوجة والموصل العراقيتين، وذلك في ظل إحكام جهود مكافحته ملاحقة قياداته وأتباعه وتقديمهم للمساءلة. ويعكس خطاب العدناني المعنون "ليحيي من حي عن بينة" عام ٢٠١٦ بوضوح على التحول نحو هذه الاستراتيجية الجديدة، وعلى الخطر المحدق الذي بات يشعر به قادة التنظيم، حيث حمل الخطاب شعورا بوطأة الخسائر التي تعرض لها التنظيم في ظل جهود مكافحته عالمية، وبدا وكأنه يهيئ أتباعه لتقبل ما هو أكثر وطأة، وحثهم على تنفيذ المزيد من الهجمات ضد المصالح الغربية في كل مكان(٣٥).

وعلاوة على ذلك، يشير الخبراء إلى أن قلق الولايات المتحدة لا يقف عند مستوى ظاهرة الذئاب المنفردة وحسب، بل يمتد كذلك ليشمل الأفراد المؤهلين في المجال الإلكترونى، الذين قد يعملون خلف الأفق، ويضطلعون بمهام دعم رسمية، وشبكات المؤيدين التي تعيد نشر تغريدات داعش الدعائية وهؤلاء الذين يضيفون قيمة الإجمالي الجهود ولكن يصعب اكتشافهم. وبحسب الرئيس الأمريكي السابق باراك أوباما، فإنه: "*في عالم اليوم، قد تأتي الأعمال الإرهابية ليس فقط من بضعة متطرفين يرتدون سترات انتحارية وإنما من بضع نقرات على مفاتيح جهاز الكمبيوتر – إنه سلاح التخريب الشامل. وتبدو هذه الأسلحة كحلقة جديدة من التهديد الإرهابي في العالم*". ويشير هذا المصطلح، بشكل عام، إلى الهجوم الذي يستخدم الوسائل الإلكترونية (مثل دودة الحاسب، الفيروس، والبرمجيات الخبيثة) لاختراق البنية التحتية الحيوية والتدخل الخطير فيها. والبنية التحتية الحيوية تعني المرافق والخدمات والشبكات، التي قد تتسبب في مخاطر جسيمة على الصحة العامة والاقتصاد

والبيئة والأمن القومي، إذا ما ظلت دون اتصال بشبكة الانترنت لفترة طويلة. وفي الوقت الذي قد تنجح فيه استراتيجية الردع الأميريكة في بعض الحالات، كانت قدرة الهاكرز على بيع البرمجيات الخبيثة هو ما فشلت في منعه استراتيجية الإدارة الأمريكية بالتعاون مع شركائها كالصين وروسيا للقضاء على قدرات داعش الإلكترونية وتحجيمها(٣٦) .

ثالثا: الاستراتيجية الأمريكية لمواجهة إرهاب داعش الالكتروني:

لقد سعت وزارة الدفاع الأمريكية إلى دمج العمليات الإلكترونية مع قدراتها العسكرية التقليدية والتخطيط الاستراتيجي للعمليات العسكرية، وكانت لديها فرق إلكترونية متكاملة ذات قيادة إقليمية، منتشرة خارج وداخل الولايات المتحدة. وقد ألقت الحرب على تنظيم داعش الضوء على ضغط البنتاجون من أجل إعداد قواته لما يسمى "العمليات متعددة المجالات"، ومنحت عملية "العزم الصلب" لعام ٢٠١٧، المخططين الفرصة لاختبار واستعراض بعض من قدرات الولايات المتحدة الإلكترونية الهجومية فى أثناء الإعداد لمعارك مستقبلية.

ووفقا للجنرال جوزيف فوتيل، قائد القيادة المركزية الأمريكية آنذاك، "*تاريخيا كانت العمليات الإلكترونية ترفع للمسئولين رفيعى المستوى وتنفذ بشكل مستقل، ومع التطور الذى حدث فى المجال، بدأ الجيش الأمريكى في دمج العمليات الإلكترونية فى كل مراحل التخطيط*". وبالرغم من ذلك يعترف الجنرال ستيفن تاونسند بأنه مازال هناك تحديات : "*الخلاصة هى أن الأمر قد استغرق أسبوعين من أجل تنظيم هذه العملية المتطورة الصغيرة متعددة المجالات، والتى استمرت أقل من أسبوع واحد، وكانت ضد عدو لا يمكنه حقا أن ينافسنا فى أى من تلك المجالات*"(٣٧).

تجدر الإشارة، ابتداء، إلى أن جهود الولايات المتحدة الأمريكية في مجال مكافحة الإرهاب الإلكتروني قد تضاعفت منذ أحداث الحادي عشر من سبتمبر، حيث تم اعتماد قانون باتريوت USA Patriot Act العام ٢٠٠١، في أعقاب هذه الأحداث مباشرة، وكان هناك اهتمام واضح من بين نصوصه بقضايا الأمن الإلكترونى.

وقد وسع القانون المذكور من سلطات الحكومة الفيدرالية في مجال مكافحة الإرهاب، وبصفة خاصة، المراقبة الإلكترونية للاتصالات واعتراضها لتيسير القبض على الإرهابيين، كما يحتوي القانون، أيضا، على أحكام خاصة بتوثيق المعاملات المالية بغرض مكافحة غسيل الأموال، وذلك لعرقلة تمويل الإرهاب(٣٨).

وأقرت الولايات المتحدة الأمريكية بعد اعتداءات ١١ سبتمبر ٢٠٠١ قانون يرخص للهيئات التنفيذية المتمثلة بأجهزة الشرطة ومكتب التحقيقات الفيدرالي صلاحيات

واسعة في مجال مراقبة المشتبه فيهم وتفتيشهم دون أن يكون لديهم أدلة ملموسة تدينهم بشكل مباشر ودون فرض رقابة كافية علي تلك الصلاحيات، فقط بإعطاء القضاء الأمريكي صلاحية مراقبة عمل أجهزة الشرطة، مع عدم تبني مزيد من التدابير التي تدعم هذه الصلاحية، مثل إنشاء وكالة مستقلة للحريات المدنية تعمل علي مراقبة الاشخاص المشتبه فيهم. وكان موقف الجمهوريين مؤيدا لتوسيع العمل بقانون باتريوت وإقرار عقوبة الإعدام في جرائم مثل تمويل الإرهاب وبعض الجرائم المرتبطة بالإرهاب، إلا أن الحزب الديمقراطي، سعي لوقف العمل ببعض مواد القانون التي تمثل تهديدا لخصوصية الأفراد وهي التي تتعلق بالتوسع في سلطات التفتيش ومصادرة الوثائق الخاصة والتنبؤ بالوصول إلى مرحلة إساءة استخدام هذا القانون(٣٩).

لكن بعد أحداث الحادي عشر من سبتمبر٢٠٠١ شهدت الساحة الأمريكية زخما غير مسبوقا من التشريعات الأمريكية لمواجهة الجريمة الإرهابية، وأهم ما يميز المجابهة التشريعية الأمريكية للإرهاب، عدم اقتصارها على صعيد واحد أو أصعدة محدودة، ولكن يمكن وصف تشريعات المواجهة ب "المتعددة الحقول والأصعدة"، وكان من أهم الأصعدة التي واجهتها التشريعات الأمريكية، ما يلي(٤٠):

١. تعزيز القدرة على تدقيق والتحقق من اللاجئين والمهاجرين، والزائرين الأجانب، وذلك من أجل التمكن من عدم تشكيلهم خطرا على الأمن القومي أو السلامة العامة، ووضع إجراءات أمنية عالية للعمل على ضمان بقاء الأفراد الخطرين خارج حدود الولايات المتحدة، إلى جانب تعزيز القدرة على جمع المعلومات والتحليل لتحديد هؤلاء الذين تمكنوا بالفعل من دخول الأراضى الأمريكية.

٢. تفعيل قوانين الهجرة؛ سواء على الحدود أو في الداخل وذلك للعمل على تحقيق ردع فعال ضد الهجرة غير الشرعية وتعظيم الجهود لتحديد واحتواء الاحتيال في عملية الهجرة، في إطار تكامل الأطر المنظمة للهجرة.

٣. دعم أمن وسائل النقل والاتصال؛ من خلال العمل على تحسين القدرة على جمع المعلومات وتشاركها بين أجهزة الحكومة الأمريكية، ومع الشركاء الأجانب لتعزيز الأمن في الطرق العامة والتي هي القناة الأساسية لعبور الأفراد والبضائع، وأن يتم العمل على الاستثمار في التكنولوجيا لاحتواء الأخطار الصاعدة في الملاحة الجوية والطائرات والطرق وقطاعات المواصلات البحرية.

٤. تعزيز الأمن الإلكترونى؛ من خلال الاستفادة من المجتمع المفتوح والتقدم في تشفير الاتصالات والإنترنت بهدف مواجهة استخدام الإرهابيين للإنترنت في التجنيد

والتعبئة والتمويل للقيام بعملياتها الإرهابية داخل الولايات المتحدة، ومحاربة داعش والجماعات الإرهابية حتى بعد هزيمتهم الميدانية في سوريا والعراق.

٥. تعطيل مؤامرات الإرهاب؛ عبر دعم الجهود الاستخباراتية وتشاركها محليا وبالتعاون مع الشركاء الأجانب للعمل على تعزيز الجبهة الداخلية بما فيها الأمن الداخلي وتعزيز القانون للعمل على وقف وإبطال الأنشطة الإرهابية قبل حدوثها.

٦. استئصال المناطق الآمنة للإرهابيين؛ وذلك من قبيل أن الوقت والأرض يسمحان للحركات الجهادية للتآمر، واتخاذ إجراءات مباشرة ضد خطابهم الديني، والعمل على منع ظهورهم مرة أخرى، والعمل على تعقبهم في شبكاتهم الرقمية والعمل مع الشركات الخاصة لمواجهة تحديات الإرهابيين والمجرمين.

٧. قطع مصادر القوة للجماعات الإرهابية؛ من خلال العمل على تعطيل موارد الدعم المالي لها، والعمل على وقف تمويلهم وحماية الولايات المتحدة ونظامها المالي الدولي من الخطر، وإصابة قدرتهم على تجنيد الشباب، ومكافحة أيديولوجية الشر التي تقودها الجماعات الجهادية ومواجهة خطاباتهم المتطرفة.

٨. تشارك المسئولية مع الحلفاء والشركاء، الذين هم عرضة أيضا لاستهداف الجماعات الإرهابية، والاستمرار في المشاركة في مقاومة هذه الجماعات، ومساعدة الحلفاء على تطوير وتوسيع المسئولية لتعزيز قدرتهم في مواجهة تلك الجماعات[٤١].

وفيما يتصل بالإرهاب الإلكتروني، يلاحظ، أن قانون باتريوت قد وضع الإرهاب وجرائم الكمبيوتر على قائمة الأفعال المجرمة به. وإضافة، تمت الدعوة، أيضا، إلى تطوير الاستخبارات الإلكترونية لتحسين قدرة الحكومة الفيدرالية على التنبؤ بالتهديدات المتعلقة بالكمبيوتر وقدرات ردعها[٤٢].

كذلك، اعتمد الكونجرس الأمريكي لاحقا، وتحديدا عام ٢٠١٢، قانون الأمن الإلكتروني Cyber Security Act، لحماية البنية التحتية الحيوية مثل شركات الطاقة والهواتف، ومحطات معالجة المياه، ومقدمي الخدمات اللاسلكية. ويهدف هذا القانون إلى حماية البلاد من الهجمات الإلكترونية على نحو مسئول وسريع من خلال إطار يشجع على تبادل المعلومات بين القطاع الخاص والحكومة بشأن تهديدات الكمبيوتر. وبموجب هذا القانون يمكن مشاركة المعلومات حول التهديد الموجود على النظام بهدف منع الهجمات أو الحد من المخاطر التي قد تؤثر على الشركات أو الوكالات أو المستخدمين الآخرين، وذلك عبر وسائل مختلفة كجمع المعلومات والفحوص الأمنية والتدابير الوقائية الأخرى، وتنسيق الأعمال الاستخبارية والدفاعية[٤٣].

كما حدد التقرير الرئاسي الأمريكي بخصوص حماية البنية التحتية الحساسة PCCIP لعام ١٩٩٧، خمسة قطاعات رئيسية قد تكون عرضة للهجمات الإرهابية إلكترونيا في المستقبل، هي[٤٤]:

١. قطاع الاتصالات والمعلومات، ويشمل شبكات الاتصالات العامة والإنترنت والحاسبات في المنزل، وفي الاستخدامات الأكاديمية والتجارية والحكومية.

٢. قطاع الطرق وشبكات المواصلات، ويشمل الطرق السريعة للمواصلات وخطوط السكك الحديدية والموانئ، والمطارات وشركات النقل وخدمات الشحن التي تستعمل لنقل الأفراد والبضائع.

٣. قطاع الطاقة، ويشمل الصناعات التي تنتج الطاقة وتوزع الطاقة الكهربائية والبترول والغاز الطبيعي.

٤. قطاع المال والبنوك، ويشمل البنوك والخدمات المالية غير المصرفية ونظم الرواتب وشركات الاستثمار والقروض المتبادلة والبورصة.

٥. قطاع الخدمات الإنسانية، ويشمل نظم التزويد بالمياه وخدمات الطوارئ والخدمات الحكومية (البطالة والضمان الاجتماعي وتعويض الإعاقات وإدارة سجلات المواليد والوفيات، ...).

كما أشار المشاركون في استقصاء مؤتمر RSA 2016 للإرهاب الإلكتروني، أن نحو ٤٩% من شركات القطاع الخاص الأمريكية قد تكون عرضة لهجمات إلكترونية إرهابية حتى العام ٢٠١٨[٤٥].

ووفقًا لوكالة مشروعات البحوث الدفاعية المتقدمة DARPA، فإن هناك ٥ أنواع للتهديدات الخارجية التي قد تتعرض لها البنى التحتية المعلوماتية، وهي[٤٦]:

١) تهديدات خارجية محايدة (مثل: التنصت، وتحليل الإشارات، وغيرهما).
٢) تهديدات خارجية نشطة (مثل: الدخول، والحمولة الزائدة، والازدحام).
٣) الهجوم على نظام عامل.
٤) الهجوم الداخلي.
٥) الهجمات للوصول إلى تعديل النظام، من خلال خرق نظم الحماية للدخول غير المشروع إلى النظام والانكشاف.

وإضافة إلى ما تقدم، بدأت الولايات المتحدة مؤخرا في بناء ترسانة عسكرية لمواجهة الإرهاب الإلكتروني، وذلك من خلال منح الجيش الأمريكي المزيد من السلطات والموارد في مجال محاربة هذا الإرهاب. يعد هذا النقل للسلطة من السلطة التنفيذية المدنية التي كانت تتصدى للإرهاب الإلكتروني بمفردها إلى الجيش دليلا قويا على أن حكومة الولايات المتحدة تخشى من استخدام الغزو الإلكترونى كأحد أعمال الحرب ضدها. وتحتل البحرية الأمريكية، في هذا الشأن، مركز الصدارة في مواجهة الهجمات الإرهابية الإلكترونية، ولا سيما أسطول القيادة الإلكترونية للولايات المتحدة/

الأسطول العاشر Cyber Command U.S 10th Fleet ، وتسعى البحرية الأمريكية لتحقيق خمسة أهداف رئيسية في سبيل مواجهة الإرهاب الإلكتروني، وهي: " تشغيل شبكة الانترنت وكأنها ساحة للقتال، عمل إشارات استخباراتية خاصة، منع تأثيرات الحرب عبر الفضاء الإلكتروني، خلق وعي مشترك لدى الشعب الأمريكي بخطورة التهديدات الإلكترونية، وتأسيس وتطوير قوة المهام الإلكترونية التابعة للبحرية". تعمل تلك الأهداف الخمسة كأساس للمعركة ضد الهجمات الإلكترونية والإرهاب الإلكتروني(٤٧).

ويبين مما تقدم، إن قانون باتريوت وغيره من القوانين والتدابير الأخرى التي اتخذتها الحكومة الأمريكية توضح التزامها بمكافحة كافة صور الإرهاب الحديثة، بما في ذلك الإرهاب الإلكتروني.

ووفقا للجنرال ستيفن تاونسند، القائد السابق للتحالف الدولي ضد تنظيم داعش، إن القيادة الإلكترونية للولايات المتحدة، القوة الرائدة للحرب الإلكترونية، شاركت سرا في شن سلسلة من الهجمات الإلكترونية ضد الجماعة الإرهابية عام ٢٠١٧، تحت قيادة قوة المهام المشتركة (Joint Task Force– Ares) (٤٨)، والتي قضت على أنظمة الكمبيوتر الخاصة بالتنظيم في العراق. ويذكر، أن هذه الهجمات كانت جزءا من عملية متعددة المجالات انطلقت في الجو والأرض والبحر والفضاء والفضاء السيبراني. وبحسب تاونسند، كانت هذه الهجمات سببا رئيسيا في ترك أفراد التنظيم لمواقعهم القيادية الثقيلة، مما جعلهم عرضة للهجوم بالأسلحة الحركية مثل الضربات الصاروخية(٤٩).

ومما هو جدير بالذكر، في هذا الخصوص، أن الإدارة الأمريكية السابقة للرئيس أوباما قد جعلت الأمن الإلكترونى "لحماية البنية التحتية الحيوية" على رأس أولوياتها، فأسست المركز الوطني لحماية البنية التحتية (National Infrastructure Planning Center) في مكتب التحقيقات الفيدرالي ومكتب ضمان البنية التحتية الحيوية (Critical Infrastructure Assurance Office) في وزارة التجارة الأمريكية، ومراكز تحليل وتبادل المعلومات (Information Sharing and Analysis Centers) في الصناعات الحيوية مثل الطاقة والصناعات المصرفية. بل إن الإدارة الديمقراطية قد ذهبت إلى ما هو أبعد من ذلك، حيث جعلت الأمن الإلكترونى جزءا أساسيا من وزارة الأمن الداخلي الجديدة. ووصف الخبراء بالخطوات الإيجابية لمكافحة القدرات الإلكترونية لتنظيم داعش، ولكن يتعين عدم الاكتفاء بها، بل إن هناك دائمة حاجة للمزيد(٥٠).

ملاحظات ختامية:

يرتبط الإرهاب عموما بالاستخدام غير المشروع للقوة بغرض تحقيق أهدافت بعينها، ومن ثم كان من الطبيعى أن يرتبط الإرهاب بظهور التطورات التكنولوجية وثورة الاتصالات والتى سمحت بظهور نمط جديد من القوة هي القوة الالكترونية، والتى تعني بشكل أساسى امتلاك الفاعلين المعنيين القدرة على تحقيق النتائج التى يهدفون إليها من خلال استخدام المعلومات وأدوات الاتصال فى العالم الافتراضى. وهذا النوع من القوة وبالرغم من أنه مازال غير محدد الملامح والأبعاد، لكنه بالقطع نمط موجود وتستخدمه القوة الإرهابية لتحقيق أهدافها، وهناك المئات، وربما الآلاف من المواقع التي تحتفظ بها الجماعات الإرهابية وأنصارهم تلعب دورا أساسيا في خلق حضور عالمي(٥١)، ويتزايد اعتمادها عليه مع الوقت، ويصبح أكثر تعقيدا لمواجهته والتصدى له.

وتستثمر آلة الدعاية لداعش الجهد والموارد فى مختلف وسائل الإعلام. حيث تقوم مؤسسة الحياة- ذراعها الإعلامى الرئيس- بإنتاج الإفلام التى تتراوح بين مقاطع فيديو مدتها ٣ دقائق تصور عمليات قطع الرأس إلى وثائقيات تزيد مدتها عن ساعة، لعدي منها عبارة عن منتجات عالية الجودة تتضمن تقنيات ومؤثرات خاصة كالمستخدم فى عالم السينما فى هوليوود. كما يلاحظ أن التقارير العسكرية والسياسية لداعش وكذلك مجلة دابق، التى تعد النشرة الإخبارية الرئيسية التى تجمع بين الأبعاد السياسية والعسكرية والدينية، جميعها يتم ترويجها باللغة الإنجليزية بشكل أساسى بدلا من اللغة العربية، وفى بعض الأحيان لديهم أيضا ترجمات إلى اللغات الأخرى، مثل الفرنسية والألمانية والروسية وحتى الألبانية. والمثل فإن مقاطع الفيديو المنتجة بالعربية التى تبثها داعش تكون مصحوبة بترجمة باللغة الإنجليزية واضحة ومهنية، وهي ميزة لم يسبق لها مثيل فى مقاطع الفيديو التى يتم إصدارها رسميا من قبل مجموعات إسلامية أخرى (٥٢).

وعن استراتيجية الولايات المتحدة الإلكترونية، فعندما كلف اشتون كارتر، وزير الدفاع الأمريكى السابق، القيادة الإلكترونية للولايات المتحدة بتوجيه قدراتها ضد تنظيم داعش، تم وصف ذلك بأنه أول اختبار حقيقى للقيادة الحديثة، وحينها أوضح الجنرال تيموثى هيو مدير الاستخبارات فى القيادة الإلكترونية الأمريكية، أنه وقتها فقط تعلم رؤساء القيادة الإلكترونية كيفية توظيف القدرات الإلكترونية على أفضل وجه، وذلك فى جلسة نقاش بمؤتمر CyberCon الذى استضافته مجلة Federal Times فى مقاطعة أرلينجتون فى ولاية فيرجينيا فى ٢٨ نوفمبر ٢٠١٧ (٥٣).

ووفقا لتيموثى هيو: "*كان من أهم تلك الدروس كيفية التعامل مع المشكلات الاستخباراتية، كيفية التعامل مع تبادل المعلومات الاستخباراتية، فهم ساحة المعركة وأيضا ضمان سلامة الإجراءات التقليدية مثل عمليات الاستهداف، وقابليتها للاندماج والتكرار فى المجال الإلكترونى*"(٥٤).

ويحرص الكثير من القادة العسكريين للولايات المتحدة على التأكيد على أن العمليات الإلكترونية لا تحدث فى الفراغ وينبغى أن تدعم مهام ومجالات الحرب الأخرى. بحيث يكون المجال الإلكترونى جزءا من خطة شاملة للمجالات القتالية الأساسية،

هوامش الدراسة

(1) Sofia Karadima, "New Trends In Terrorism: The Use Of Social Media, Cyber-Terrorism, The Role Of Open Source Intelligence And The Cases Of rightwing Extremism And Lone Wolf Terrorism", Master Thesis, University of Piraeus, Department of International and European Studies, 2016, p.55. http://dione.lib.unipi.gr/xmlui/handle/unipi/9315.

(٢) ريهام العباسي، "أثر الارهاب الالكتروني على تغير مفهوم القوة في العلاقات الدولية دراسة حالة: تنظيم الدولة الإسلامية"، المرطز الديمقراطى العربي، ٢٤ يوليو ٢٠١٦، http://democraticac.de/?p==34528

(٣) محمود رشدي، "الاتجاهات السيبرانية للمحتوي الإرهابي.. "داعش" نموذجا"، مركز سمت للدراسات، ٢١ ديسمبر ٢٠١٨، http://smtcenter.net

(٤) جهاد فتحى ، كيف استخدمت التنظيمات الإرهابية التكنولوجيا في صناعة الإرهاب، مركز البديل للتخطيط والدراسات الاستراتيجية، ١٧ يناير ٢٠١٧.

(٥) رايات السواد: كتاب يقرأ الجوانب غير التقليدية لإرهاب "داعش"، مركز سمت للدراسات، ٢ أكتوبر ٢٠١٨.

(6) Mark Pomerleau, How ISIS harnesses commercial tech to run its global terrorist network, C4ISRNET, August 15, 2017. At: https://www.c4isrnet.com/show-reporter/dodiis/2017/08/15/how-isis-harnesses-commercial-tech-to-run-its-global-terrorist-network /

(٧) ريهام العباسي، م س ذ.

(8) Sofia Karadima, New Trends in Terrorism: The Use of Social Media, Cyber Terrorism, The Role of Open Source Intelligence and the cases of Rightwing Extremism and Lone Wolf Terrorism, op.cit., p. 55.

(٩) محمود رشدي، م س ذ.

(10) Agnese Carlini, A new threat in cyber dimension: ISIS and the Cybercaliphate, Mediterranean Affairs, May 26, 2015. At: http://mediterraneanaffairs.com/a-new-threat-in-cyber-dimension-isis-and-the cybercaliphate

(11) Kimberly Underwood, ISIS takes fight to cyber battlefield: The Cyber edge, November 1, 2017. Available at: https://www.afcea.org/content/isis-takes-fight-cyber-battlefield

(12) John Muller, The Cybercoaching of Terrorists: Cause for Alarm?, CTCSentinel, Combating Terrorism Center, Volume 10, Issue 9, October 2017.pp.29-30. At: http://ctc.usma.edu/the-cybercoaching -of-terrorists-cause-for-alarm/

(١٣) مجلة دابق (بالإنجليزية dabiq)، تصدر شهريا وتعتبر المجلة الرسمية لتنظيم الدولة الإسلامية. صدر العدد الأول في رمضان ١٤٣٥ ه الموافق يوليو ٢٠١٤م، وتصدر باللغتين العربية والإنجليزية، واسمها مستوحى من قرية دابق السورية حيث وقعت معركة مرج دابق الشهيرة بين العثمانيين والمماليك. كان «عودة الخلافة» عنوان العدد الأول من المجلة.

(14) John Mueller, Op. cit., pp. 30-32.

(١٥) المزيد من التفاصيل حول استخدامات داعش المواقع التواصل الاجتماعي المختلفة، انظر على سبيل المثال: د. محمد قيراط، الإعلام الجديد والإرهاب الإلكتروني: آليات الاستخدام وتحديات المواجهة، مجلة الحكمة للدراسات الاتصالية والإعلامية، العدد التاسع، يناير ٢٠١٧، ص ص ٢٤-٢٧، متاح على الرابط:

https://www.researchgate.net/profile/Mohamed Kirat/publication/٣١٢٣٧٦٩٥٦.

(16) Mark Pomerleau, op.cit.

(17) Ibid.

(18)Joanie Chung Yin Yeung, "A Critical Analysis on ISIS Propaganda and Social Media Strategies", University of Salford, Terrorism & Security Studies Dep., March 2015. At: https://www.researchgate.net/ publication/316146537.

(19) Returning ISIS Fighters: Where Are They?. Clarion Project, An info graphic detailing the countries where ISIS fighters have returned and their numbers, October 26, 2017. At: https://clarionproject.org/isis-fighters-returned /

(20) Gabriel Weimann, "Lone Wolves in Cyberspace", Journal of Terrorism Research, Volume 3, Issue 2. Autumn 2012. At: https://www.files.ethz.ch/isn/164616/468-956-1-SM%20Full.pdf

(21) George Michael, "Disturbing Trends in Lone Wolf Terrorism: The Convergence of Mental Illness, Marginality, and Cyber Radicalism", SKEPTIC MAGAZINE, volume 22, no. 1, 2017, pp. 15-19.

(22) Ahmet S. Yayla,"How to Counter ISIS Wolf- packs", Modern Diplomacy, August 25, 2017. At:https://moderndiplomacy.eu/2017/08/25/how-to-counter-isis-wolf-backs

(٢٣) "الذئاب المنفردة لا تزال الاستراتيجية المفضلة لدى تنظيم داعش"، المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات، ١٧-١٢-٢٠١٨،

http//:www.europarabct.com?/p=34896

(24) George Michael, op.cit., pp. 15-19.

(٢٥) الذئاب المنفردة لا تزال الاستراتيجية المفضلة لدى تنظيم داعش"، م س ذ.

(26) Gabriel Weimann, op.cit.

(27) Arije Antinori, The "Jihadi Wolf Threat: The Evolution Of Terror Narratives Between The (Cyber-) Social Ecosystem And Self-Radicalization "Ego-System", Paper Presented At The 1st European Counter Terrorism

Centre (ECTC) Conference On Online Terrorist Propaganda, The Hague. 10-11 April 2017.At:https://www.linkedin.com/pulse/jihadi-wolf-threat-evolution-terror- narratives-pdf-antinori-phd

(28) Ibid.

(29) Gabriel Weimann, "Lone Wolves in Cyberspace", op.cit

(30) Arije Antinori, Op.Cit.

(31) Ahmet S. Yayla, Op.Cit.

(32) Ibid.

(٣٣) د. شادى عبد السلام، الإرهاب عن بعد: نمط تنظيمى جديد لاستهداف الدول الغربية والآسيوية، مجلة اتجاهات الأحداث، العدد ٢٤، نوفمبر- ديسمبر ٢٠١٧، ص ص ٥٠-٥٣.

(٣٤) فالح فليحان فالح الرويلي، استراتيجيات التنظيمات المتطرفة في التجنيد عبر الإنترنت: داعش نموذجة، الرياض: جامعة نايف العربية للعلوم الأمنية، ٢٠١٨، ص ص ٨ - ١٠، متاح على الرابط: https://repository.nauss.edu.sa/bitstream/handke/123456789/65979

(٣٥) محمود البازي، الذئاب المنفردة: الملاذ الأخير لداعش، مجلة المستقبل العربي، العدد ٤٥٦، متاح على رابط مركز دراسات الوحدة العربية :https://caus.org.lb/ar

(36) Charlotte Mellgard, "The Silent war of Cyber-Terrorism", VANDERBILT Political Review, November 10, 2015. At: http://vanderbiltpoliticalreview.com/the-silent-war-of-cyber-terrorism/

(37) Ryan Duffy, The U.S. military combined cyber and kinetic operations to hunt down ISIS last year, general says, Cyberscoop, MAY 29, 2018. At: https://www.cyberscoop.com/u-s-official-reveals-military-combined-cyber-kinetic-operations-hunt-isis/

(38)Fawzia Cassim, Addressing the spectre of cyber terrorism,: A comparative perspective, Potchefstroom Electronic Law Journal, Vol. 15, Nov.2, 2012. Available at: http:www.ajol.info/index.php/pelj/article/viewfile/81295/71495, p. 389.

(٣٩) ذكرت الواشنطن بوست الأمريكية يوم ٢٨ أكتوبر ٢٠٠١ أن وكالة ال CIA تنظر في أمر اغتيالات فردية حول العالم ضمن تفويض رسمي من الرئيس بوش الابن، و لكن الوكالة لا تريد اختيار الأهداف بنفسها، بل تريد أن يختارها الرئيس لها، لعلم الوكالة أن هذه الاغتيالات يحظرها القانون، وهي لا تريد أن تصبح كبش فداء حين تنقضى الحاجة إلى هذه الاغتيالات و يصبح المطلوب إعادة القناع الديمقراطي إلي وجه النظام. وتزعم الصحيفة أن أوامر الرئيس بوش تسمح باختيار أهداف خارج افغانستان او منظمة القاعدة، و أن لوائح قد اعدت بأسماء المزمع استهدافهم، وأنها تضم أشخاصا لا يمارسون إلا تمويل الإرهاب وليس ارتكابه مباشرة .

-Bush gives green light to CIA for assassination of named terrorists. 'Covert killings to take in less important al-Qaida figures', The Guardian, Mon 29 Oct 2001. At: https://www.theguardian.com/world/2001/oct/29/afghanistan.terrorism3

(40)Jeffrey Richelson and Michael L. Evans, National Security Archive Electronic Briefing Book No. 55, September 21, 2001, The National Security Archive, The September 11th Sourcebooks. At: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB55 /index1.html

(41) Ibid.

(42) Sudha N. Setty, The United States, In: Kenth Roach (Editor), Comparative Counter-Terrorism law, New York: Cambridge University Press, 2015, pp. 50-52.
(43) Ibid.
(44) Critical Foundations, Protecting America's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection, Washington DC, October 1997, pp. 3-4. At: https://fas.org/sgp/library/pccip.pdf
(٤٥) نتائج وأفكار استقصاء مؤتمر RSA2016 حول الإرهاب الإلكترونى، ٤ أبريل ٢٠١٦، متاح على الرابط:
-RSA 2016 Cyber Terrorism Survey Results and Thoughts, April 4th, 2016. At: https://thycotic.com/company/blog/2016/04/04/rsa-2016-cyberterrorism-survey-results-thoughts/
(46) Walter Weiss, Rapid Attack Detection, Isolation and Characterization Systems, Defense Advanced Research Projects Agency. At: https://www.darpa.mil/program/rapid-attack-detection-isolation-and-characterization-systems
(47) Charlotte Mellgard, The Silent war of cyber terrorism, VANDERBILT Political Review, Nov. 10, 2015. At: http://vanderbiltpoliticalreview.com/the-silent-war-of-cyber-terrorism /
(48)Chris Bing, Why the U.S is struggling with the digital war on ISIS, CYBERSCOOP, June 14, 2017, At: https://www.cyberscoop.com/us-cyber-command-digital-war-isis /
(49) Ryan Duff, The U.S military combined cyber and kinetic operations to hunt down ISIS last year, op.cit..
(50) LISA MONACO, Expanding Our Ability to Combat Cyber Threats, The White House, APRIL 1, 2015. At: https://obamawhitehouse.archives.gov/blog/2015/04/01/expanding-our-ability-combat-cyber-threats
(51) James A. Lewis, The Internet and Terrorism ،Center for Strategic and International Studies, April 2005. At:https://www.csis.org/files/media/csis/pubs/050401_internetandterrorism.pdf
(52) Joanie Chung Yin, A Critical Analysis on ISIS Propaganda and Social Media Strategies, University of Salford, Department of Terrorism and Security Studies, March 2015. At: http://www.researchgate.net/publication/316146537
(53) Mark Pomerleau, What Cyber Command learned from ISIS operations, Federal Times, November 19, 2017 At: https://www.federaltimes.com/smr/cybercon/2017/11/29/what-cyber-command-learned-from-isis-operations/
(54) Ibid.