مجلة الباحث للدراسات الأكاديمية
ISSN: 2352-975X ELBAHITH for Academic Studies EISSN: 2588-2368
المجلد: 07 / العدد: 02 / السنة: 2020 / ص ص: 558 ـ 578

الإرهاب الإلكتروني والتحول في مفهوم القوة

Electronic Terrorism And Transformation In The Concept Of Power

تاريخ الإرسال:2019/12/01 تاريخ القبول:2020/02/12

شرقي صبرينة (*)
المدرسة الوطنية العليا للعلوم السياسية - الجزائر
mirouislem@yahoo.fr

غريب حكيم
المدرسة الوطنية العليا للعلوم السياسية - الجزائر
gheriebhakim@hotmail.fr

ملخص:

رغم تعدد الاستخدامات السلمية ذات الطابع المدني التي قدمها، ولا يزال يقدمها الفضاء الإلكتروني والمعلوماتي عبر شبكة الإنترنت، إلا أنه ظهرت استخدامات أخرى غير سلمية لهذا الفضاء المتشعب الاتجاهات باستغلاله كساحة جديدة للأعمال الإرهابية، بحيث شكل هذا الفضاء السيبراني ما يسمى بظاهرة الإرهاب الإلكتروني الناشئة في الأساس من التزاوج بين تكنولوجيا الاتصال والمعلومات من جهة والإرهاب والحرب من جهة ثانية، الأمر الذي أدى إلى تغيرات وتحؤلات في مستويات القوة من القوة الصلبة إلى الناعمة إلى القوة الذكية فقوة إلكترونية، إضافة إلى انتقال القوة إلى فاعلين آخرين من غير الدولة، الأمر الذي أدى إلى زيادة الأعمال الإرهابية.

الكلمات المفتاحية: الإرهاب الإلكتروني؛ القوة؛ القوة الإلكترونية؛ الفضاء الإلكتروني؛ الانترنت المظلم.

Abstract:

Despite the multiplicity of the peaceful civil uses provided by the electronic space through the internet, new non peaceful uses have emerged which tend to use the internet as a space for terrorism. This has led to the emergence of the so-called electronic terrorism which has grown out of the blend between communication technology and information on the one hand and terrorism and war on the other. This led to changes and shifts in power levels from a solid to soft to smart to electronic power. In addition to the transfer of power to other non-state actors which led to the increase in the acts of terror.

Keywords: *Electronic Terrorism; Power; Electronic Power; Cyberspace; The Dark Web.*

(*)- المؤلف المُراسل.

مقدمة:

يشهد العالم منذ السنوات الأخيرة تقدما تقنيا وتكنولوجيا، قلما عرفه عصر من العصور السابقة من قبل، حتى بات هذا التقدم ثورة قائمة بذاتها في عالم الاتصالات والعلاقات الدولية كما أصبح العالم بفضلها بمثابة قرية كونية، بحيث أصبح للفضاء الإلكتروني دورا في حركة التفاعلات والتحولات البنيوية كمجال جديد في العلاقات الدولية، وبدأ ينتقل تأثيره من تغييرات هيكلية وتحتية إلى إحداث تغييرات كيفية في النظام الدولي حتى أصبح العالم اليوم يشهد تطورا في المخاطر الأمنية مع تطور مراحل النضج التكنولوجي ومع الانتقال من مرحلة النمو السريع إلى مرحلة الاستخدام الكثيف، الأمر الذي أدى إلى بروز جرائم إلكترونية عديدة على الساحة الدولية، وقد ارتبط بروز هذه الجرائم والتهديدات بالتغير في مفهوم القوة، وذلك راجع إلى بروز أنماط من التهديدات والتحديات المستحدثة والمتغيرة التي جاء بها الواقع الإلكتروني على الدول تجاه العديد من الأمور والقضايا والإشكاليات، وعلى رأسها تأتي التهديدات النتية، ومن بينها نجد تهديد الإرهاب الإلكتروني ومخاطره على مختلف الأصعدة، كالتجنيد أو صناعة الأسلحة والمتفجرات على اختلافها التي يستخدمها الإرهاب الإلكتروني أو في طرح الأيديولوجيات الإرهابية الدينية والمذهبية والعرقية وتوزيعها على الفضاءات حديثة النشأة، من ناحية أخرى استخدام الفضاءات التخيلية أو الافتراضية في نقل الرسائل الإرهابية المشفرة إلى خلايا نائمة أو يقظة في بلدان أخرى.

وبفضل الثورة التكنولوجية والاتصالية، وظهور الفضاء الإلكتروني طرأت تحولات جديدة على مفهوم القوة، وقد ظهر على الساحة الدولية مفهوم جديد أطلق عليه "جوزيف ناي " القوة الإلكترونية والتي أدت إلى توزيع القوة بين عدد أكبر من الفاعلين من غير الدول، بما فيهم الإرهاب، وذلك بعد أن كانت الدولة هي المحتكر الوحيد للقوة، مما جعل قدرة الدولة على الهيمنة على هذا المجال موضع شك، خاصة مع زيادة تأثير الجماعات الإرهابية على السياسية سواء على المستوى الوطني أو الدولي.

ولقد اتجهت الجماعات الإرهابية إلى امتلاك القوة الإلكترونية بعد أن واجهت صعوبة كبيرة في استخدام القوة الصلبة، الأمر الذي أدى إلى تزايد الخطر الإرهابي

EISSN: 2588-2368————————ISSN: 2352-975X

الذي أصبح يستغل وبصورة كبيرة الجانب المظلم للأنترنت، أو ما يطلق عليها بالشبكة المظلمة، أو الشبكة العميقة.

ومن هنا سنسعى من خلال مقالتنا هذه إلى دراسة الإرهاب الإلكتروني والتحول في مفهوم القوة ومحاولة تبيان العلاقة الترابطية بين الإرهاب الإلكتروني كتهديد دولي جديد والتغير في مفهوم القوة وأدواتها، وكيف وظفت هذه الجماعات الإرهابية الفضاء الإلكتروني للتأثير في التفاعلات الدولية.

- **المشكلة البحثية:** لقد أصبح الفضاء الإلكتروني اليوم العمود الفقري لمعظم التفاعلات الدولية، واتجاه معظم الدول والحكومات لتبني الحكومات الذكية، ومع سهولة الاستخدام ورخص التكلفة، وسهولة الاتصال وهشاشة القدرات والتنظيمات الرقابية في مقابل تزايد القوة الإلكترونية الأمر الذي أدى إلى توفير بيئة مناسبة لتواصل التنظيمات الإرهابية.

ومن هنا يمكن صياغة المشكلة البحثية في سؤال رئيسي متمثل في: " إلى أي مدى أثر الإرهاب الإلكتروني على التحول في مفهوم القوة في العلاقات الدولية ؟"

- **الأسئلة الفرعية:** ولقد تفرعت عن المشكلة البحثية أسئلة فرعية أهمها:

- ما المقصود بالإرهاب الإلكتروني ؟

- ما هو مفهوم القوة؟ وكيف أثر الفضاء الإلكتروني على التحول في مفهوم القوة وعناصرها وأيضا فواعلها ؟

- كيف وظفت الجماعات الإرهابية عناصر القوة الإلكترونية ؟

- **الفرضيات المستعملة:**

- أثر الإرهاب الإلكتروني على طبيعة القوة التي تمارس من خلاله بالإضافة إلى طبيعة النتائج والآثار المترتبة عنه.

- أدت الأساليب والطرق المختلفة والمتطورة للإرهاب الإلكتروني إلى التحول في مفهوم القوة وعناصرها.

- **أهمية الدراسة:**

- **الأهمية العلمية:** تظهر الأهمية العلمية للدراسة في تناولها أحد القضايا المهمة الجديدة في العلاقات الدولية، والتي أصبحت تشغل حيزا كبيرا من اهتمامات

EISSN: 2588-2368 ——— ISSN: 2352-975X

الباحثين والمراكز البحثية الغربية والعربية على حد سواء، فموضوع الإرهاب الإلكتروني والتحول في مفهوم القوة أصبح من اهتمامات الباحثين.

- **الأهمية العملية:** تكمن الأهمية العملية للدراسة بالأساس في تحليل استخدام الإرهاب الإلكتروني لعناصر القوة الإلكترونية من خلال استغلالهم لمواقع التواصل الاجتماعي، وأيضا استعمالهم لكافة عناصر القوة الإلكترونية من فيروسات، هاكر، تجسس...، الأمر الذي أصبح يستدعي استراتيجيات وأنظمة أمنية لمواجهة هذا التهديد الإرهابي الجديد.

المحور الأول: قراءة في الإرهاب الإلكتروني

سنحاول من خلال هذا المحور دراسة الإرهاب الإلكتروني، لذا سينقسم هذا المحور إلى ثلاثة نقاط، تدرس النقطة الأولى: مفهوم الإرهاب الإلكتروني، بينما تحلل النقطة الثانية خصائص الإرهاب الإلكتروني، أما النقطة الثالثة سنعرض أدوات الإرهاب الإلكتروني.

أولا- مفهوم الإرهاب الإلكتروني وخصائصه:

إن من أهم القضايا الجدلية على المستوى الدولي هو عدم وجود تعريف محدد للإرهاب بشكل عام، ولم يصل المجتمع الدولي حتى الآن إلى تعريف جامع مانع متفق عليه للإرهاب، ويرجع ذلك إلى تعدد أشكاله ومظاهره، وتعدد أساليبه وأنماطه، واختلاف وجهات النظر الدولية فما يراه البعض عملا إرهابيا، يراه البعض الآخر عملا مشروعا، وعليه سنحاول من خلال دراستنا هذه توضيح مفهوم الإرهاب والإرهاب الإلكتروني.

فالإرهاب في اللغة مشتقة من الفعل المزيد (أرهب) يرهب، إرهابا، وترهيبا، ويقال أرهب فلان أي خوفه وفزعه وهو نفس المعنى الذي يدل عليه الفعل المضاعف أو الثلاثي رهب والذي مصدره رهبا، أما الفعل المجرد يرهب، رهبة فيعني خافه، والرهبة هي الخوف والفزع.[1]

وبالانتقال إلى اللغة الفرنسية نجد كلمة Terreur, Terrorisme وتحملان المعنى نفسه وبترجمة كلمة Terreur إلى العربية نجد أنها تعني عدة معاني هي الرهبة، الذعر، والخوف الشديدين، وترادفها كلمة Terrorisme والتي تعني الإرهاب.[2]

EISSN: 2588-2368 ISSN: 2352-975X

في اللغة الانجليزية تعني كلمة Terrorisme الفزع والرعب، ويعرف قاموس السياسية الإنجليزي الإرهاب بأنه " الجماعات السياسية التي تستخدم العنف كأسلوب للضغط على الحكومات لإجبارها على إحداث التغيير".(3)

أما ريمون آرون Remond Aron فيعرف الإرهاب بأنه " فعل العنف الذي يتجاوز أهميته تأثيراته السيكولوجية أهمية نتائجه المادية البحتة، ويحدث هذا عند آرون بالاستغلال الكامل للحد المتوسط القائم بين العنف والرهبة، والتي هي عنصر أساسي واستراتيجي ثابت في كل العمليات الإرهابية، حيث يرى أن الرعب الناجم عن العنف في العملية الإرهابية ليس هدفها النهائي، بيد أنه ليس إلا وسيلة إجبار وضغط لتحقيق الهدف المنشود".(4)

ومن الملاحظ أن كل هذه التعريفات السابقة للإرهاب نجدها تشترك في حالة الرعب والفزع اللذين يسببهما الإرهاب للأفراد، من أجل بلوغ هدف ما.

هذا بالنسبة للإرهاب بصورته التقليدية، لكن ومع التطور الهائل لوسائل التقنية والتكنولوجية برز لنا مفهوم آخر للإرهاب وهو الإرهاب الإلكتروني.

وقد كانت بداية استخدام مصطلح الإرهاب الإلكتروني Cyber Terrorism في فترة الثمانينات على يد "باري كولين Barry Collin" والتي خلص فيها إلى صعوبة وضع تعريف متفق عليه للإرهاب الإلكتروني، ولكنه تبنى تعريفا للإرهاب الإلكتروني مقتضاه، بأنه " هجمة إلكترونية غرضها تهديد الحكومات أو العدوان عليها، سعيا لتحقيق أهداف سياسية أو دينية، وأيديولوجية، وأن الهجمة يجب أن تكون ذات أثر مدمر وتخريبي مكافئ للأفعال المادية للإرهاب".

أما "مارك بوليت" فيعرف الإرهاب الإلكتروني على أنه: "الهجوم المعتمد بدوافع سياسية ضد المعلومات ونظم الحاسوب وبرامج الكمبيوتر والبيانات التي تؤدي العنف ضد غير المقاتلين من قبل مجموعات دون وطنية أو عملاء سريين لتحقيق أهدافهم".(5)

أما البروفيسور "دوروثي دينينغ Dorothy. E. Denning" فيعرف الإرهاب الإلكتروني بأنه " التقارب بين الإرهاب والفضاء السيبراني وهو يعني الهجمات غير المشروعة والتهديدات بالهجوم على أجهزة الكمبيوتر".(6)

EISSN: 2588-2368 ISSN: 2352-975X

وكتعريف إجرائي للإرهاب الإلكتروني يمكن تعريفه بأنه: " نشاط أو هجوم متعمد ذو دوافع سياسية بغرض التأثير على القرارات الحكومية أو الرأي العام باستخدام الفضاء الإلكتروني كعامل مساعد ووسيط في عملية التنفيذ للعمل الإرهابي من خلال هجمات مباشرة على البنية التحتية للمعلومات، مما يؤدي إلى خلق خسائر مادية وحتى معنوية داخل المجتمع ".

ومما لا شك فيه أن الإرهاب الإلكتروني ينفرد بعدد من الخصائص التي يختص بها دون سواه، ويتميز بها عن غيره من الظواهر الإجرامية الأخرى، وعليه يتميز الإرهاب الإلكتروني بجملة من السمات والخصائص وهي كالتالي:(7)

1- يتسم الإرهاب الإلكتروني بكونه جريمة إرهابية متعدية الحدود، وعابرة للدول والقارات، وغير خاضعة لنطاق إقليمي محدد.

2- إن الإرهاب الإلكتروني لا يحتاج في ارتكابه إلى العنف والقوة العسكرية، بل يتطلب وجود حاسوب متصل بالشبكة المعلوماتية ومزود ببعض البرامج اللازمة على عكس الإرهاب التقليدي الذي كان يتم فيه استخدام أو التهديد باستخدام العنف.(8)

3- صعوبة اكتشاف جرائم الإرهاب الإلكتروني، ونقص الخبرة لدى بعض الأجهزة الأمنية والقضائية في التعامل مع هذا النوع من الجرائم، بالإضافة إلى صعوبة الإثبات في الإرهاب الإلكتروني، نظرا لسرعة غياب الدليل الرقمي، وسهولة إتلافه وتدميره.(9)

4- يتسم الإرهاب الإلكتروني أيضا بأنه يعتمد على المهارة في التعامل مع الحاسب والذكاء الفردي.

5- يتسم الإرهاب الإلكتروني بالقدرة على التخفي وتجهيل مصدر الهجمات.(10)

ثانيا- أدوات الإرهاب الإلكتروني:

تعتمد الجماعات الإرهابية وسط الفضاء الإلكتروني على مجموعة من الأدوات التي يستغلها من أجل تحقيق مآربها وأهدافها الإرهابية ومن أهم هذه الأدوات نذكر منها:

1- الفيروسات: والفيروسات الإلكترونية عبارة عن برامج تستنسخ نفسها في الجهاز المصاب عندما تنشط لتحدث تغييرات في البرامج أو البيئة التي تعمل فيها تلك البرامج

EISSN: 2588-2368————————ISSN: 2352-975X

ممـا يـؤدي إلى أضـرار مختلفـة، وقـد تصـل هـذه الأضـرار إلى فقـدان الملفـات المخزنـة، تحطم نظام التشغيل في الجهاز.[11]

2- التجسس على المواقع وتدميرها: يقوم الإرهابيون المبرمجون (قراصنة الحاسوب) باختراق المواقع أو الحواسيب الإلكترونية، باستخدام برامج للتجسس على الشبكات والأنظمة الإلكترونية، والاعتداء على البنية التحتية المعلوماتية للمؤسسات الحكومية والخاصة على حد سواء.[12]

3- اختراق المواقع الإلكترونية: حيث يقوم شخص أو أكثر باختراق موقع مضاد لتغيير محتوياته، أو سرقة معلومات سرية، أو تعطيل الموقع عن العمل، أو الاستيلاء عليه بشكل كامل عن طريق السيطرة على اسم النطاق.[13]

4- إنشاء المواقع الإلكترونية: فالمواقع الإلكترونية سهلت على المنظمات الإرهابية توسيع أنشطتهم لأبعد الحدود من خلال تبادل الآراء والأفكار والمعلومات، كما ساعدتهم على جمع أكبر عدد ممكن من الأتباع والأنصار عبر إشاعة أفكارهم ومبادئهم من خلال هذه المواقع ومنتديات الحوار، وغرف الدردشة.[14]

ثالثا- المواقع الإلكترونية المستخدمة من قبل الجماعات الإرهابية:

لقد استفادت التنظيمات الإرهابية في الألفية الجديدة من التقنيات والإمكانيات الوفيرة والحديثة التي وفرها الفضاء الإلكتروني لنشر أفكارهم المتطرفة واستغلالها في إتمام عمليّاتهم ضد أمن الشعوب والمجتمعات، فقد وفّرت شبكات التواصل الاجتماعي طريقة سهلة لنقل الأفكار والبيانات والمعلومات إلى عناصر الجماعات الإرهابية في غفلة من أجهزة الأمن في بداية الأمر، وهو ما حقّق لها نموًا كبيرًا وقدرة على تجنيد أعداد كبيرة من الشباب لخدمة أهدافها الإرهابية، كما أنّها تجعل تتبع النشاط الإلكتروني من قبل مزود الخدمة مثلا أو من قبل الحكومة أمراً شبه مستحيل، فالشبكة المظلمة هي المكان الأفضل للتخفي بعيداً عن أعين المراقبين.

1- شبكات التواصل الاجتماعي والإرهاب الإلكتروني: وعليه يمكن رصد بعض المواقع الأكثر استعمالا من قبل الجماعات الإرهابية على مواقع التواصل الاجتماعي وهي كالتالي:

EISSN: 2588-2368 ISSN: 2352-975X

أ- الفيسبوك: اهتمت الجماعات الإرهابية باستخدام الفيسبوك ودعت إلى غزوه نظرا لفعاليته وتحقيق الأهداف المختلفة من خلاله، كتقديم المعلومات الخاصة بصناعة القنابل والقيام بعمليات القتال وتقديم مختلف المعلومات للمنتسبين والقيام بالدعاية واستخدامه كذلك جمع المعلومات[15].

وحسب تقرير وزارة الأمن الداخلي الأمريكية فإن الاستخدامات الإرهابية للفيسبوك تتمثل في:[16]

- يعد الفيسبوك طريقة لتبادل المعلومات التشغيلية والتكتيكية، مثل صناعة القنابل، صيانة الأسلحة واستخدامها، .... وما إلى ذلك.

- يعد الفيسبوك كبوابة للدخول إلى المواقع المتطرفة والمحتوى الراديكالي الآخر، عبر ارتباط صفحات الفيسبوك بمنتديات أو مجموعات أخرى.

- يعتبر الفيسبوك كوسيلة إعلامية للدعاية الإرهابية والرسائل الأيديولوجية المتطرفة.

- يعتبر الفيسبوك ثورة من المعلومات التي يتم من خلاله البحث والاستطلاع على الأشخاص المستهدفين أو المنظمات.....

وعلى سبيل المثال لا الحصر نجد تنظيم داعش يقوم باستخدام موقع الفيسبوك، ليس فقط لتجنيد الشباب ولكن أيضا للترويج للسلاح والمخدرات وغيرها، حيث استخدم تنظيم داعش على الفيسبوك في ليبيا لبيع وشراء الأسلحة الثقيلة، بالإضافة إلى أن هناك مجموعات سرية في ليبيا تنتمي للتنظيم وتستخدم موقع الفيسبوك للترويج للأسلحة ولا يقتصر الأمر على الجماعات المسلحة في ليبيا بل إن هناك بعض الجماعات المسلحة في سوريا لجأت أيضا للطريقة ذاتها، حيث ظهرت العديد من الصفحات التي تروج للسلاح مثل "صفحة السلاح الأول في إدلب".

ب- تويتر: يستخدم موقع تويتر لخلق الموقف الأيديولوجي الذي يهدف إلى التخويف والتسبب في الخوف، وعلى الرغم من أن تويتر يسمح فقط بـ 140 حرف لنشر رسالة، فإن هذه الحسابات تسمح بنشر إعلانات والتعليق على حجم صغير[17].

والهدف من استخدام الإرهاب لموقع تويتر وبث الرسائل عليه يتمثل في:

- قدرة الموقع على خلق مناخ من الخوف والقلق.

EISSN: 2588-2368————————ISSN: 2352-975X

- قدرة الموقع على كسب عقول وقلوب الجماهير.

ج- موقع اليوتيوب: أصبحت خدمة تبادل الفيديو منصة مهمة للجماعات الجهادية والداعمين، وتعزيز التواصل، والدعاية وتجنيد أفراد جدد[18] . ومن جهة أخرى يستخدم اليوتيوب لبناء شبكات التواصل بين أعضاء ومنتسبي ومناصري ومتتبعي الجماعات الإرهابية مما يسمح بإرسال رسائل خاصة للمستخدمين وكذلك التعرف على بعضهم مما ينتج في النهاية مجتمع إرهابي افتراضي.[19]

ويساهم اليوتيوب في نقل الخبرات العسكرية مثل مهارات صناعة القبائل واستخدام الأسلحة كما يمكن اعتباره ساحة افتراضية للتدريب، وبحسب المرصد الدولي للدراسات حول الإرهاب فإن ما بين عامي 2014-2015م أنتجت الآلة الإعلامية لداعش أكثر من 15000 وثيقة دعائية منها 845 فيلما.[20]

د- الألعاب الإلكترونية: تعد الألعاب الإلكترونية من بين الوسائل التي يعتمد عليها الإرهاب الإلكتروني والجماعات الإرهابية لبث أفكاره واعتمد على استخدام الرسائل البصرية الجذابة وألعاب الفيديو كوسيلة جديدة لجذب الشباب إلى الجهاد، ومن ذلك تم إطلاق بعض الألعاب الجديدة "Call of Duty" والتي أصدر منها تنظيم داعش نسخة خاصة به.

كما استخدم الإرهاب الإلكتروني بعض الألعاب للتواصل بين أعضائه لأغراض التخطيط عبر الذبذبات الصوتية، مثل محاولتهم تجنيد أطفال في الولايات المتحدة الأمريكية من داخل لعبة "Roblox" الطفولية بهدف تنفيذ عمليات إرهابية داخل أراضيهم، وسجل التنظيم أيضا عروض فيديو لألعاب عنيفة مثل Grand the Ftauto V، وتطورت المجموعة كذلك تعديلا مجانيا للعبة AR MA3 الحربية المشهورة بواقعيتها في محاكاة الأسلحة والآليات في المعارك، وذلك لأهداف تدريبية.

2- الإنترنت المظلم والإرهاب الإلكتروني: في السنوات الأخيرة، أصبحنا أمام تحدي خطير تمثل في الجانب المظلم لتصفح الإنترنت، Dark Web أو Deep Web حيث يتم غلق البيانات والمعلومات بكلمة مرور، حيث يُطلب من المستخدم استخدام برنامج خاص للوصول إلى هذه البيانات، وتشير التقديرات إلى أن هذا الجانب المظلم من

EISSN: 2588-2368 ——— ISSN: 2352-975X

الإنترنت هو أكبر بكثير من الإنترنت العادي وأن المتسللين والمجرمين والإرهابيين أو المتحرشين بالأطفال يمكنهم القيام بأنشطتهم غير القانونية بحرية كاملة من خلال شبكة الويب العميقة.

فالإنترنت المظلم هي جزء من الإنترنت لا يمكن الوصول إليه من خلال أدوات التصفح العادية أو طرق التصفح اليومية، فهي جزء من الفضاء الإلكتروني استنادًا إلى الخدمات والبروتوكولات القياسية، ولكنه يتطلب تحديدًا محددًا للاستخدام، فهي ليست خدمات عامة، ويُعد Dark Web أو Dark Net جزءًا من الإنترنت، لكنه يتطلب مهارات أو بيانات خاصة من أجل توصيل الأنشطة غير القانونية المختلفة في الفضاء الإلكتروني[21].

فالإنترنت العميق The Deep Web هو مجموع جميع المواقع الإلكترونية التي لم تدرج في محركات البحث، وبعض المواقع العميقة، وهي أسواق غير تقليدية تقدم مجموعة من المنتجات أو الخدمات، حيث يمكن شراء أو التوسط في شراء العقاقير غير المشروعة والأسلحة والسلع المقلّدة وبطاقات الائتمان المسروقة والبيانات المخترقة، أو العملات الرقمية، أو البرامجيات الضارة وبطاقات الهوية الوطنية أو جوازات السفر، ويمكن[22].

المحور الثاني: قراءة في مفهوم القوة وطبيعة تحولاتها

سنحاول من خلال هذا المحور دراسة مفهوم القوة وطبيعة تحولاتها لذا تم تقسيمه إلى ثلاثة نقاط أساسية، بداية بمفهوم القوة، مرورا بدراسة الفضاء الإلكتروني وتحولات القوة، وصولا إلى عناصر القوة الإلكترونية.

أولا- مفهوم القوة:

تعتبر القوة من أكثر المفردات استخداما في العلاقات الدولية في ظل نظام يفتقد الحكومة العالمية المشتركة، لذلك تهدف الدول إلى ضمان أمنها من خلال امتلاك القوة، والتي يراها " هانس مورجانتو " بأنها: " الغاية والوسيلة في السياسة العالمية ".[23]

ويرى "ستيفن لوكس Stephen Lux" في كتابه عام 1974م بأن القوة مرتبطة بتحديد الأجندة، للتأثير في سلوك الدول وبالتالي لا تعني القوة لا تعني القوة بالضرورة الإكراه، وقد طور "جوزيف ناي Joseph Nye" أفكار لوكس وقدم مفهوما للقوة،

EISSN: 2588-2368————————ISSN: 2352-975X

حيث اهتم بالعناصر غير المادية مثل الثقافة والقيم من خلال مفهوم القوة الناعمة والتي عرفها بأنها: " قدرة الدولة على الحصول على ما تريد بالاعتماد على الجاذبية بدلا من الإكراه"[24].

ويمكن الإشارة إلى أن مضمون وعناصر القوة وفق مصادر التهديد المحتملة والفعلية للأمن، ومن هنا سنحاول التركيز على السياق الفكري وحجم التغير في مفهوم القوة وفق رؤى نظريات العلاقات الدولية.

1- النظرية الواقعية ورؤيتها للقوة: تركز هذه النظرية على القوة الصلبة التي تعتبر أن القوة هي الإكراه والإجبار وتعتمد بشكل رئيسي على القوة العسكرية، وقد سيطر هذا المفهوم على أدبيات العلاقات الدولية لفترة طويلة، وقد تميزت بغلبة الطابع الصراعي بين الدول لامتلاك القوة.

2- النظرية الليبرالية والقوة الناعمة: بفعل تنامي فاعلين جدد إلى جانب الدولة كفواعل مؤثرة على العلاقات الدولية، أدى هذا إلى تزايد أهمية العلاقات العابرة للقوميات، الأمر الذي أدى إلى ظهور مفاهيم جديدة خاصة مفهوم القوة حيث انتقلت من مفهومها الصلب إلى مفهومها الناعم وقد عرف جوزيف ناي القوة الناعمة بأنها: "القدرة على إقناع الآخرين لجعلهم يتفقون مع قيمك، ومبادئك ومؤسساتك، وهي قوة تعتمد على الأفكار والثقافة ".[25]

وأخيرا يمكن القول أن القوة هي " الاستخدام الواعي لأي قدرة تمتلكها سوى كانت عسكرية أو ثقافية أو إلكترونية أو حتى اقتصادية للتأثر في سلوك الآخرين، للحصول على نتائج متوقعة من قبل من يمارس القوة".

ثانيا- الفضاء الإلكتروني وتحولات مفهوم القوة:

ونقصد بالفضاء الإلكتروني: " ذلك المجال الذي يتميز باستخدام الإلكترونيات والمجال الكهرومغناطيسي لتخزين وتعديل أو تغيير البيانات عن طريق النظم المتصلة والمرتبطة بالبنية التحتية الطبيعية ".

1- القوة الصلبة وعلاقتها بالفضاء الإلكتروني: أدى الفضاء الإلكتروني دورا كبيرا في تطور القوة الصلبة، وذلك بقيام الثورة في الشؤون العسكرية، وكذلك

EISSN: 2588-2368 ——— ISSN: 2352-975X

تطور نظام التسلح وطبيعة ونوعية الأسلحة، وقدرتها التدميرية وبالتالي التأثير على قوة الدولة النسبية، وقدرتها على الهيمنة على النظام الدولي.[26]

2- القوة الناعمة وعلاقتها بالفضاء الإلكتروني: أدى بروز القوة الناعمة إلى اعتماد الدول وبشكل كبير على بناء القوة من خلال الاعتماد على أهمية الأفكار والابتكار كأساس للاستحواذ على القوة، وبالتالي أهمية تطوير مفاهيم استراتيجية، والتقدم الاستخباراتي في المجال التقني والاقتصادي ونظم الاتصالات.

3- بروز القوة الإلكترونية: Cyber Power يعتبر جوزيف ناي من أهم من تحدثوا على القوة الإلكترونية كشكل جديد للقوة، وهي مرتبطة بامتلاك المعرفة التكنولوجية، والقدرة على استخدامها، وهي تعني: " القدرة على الحصول على المخرجات المرغوبة من خلال استخدام المعلومات المترابطة إلكترونيا عبر الفضاء الإلكتروني".[27]

ثالثا- عناصر القوة الإلكترونية:

وتتركز عناصر القوة الإلكترونية لدولة ما في ثلاثة محاور أساسية وهي كالتالي:

1- بنية تكنولوجية: وهي بمثابة البنية التحتية اللازمة للقوة الإلكترونية فبدلا من الدبابات والطائرات والغواصات، تحتاج الدولة في هذا النوع إلى أجهزة الكمبيوتر، وشبكات اتصالات مرتبطة بأجهزة الكمبيوتر بعضها ببعض، وبرمجيات متطورة، بالإضافة إلى العنصر البشري المدرب على استخدام هذه الأجهزة والشبكات.[28]

2- الأسلحة الإلكترونية: وهي برامج تم تصميمها للقيام بوظائف مختلفة والتي من بينها (الفيروسات، الديدان، أحصنة طروادة، قنابل منطقية، وغيرهم الكثير....). [29]

3- العمليات الإلكترونية: وتنقسم إلى ثلاثة أنواع:

- مهاجمة شبكات الحاسب الآلي.

- الدفاع عن شبكات الحاسب الآلي وتشمل هذه العملية حماية الشبكات وأجهزة الكمبيوتر من أية عملية اختراق خارجي.

- استطلاع شبكات الحاسب الآلي وتعني القدرة على الدخول غير المشروع والتجسس على شبكات الخصم، دون أن يصاحب ذلك تدمير أو تخريب للبيانات والمعلومات.

EISSN: 2588-2368————————ISSN: 2352-975X

المحور الثالث: الإرهاب الإلكتروني واستخدام القوة الإلكترونية

سنتطرق من خلال هذا المحور إلى دراسة الإرهاب الإلكتروني واستخدام القوة الإلكترونية، وذلك من خلال توزيعه إلى ثلاثة نقاط أساسية وهي كالتالي:

أولا- كيفية توظيف الإرهاب الإلكتروني للقوة الإلكترونية:

وقد وظف الإرهاب الإلكتروني القوة الإلكتروني كالتالي:

1- استخدام الفضاء الإلكتروني كمنصات إعلامية: حيث تتولى المواقع التابعة للجماعات الإرهابية نشر أخبارهم، وكذلك نشر العمليات التي يقومون بها أو حتى نفي مسؤوليتهم عن بعض الأنشطة.

2- الدعاية والترويج للأفكار الإرهابية: يعد الفضاء الإلكتروني من الوسائل المهمة بنشر أفكارهم وكسب متعاطفين جدد، وكحرب نفسية على الأعداء، ولقد نمت الآلة الإعلامية الإلكترونية للجماعات الإرهابية في الفترة الأخيرة بشكل كبير.

3- تجنيد أتباع جدد: أتاح الفضاء الإلكتروني للتنظيمات الإرهابية فرصة تجنيد أعضاء جدد في التنظيمات بما يضمن استمرارية وبقاء هذه التنظيمات وذلك من خلال قدرة هذه الأخيرة على الدعاية وبث الأفكار المروجة للعمل الإرهابي.(30)

ولتوظيف الإرهاب القوة الإلكترونية فقد اعتمد على أدوات مختلفة ويمكن تقسيم هذه الأدوات إلى أداتين رئيستين وهما:

أ- المواقع الإلكترونية: وهي مجموعة من صفحات على الويب مرتبطة ببعضها، ومخزنة على نفس الخادم، وتختلف حسب الهدف منها فهناك مواقع تجارية، ومواقع خاصة بالمحادثات أو منتديات النقاش، بجانب المدونات الإلكترونية، وقد زاد عدد المواقع الإلكترونية الإرهابية من 12 موقع سنة 1998م إلى حوالي 4800 موقع اليوم وهذا حسب ما أورده "غابريال ويمان Gabriel Weimann" في كتابه المعنون بـ "الإرهاب على الانترنت: ساحة جيدة، تحدي جديد " الصادر سنة 2006 عن معهد السلام الأمريكي، ويمكن رصد مجموعة من المواقع الإلكترونية التي توظفها الجماعات الإرهابية لتحقيق أهدافها ويمكن ذكر البعض منها:(31)

أ- 1- منتدى شبكة أخبار العالم: ويضم العديد من رسائل المنظمات الإرهابية، من بينها القاعدة وتنظيم داعش.

EISSN: 2588-2368————————ISSN: 2352-975X

أ- 2- منتدى الساحة: الذي يضم إنتاج شركة " السحاب " وخطابات قيادات تنظيم القاعدة.

أ- 3- موقع النداء: وهو الموقع الرسمي لتنظيم القاعدة بعد أحداث الحادي عشر من سبتمبر من عام 2001م، ومن خلاله تصدر البيانات الإعلامية للقاعدة.(32)

أ- 4- شبكات التواصل الاجتماعي: وأهمها الفيسبوك، تويتر، اليوتيوب، وانستجرام، وعبر هذه الوسائل تعمل المنظمات الإرهابية على تحقيق أهدافها، ويمكن عرض أربعة مستويات من النشاطات الإرهابية عبر مواقع التواصل الاجتماعي وهي كالتالي:(33)

- **المستوى الأول:** ويتضمن هذا المستوى مجموعة من نشاطات المحتوى الذي تطرحه التنظيمات الإرهابية عبر " تويتر " وحساباته بشبكات التواصل الاجتماعي الأخرى، بحيث يجري رفع معظم الشرائط المصورة بصورة مركزية، وتستخدم هذه التنظيمات وخاصة تنظيم داعش العديد من الأساليب المتقدمة، منها تصوير الحركة البطيئة ورسوم الجرافيك.

- **المستوى الثاني**: يتألف من نشر حسابات إقليمية أو محلية لتقارير حية لضربات بجانب رسائل محلية.

- **المستوى الثالث:** الأفراد المقاتلين الذين ينشرون تحديثات بخصوص تجاربهم عبر ما يبدو أنها حسابات شخصية، وتحمل هذه المنشورات طابعا شخصيا وعاطفيا أكبر تجذب أكثر الشباب الذين من المحتمل أن ينظموا لهذه التنظيمات.

- **المستوى الرابع:** بقع خارج سيطرة التنظيم الإعلامية ويضم المتعاطفين والأنصار (الناشرين) الذين يقومون بإعادة نشر رسائل ومحتويات التنظيم عبر حساباتهم أو محتويات أخرى من إنتاجهم.(34)

فقد أصبحت التنظيمات الإرهابية تعتمد وبشكل كبير على استغلال شبكات التواصل الاجتماعي ليس فقط للاستقطاب بل لاستعراض نفوذها وشراستها بغرض الحشد والتعبئة أو التخويف من مواجهتها، أو حتى لتوجيه رسائل تهديد لمن تعتبره عدوا لها.

EISSN: 2588-2368————————ISSN: 2352-975X

وفي دراسة قام بها مركز سياسة الشرق الأوسط بينت أن تنظيم داعش الإرهابي استطاع الترويج لأفكاره الإرهابية من خلال 46000 حساب تويتر تستخدم لبث تغريدات واستهداف عناصر جديدة، ويكمن إقبال داعش على تويتر نظرا لأنه يسمح بنقل الأخبار بصورة سريعة عند وقوع الحدث.

وقد نشطت في عامي 2017م-2018م الكثير من الجماعات الإرهابية على تطبيق تليغرام وبدأت تستخدمه على نطاق واسع وهو من حيث أصل المنشأ موجود في جمهوريات الاتحاد السوفييتي السابقة، وزاد عدد مستخدميه تدريجيا، حتى بلغ 200 مليون وهو ما أثار جدلا في السنوات الأخيرة،

ثانيا- الإنترنت المظلم (The Dark Web) أرض النشاطات الإرهابية:

سنحاول تسليط الضوء من خلال هذه النقطة على الاستخدامات الإرهابية للإنترنت المظلم واستغلاله كوسيلة قوة في اداء مهامه الغير قانونية وتحقيق أهدافه وذلك عبر:

1- يستخدم الإرهابيون شبكة Dark web للتجنيد: حيث يتم إجراء اتصال أولي على منصات الويب السطحية، وغالبًا ما يتم تقديم المزيد من الإرشادات حول تطبيقات التشفير من طرف إلى طرف مثل استخدام تطبيق التليغرام Telegram للوصول إلى مواقع الجهاديين على الأنترنت المظلم.

2- يستخدم الإرهابيون شبكة الإنترنت المظلم للاختباء: أدت مراقبة شبكة الإنترنت من قبل شركات التواصل الاجتماعي ومسؤولي الأمن إلى زيادة معدل إزالة المحتوى المتطرف من منصات وسائل التواصل الاجتماعي، الأمر الذي أدى زيادة استخدام الإنترنت المظلم للاتصالات والهجمات المتطرفة والتخطيط للعمليات الإرهابية.(35)

3- التشفير والمراوغة للإنترنت المظلم: يستخدم الكثير من مستخدمي الإنترنت التشفير، على سبيل المثال، شبكات الإنترنت الافتراضية الخاصة (VPNs) للحفاظ على خصوصية أنشطة الإنترنت، وعادةً ما تلتزم ارتباطات شبكة الإنترنت الافتراضية الخاصة (VPN) بمعايير السلوك التقليدية لتوجيه الإنترنت..

4- بعض العمليات الإرهابية عبر الإنترنت المظلم: ومن العمليات الإرهابية التي اعتمدت على التقنيات الإلكترونية نذكر منها:

EISSN: 2588-2368 ——— ISSN: 2352-975X

أ- قيام منظمة إرهابية في أستراليا بتدمير شبكة الصرف الصحي بواسطة عملية إلكترونية، مما نجم عنها أضرار صحية واقتصادية فادحة.

ب- كما قامت منظمة آوم شيريكو الإرهابية اليابانية باختراق نظام البرمجة المتحكم في مسار أعداد هائلة من سيارات الخدمة العامة، ولقد نجحت تلك المنظمة بواسطة التلاعب بأنظمة الحاسب والإنترنت من تعطيل أنظمة أكثر من خمسين شركة يابانية كبرى واختراق أنظمة عشر إدارات حكومية وتوجيهها لصالحها.

ج- كذلك استطاعت إحدى المنظمات الإرهابية من مسح جميع البيانات السكانية لليابان بواسطة اختراق أحد المواقع الحكومية، وهذه الهجمات تزيد بمعدل 60٪ سنوياً.

ثالثا: المواجهة الدولية للإرهاب الإلكتروني

أدرك المجتمع الدولي مدى خطورة الأعمال الإرهابية الإلكترونية، وأضرارها بعد أن تجاوزت النطاق المحلي والإقليمي، وباتت ظاهرة قومية تهدد المجتمع الدولي، وأضحت الجماعات الإرهابية فاعل دولي غير رسمي، الأمر الذي فرض أغلب الدول والحكومات إلى اعتماد مجموعة من الإجراءات الإلكترونية والتي كانت على شكل مجموعة من الأجهزة والأنظمة والبرامج المتكاملة مع بعضها وفقا لبرنامج موضوع مسبقا للتصدي لأي اختراق في نظم المعلومات بهدف حمايتها تقنيا من الهجمات الإرهابية.

1- مواجهة الإرهاب الإلكتروني على المستوى الدولي:

أ- منظمة الأمم المتحدة ومواجهة الإرهاب الإلكتروني: ذكر التقرير السنوي لمكتب الأمم المتحدة المعني بمحاربة المخدرات والجريمة لسنة 2015، أن عدم وجود اتفاق دولي بشأن الجريمة السيبرانية والإرهاب يعرقل الجهود الرامية إلى تقديم الإرهابيين للعدالة، وعليه وجب:

- أن تعمل وكلات إنفاذ القانون مع مقدمي خدمات الإنترنت لجمع الأدلة الرئيسية في قضايا الإرهاب الإلكتروني.

- وجب على مشغلي شبكات Wi-fi ومقاهي الإنترنت النظر في مطالبة مستخدميها بالتسجيل وتحديد هويتهم.

EISSN: 2588-2368————————ISSN: 2352-975X

- وجب على الحكومات الوطنية أن تحظر أي نشاط إرهابي الإنترنت.

ب- الاتحاد الأوروبي ومواجهة الإرهاب الكتروني: بذل الاتحاد الأوروبي دورا هاما في مجال مواجهة الإرهاب الإلكتروني ويمكن تحديد مجالين رئيسين للسياسات في مجال الأمن الإلكتروني وهما: (36)

المجال الأول: اتخذ الاتحاد الأوروبي إجراءات لتعزيز قدرة الشبكة على مواجهة الهجمات المحتملة وقدرات الاستجابة للحوادث، وتدخل هذه التدابير تحت عناوين مثل الشبكة وأمن المعلومات (NIS)، وحماية البنية التحتية الحرجة (CIP)، وحماية النية التحتية المعلوماتية الهامة (CLIP).

المجال الثاني: عالج الاتحاد الأوروبي الجريمة السيبرانية والإرهاب الإلكتروني من منظور إنفاذ القانون. وقد كان تفصيل مستوى الأمن السيبراني في الاتحاد الأوروبي احد أهم الأهداف الاستراتيجية لأمن الداخلي التي اعتمدت في عام 2010، وقد نصت الاستراتيجية على إنشاء مركز الاتحاد الأوروبي لمكافحة الجريمة السيبرانية سنة 2013.

2- السياسات الحكومية في مواجهة الإرهاب الإلكتروني: ومن بين السياسات الحكومية لمكافحة قوة الإرهاب الإلكتروني على الأنترنت نجد:

أ- السياسات الأمريكية لمواجهة الإرهاب الإلكتروني: ففي الولايات المتحدة الأمريكية، أنشأت وكالة الاستخبارات المركزية (CIA) مجموعة منظمة تتعاط مع جوانب تخص الإرهاب الإلكتروني وأطلقت عليها اسم (مركز حرب المعلومات)، الذي يضم نحو ألف موظف بينهم مجموعة تعمل على مدار الساعة مناوبة على الرد على أي تطورات أو استفسارات.(37)

وقد تميزت الاستراتيجية الأمريكية لمكافحة الإرهاب الإلكتروني بطابع استباق الهجمات المحتملة، وذلك عن طريق رصد خطة للهجوم المعلوماتي، وتعتمد بالأساس على تطوير تقنيات الحرب المعلوماتية، كشف هجمات استباقية تستهدف شبكات الدول المعادية، وتسمح بالمقابل بتعزيز دفاعها ضد الهجمات الإلكترونية والإرهاب الإلكتروني.

EISSN: 2588-2368 ——— ISSN: 2352-975X

أما على المستوى التشريعي، فتعمل الحكومة الفيدرالية الأمريكية جاهدة على سن تشريعات متطورة لمكافحة هذه الأنماط المستجدة للظاهرة الإرهابية، بحيث تحاول تقنين استخدام محرك البحث في مجموعة من شركات الاتصال ك: "MSN" و"YAHOO" و"GOOGLE".[38]

ب- السياسات السعودية في مواجهة الإرهاب الإلكتروني: أصدر المنظم السعودي جملة من الأنظمة المعنية لمكافحة جرائم الإرهاب، بما في ذلك جرائم الإرهاب الإلكتروني، ولعل من أهمها: نظام مكافحة الإرهاب وتمويله ونظام مكافحة الجرائم المعلوماتية. وقد وضعت المملكة السعودية استراتيجية قائمة على ثلاث (3) محاور أساسية لمواجهة خطر الإرهاب الإلكتروني، وتتمثل محاور هذه الاستراتيجية في:[39]

ب-1- الرصد: ويهدف إلى القراءة الصحيحة للواقع، وتحليل مؤشرات الخطورة في مسارات العقل الإرهابي.

ب-2- المواجهة: ويهدف إلى التفاعل المباشر مع العقول والأفكار والمشاعر، بدون تفاعل مباشر واتصال بشري مع المستهدفين.

ب-3- الوقاية: وتعني صناعة "رأي عام صحي" داخل بيانات مستهدفة، وهذا لا يتم إلا بوجود "محتوى" وحضور بشري مؤهل.

ج- السياسات المصرية لمواجهة الإرهاب الإلكتروني: اتخذت وزارة الاتصالات والمعلومات في مصر بإصدار نظام عن الجريمة الإلكترونية، يتضمن عقوبات رادعة لمن يقوم من الأفراد أو المؤسسات بتزوير أو إفساد مستند إلكتروني على الشبكة، أو الكشف عن بيانات ومعلومات بدون وجه حق، وغيرها من صور الجريمة الإلكترونية. ففي 2002 صدر القرار الوزاري رقم 13507 بإنشاء إدارة لمكافحة جرائم الحاسوب وشبكات المعلومات ويساهم في مكافحة الإرهاب الإلكتروني.

خاتمة:

مما سبق يمكن القول أن الإرهاب الإلكتروني أصبح يمثل هاجسا وخطرا كبيرا يهدد كافة الدول، بالإضافة إلى تأثيره المتزايد على السياسة العالمية خاصة بعد أحداث الحادي عشر من سبتمبر 2001م.

EISSN: 2588-2368————————ISSN: 2352-975X

أما بالنسبة لمفهوم القوة فقد طرأت عليها تغيرات عديدة وفقا لتطورات السياسة الدولية وقد اختلفت منظورات العلاقات الدولية في تناولها وظهر مفهوم القوة الصلبة ثم الناعمة ثم القوة الذكية وأخيرا القوة الإلكترونية.

وقد أثرت الثورة المعلوماتية والفضاء الإلكتروني والتهديدات الناجمة عنه وخاصة الإرهاب الإلكتروني على تحولات مفهوم القوة، وظهر مفهوم القوة الإلكترونية كما ساعد على انتشار القوة على المستويين الداخلي والخارجي، إذ أصبحت القوة في متناول الفاعلين من غير الدول، الأمر الذي أدى إلى تفاقم مخاطر الإرهاب الإلكتروني وقد حاولت بعض الدول اتخاذ تدابير وإجراءات لازمة لمواجهة الإرهاب الإلكتروني، إلا أن هذه الجهود قليلة ومازالت بحاجة إلى المزيد من العمل المكثف والتنظيم والتنسيق،

- التوصيات:

بناء على هذه النتائج نقدم عددا من التوصيات للموضوع المدروس ومن بينها نجد:

- رصد أنشطة الجماعات الإرهابية على الفضاء الإلكتروني وتحليل محتواها وأهدافها والاستراتيجيات المعتمدة.

- محاولة إشراك المجتمع المدني للتعاون والإبلاغ على المواقع ذات العلاقة بالإرهاب.

- العمل على نشر الثقافة الوقائية وتوعية المجتمع بمخاطر الإرهاب الإلكتروني.

- العمل على تحقيق التعاون الدولي في مجال مكافحة الإرهاب الإلكتروني من خلال تبادل المعلومات والخبرات والاستفادة من المنظمات الدولية المختصة ذات الخبرة.

- تفعيل برامج لمواجهة خطر الإرهاب الإلكتروني والعمل على تطوير القوة الإلكترونية لمحاربة هذا الخطر.

الهوامش والمراجع:

[1]- العياشي وقاف: مكافحة الإرهاب بين السياسة والقانون، دار الخلدونية للنشر والتوزيع، الجزائر، 2006، ص. 12.

[2]- محمد مطليسي، الإرهاب الدولي والحصانة الدبلوماسية، أطروحة الدكتوراه، كلية الحقوق، جامعة القاهرة، 1998، ص.36.

[3]- محمد صادق صابور، الإرهاب في العالم، دار الأمين، القاهرة، 2002، ص. 37.

[4]- مايا حسن ملا خاطر، "الاطار القانوني لجريمة الإرهاب الإلكتروني، مجلة جامعة الناصر، ع.5، جانفي، جوان 2015، ص. 132.

[5]- Zahir Yonos, Cyber security Malaysia , star in - tech, February 2009, p. 2.

EISSN: 2588-2368————————ISSN: 2352-975X

(6)- ibid, p. 2.

(7)- أيسر محمد عطية، دور الآليات الحديثة للحد من الجرائم المستحدثة الإرهاب الإلكتروني وطرق مواجهته، في مؤتمر، الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، عمان، ط2- 2014/9/4، ص. 12.

(8)- عادل عبد الصادق، الإرهاب الإلكتروني القوة في العلاقات الدولية نمط جديد وتحديات مختلفة، القاهرة: مركز الدراسات السياسية والاستراتيجية، 2009، ص. 112.

(9)- أيسر محمد عطية، المرجع السابق، 12.

(10)- عادل عبد الصادق، المرجع السابق، ص ص. 112-115

(11)- مايا حسن ملا خاطر، المرجع السابق، ص. 135.

(12)- عبد العزيز بن حميدان الثمالي، تأثير الإرهاب الإلكتروني، وسبل مكافحته، في مؤتمر، المؤتمر الإسلامي العالمي، المعنون ب: مكافحة الإرهاب، مكة المكرمة، 22-2010/02/25، ص. 15.

(13)- عادل عبد الصادق، المرجع السابق، ص. 119.

(14)- أيسر محمد عطية، المرجع السابق، ص. 16.

(15)- محمد قيراط، الإعلام الجديد والإرهاب الإلكتروني: آليات الاستخدام وتحديات المواجهة، مجلة الحكمة للدراسات الاتصالية والإعلامية، جانفي، جوان، 2017، ص. 25.

(16)- Gabriel weimann, New terrorissm and new mediam, Washington: commons lab of the woodrom Wilson international center for scholars, 2014, p.6.

(17)- Imran Awan, cyber - extremism: isis and the pouer of social media, social science and public policy, 2017, p. 142.

(18)- Gabriel weimann, ibid, p.10.

(19)- محمد قيراط، المرجع السابق، ص. 25.

(20)- عسلون بنعيسى، مواقع التواصل الاجتماعي: منصات حية تستغل لصناعة الإرهاب والموت، مجلة الإذاعات العربية، ع. 1، 2016، ص. 53.

(21)- Vida Vilic, Dark web, cyber terrorism and cyber warfar: dark side of the cyber space, Balkan social science, vol.10, December, 25-07-2017, p. 3.

(22)- مصطفى سعيد، الإنترنت المظلم أرض الأنشطة الإرهابية المخفية، نقلا عن الرابط التالي:

https://www.hafryat.com/ar/blog/

تاريخ التصفح: (06-10-2019).

(23)- جيمس دورتي، النظريات المتضاربة في العلاقات الدولية، تر: وليد عيد الحي، مكتبة شركة كاظم للنشر والتوزيع، بيروت، د. ت، ص ص (61-107).

(24)- المرجع نفسه، ص ص. 18-19.

EISSN: 2588-2368————————ISSN: 2352-975X

(25)- صباح عبد الصبور عبد الحي، استخدام القوة الإلكترونية في التفاعلات الدولية تنظيم القاعدة نموذجا، ج.2، دراسات سياسية، 2016/11/5، ص ص. (16-18).

(26)-صباح عبد الصبور، المرجع السابق، ص. 19.

(27)- Franklin D. Kramer, Sturat H. Starr, Larry Wenty, Cyber power and national security, USA: university of Nebraska press, Potomac books, 2009, p. 30

(28)- إيهاب خليفة، " القوة الإلكترونية وأبعاد التحول في خصائص القوة "، أوراق، ع. 12، 2014، ص. 45.

(29)- المرجع نفسه، ص ص. (46-50).

(30)- فالح فليحان فالح الرويلي، استراتيجيات التنظيمات المتطرفة في التجنيد عبر الانترنت داعش نموذجا، ورقة بحثية مقدمة: لجامعة نايف العربية للعلوم الأمنية، 2018، ص. 4.

(31)- صباح عبد الصبور، استخدام القوة الإلكترونية في التفاعلات الدولية تنظيم القاعدة نموذجا، ج. 4، دراسات سياسية، 2016/11/19، ص.7.

(32)- أيسر محمد عطية، المرجع السابق، ص. 17.

(33)- صباح عبد الصبور، المرجع السابق، ص. 7.

(34)- مروى صبري، استراتيجية داعش عبر شبكات التواصل الاجتماعي، نقلا عن الرابط التالي:
http://futureuae.com/ar/mainpage/item/229/
تاريخ التصفح (2018/11/25).

(35)- wilson center, Going darker ? the challenge of the dark net terrorism , Quoting the following link:
https://www.wilsoncenter.org/sites/default/files/going_darker
Date of visit (09-10-2019).

(36)- PiotrBakawski, cuber security in the european union ,European parliamentary research service, (v.1,2013), p.4.

(37)- على عدنان الفيل، الإرهاب الإلكتروني، مجلة الجامعة الخليجية، م2، ع.2. 2010، ص.25.

(38)- المرجع نفسه.

(39)- السكينة، استراتيجية سعودية في مواجهة الإرهاب الإلكتروني، نقلا عن الرابط التالي:
https://www.assakina.com/awareness.net/processors/101804.htmc
تاريخ التصفح (25/ 09/ 2019).

EISSN: 2588-2368————————ISSN: 2352-975X