دور الاستخبارات الإلكترونية في مكافحة الإرهاب السيبراني

The Role of Cyber Intelligence in the Fight against Cyber-Terrorism

قوادرة حسين *

جامعة أم البواقي ، الجزائر، hocine751@yahoo.fr

كحلوش منى

جامعة سكيكدة، الجزائر، Kahlouche.mouna41@gmail.com

تاريخ الإرسال: 2021/01/20 **تاريخ القبول: 2020/03/16**

ملخص:

أضحت الإنترنت وسيلة ذات أهمية حاسمة في العمليات اليومية للجماعات المتطرفة خصوصا تلك المرتبطة بحركة الجهاد العالمي. حيث تزود الإنترنت الحركات الإرهابية المتطرفة بواجهة التجنيد والدعاية، فضلاً عن وسائل النمو الإيديولوجي وتبادل الأفكار، باعتبار أن التواجد الجهادي المتطرف على الإنترنت يمثل العقل المادي لحركة الجهاد العالمية. لذلك فإن انفتاح الإنترنت وإمكانية الوصول إليها يوفران لمجتمع الاستخبارات السيبرانية مجموعة كبيرة من المواد المساعدة على جمع المعلومات الإستخباراتية وتحليلها. وبالرغم من إهمال هذا المورد في السنوات الأخيرة، فقد يكون السبيل لمواجهة مشكلة الإرهاب السيبراني في تسخير القطاعين الخاص والأكاديمي كأذرع بحثية غير رسمية لمجتمع مكافحة الإرهاب السيبراني.

الكلمات المفتاحية: الإرهاب السيبراني؛ الاستخبارات الإلكترونية؛ مكافحة الإرهاب؛ تحليل المواقع الجهادية؛ الهجمات المضادة.

Abstract:

The Internet has become means of critical importance in the day-to-day operations of extremist groups, especially those associated with the global jihad movement. The Internet provides extremist terrorist movements with the interface of recruitment and propaganda, as well as means of ideological growth and the exchange of ideas, given that the jihadist presence on the internet represents the material mind of the global jihad movement. Therefore, the openness and accessibility of the internet provide the cyber intelligence community with a wide range of materials to gather and analyze intelligence information. Although this resource has been neglected in recent years, the way to confront the problem of cyber-terrorism may be to harness the private and academic sectors as informal research arms for the cyber-terrorism community.

***Keywords**: Cyber-Terrorism; Cyber Intelligence; Counter-Terrorism; jihadist site analysis; counterattacks.*

* المؤلف المراسل

مقــدمة

أثرت ثورة المعلومات وتكنولوجيات الاتصالات الجديدة بشكل كبير على كيفية ارتباط الدول والمجتمعات ببعضها البعض، وأكدت على العديد من التحديات التي تواجه الحكم والأمن الدوليين. ويشمل ذلك إنشاء منصات إلكترونية عالمية حيث ظهرت فواعل جديدة مؤثرة على أجندة السياسات، متجاوزة قنوات المشاركة القائمة، كما أدت إلى تغيير كيفية تعريف الدول القومية لمصالحها، وأسس قوتها وأمنها، وصعوبة تحكم الدول في نشر المعلومات والسيطرة عليها.

وبالتالي تزايد استخدام المنظمات الإرهابية والجماعات المتطرفة للفضاء السيبراني. إذ يوظف المتطرفون والإرهابيون شبكة الإنترنت لنفس الأسباب وبالطريقة نفسها التي نستخدمها جميعًا في الشبكة، من أجل التسويق، الاتصالات، التحكم والمراقبة، جمع المعلومات الاستخباراتية وتحليل البيانات. وقد ظل المحللون يؤكدون هذه الحقيقة منذ ما يقارب عقد من الزمان، مشيرين إلى أن وكالات الاستخبارات تتخلف باستمرار عن الإرهابيين في استخدام الإنترنت.

في الوقت الحالي، تركز وكالات الاستخبارات معظم جهودها على التهديد الذي تمثله حركة الجهاد العالمي. ومصطلح الجهاد العالمي في هذه الدراسة لا يشير فقط إلى الشبكة الفضفاضة للمنظمات والخلايا الراديكالية الخاضعة للتدقيق من قبل مجتمع الاستخبارات، ولكن أيضًا يشمل الحركة الاجتماعية الأكبر التي تتبنى أيديولوجية الجهاد. فبدون هذه الحركة الاجتماعية، لن يكون هنالك تهديد من قبل حركة الجهاد العالمي.

علاوة على ذلك، فبدون الإنترنت، ستبقى الجماعات المتطرفة التي تشكل كوادر الجهاد العالمي من المسلحين مجرد مجموعة من الخلايا المتفرقة والمعزولة على نطاق واسع والتي تدّعي بأن لها نفس الجذور التاريخية. وبالتالي لعبت شبكة الإنترنت دورا بارزا في عولمة حركة الجهاد. إذ أن شبكة الجهاد العالمي هي نتاج ثورة الاتصالات والمعلومات. باعتبار أن التواجد الجهادي على الإنترنت يمثل العقل المادي لحركة الجهاد العالمية.

وبالتالي، تنبع أهمية الموضوع من القضايا المهمة المثارة التي تتناولها هذه الدراسة خصوصا حول طبيعة واستخدام تكنولوجيا الإنترنت من قبل الحركات الإرهابية في حرب معلومات غير متماثلة، وكيف يتم تصور أفكار الإرهاب السيبراني، والطريقة التي تتم بها إعادة تحديد دور الدولة القومية في مواجهة واستباق الأخطار التي تهدد الأمن القومي. باعتبار أن انفتاح هذه الوسيلة وإمكانية

الوصول إليها يوفران لمجتمع الاستخبارات قاعدة مادية صلبة للعمل الاستخباراتي وتحليل المعلومات. ولكن تم إهمال هذا المورد في السنوات الأخيرة بسبب نقص الباحثين واللغويين المؤهلين لأداء هذه المهام. لذلك ستحاول هذه الدراسة معالجة الإشكالية التالية: كيف يمكن لمجتمع الاستخبارات السيبرانية المساهمة في مكافحة الإرهاب السيبراني؟. سيتم إتباع المنهج الاستنباطي لمحاولة استنتاج كيفية مواجهة الاستخبارات السيبرانية للإرهاب السيبراني، وتحديد مختلف الأدوار التي تقوم بها في هذا المجال.

فرضية الدراسة: كلما كان هناك توظيف عقلاني للفضاء السيبراني من طرف الاستخبارات الالكترونية، كلما كانت الفعالية في مكافحة الإرهاب السيبراني.

ولمعالجة إشكالية البحث، سيتم التطرق للعناصر التالية:

المحور الأول: توظيف الجماعات الإرهابية لشبكة الإنترنت

المحور الثاني: تطور الاستخبارات في الفضاء السيبراني.

المحور الثالث: تحليل الاستخبارات السيبرانية لمواقع ومنتديات الجماعات الإرهابية- الجهادية.

المحور الرابع: الهجمات المضادة للاستخبارات السيبرانية ضد الإرهاب السيبراني.

المحور الأول: توظيف الجماعات الإرهابية لشبكة الإنترنت

يعنى هذا الجزء بمحاولة فهم كيفية استخدام الفضاء السيبراني من قبل الجماعات والشبكات الإرهابية، التي تهدف إلى تسخير قدرات وإمكانات تكنولوجيات المعلومات والاتصالات الرقمية الجديدة للاستفادة من وفورات تعزيز القوة والسيطرة في هذا الفضاء. وفي هذا السياق، يمكن تحديد خمسة استخدامات أساسية لتكنولوجيا الإنترنت والتطبيقات المرتبطة بها من قبل الجماعات الجهادية المتطرفة، وتتمثل في:

أولا: جمع المعلومات

أدى ظهور الإنترنت، وخاصة تطوير شبكة الويب العالمية والمحتوى الرقمي المتعدد الوسائط الثري إلى منح الإرهابيين فرص كبيرة في متابعة أنشطتهم عبر الإنترنت، وتعزيز جهودهم للمشاركة في الدعاية والإعلان، وبالتالي في الحرب النفسية.[1] قد يظهر هذا المسعى في شكل مواقع ويب مدفوعة التكاليف، أو ممولة توفر معلومات تاريخية، أو في انتشار ملفات تعريف القادة على شبكات أو منصات وسائط التواصل الاجتماعي الشهيرة الأخرى أو في نشر البيانات، وغيرها من أنواع الدعاية

الأيديولوجية عبر الإنترنت.[2] كما أن المنظمات الإرهابية قد تستخدم أيضًا الإنترنت كأداة للحرب النفسية، باستخدام هذه الوسيلة لنشر المعلومات المضللة، وتقديم التهديدات، ونشر صور بصرية مزعجة أو شديدة الجاذبية.[3]

وبالتالي، توفر الإنترنت للجماعات الإرهابية مستوى غير مسبوق من السيطرة المباشرة في إدارة منظماتها، وعلى محتوى رسائلها، علاوة على توسيع نطاق كلاً من شرعيتها وقدرتها على التلاعب، وصياغة كيف تنظر إليها مختلف الجماهير المستهدفة وخصومها المعلنين.

ثانيا: التمويل وجمع التبرعات

تحتاج الشبكات والمنظمات الإرهابية إلى مستويات عالية من التمويل المستدام لتمويل ما يسمى عادة بمحرك النضال المسلح. فالموارد المالية تمثل هدفا حيويا للنشاطات الإرهابية. وبالنظر لبنية الإنترنت، والنطاق العالمي للمنصات الإلكترونية، وقدرتها على التواصل الفوري والتفاعلي، قد جعلتها وسيلة جذابة بالفعل لمجموعة من المنظمات السياسية غير العنيفة وفواعل المجتمع المدني كقناة لزيادة التبرعات والمعاملات المالية.[4] وبالطريقة نفسها تقريبًا، تسعى المنظمات والشبكات الإرهابية للحصول على تمويل لعملياتها وأنشطتها، سواء من خلال مواقعها الإلكترونية الفردية، أو من خلال تسخير البنية التحتية للإنترنت للتفاعل مع المجتمع بشكل عام، وتعبئة الموارد بشكل غير قانوني وفعال.

وفي هذا الصدد، قد تلجأ الجماعات والشبكات الإرهابية لتمويل الأعضاء وعملياتهم المتعددة إما من خلال التماس المباشر عبر مواقع إرهابية، حيث تطلب جماعة أو منظمة إرهابية الأموال من الجمهور مباشرة، كمتصفحي الويب الذين يزورون مواقعهم في شكل بيانات عامة تؤكد حاجة المنظمة إلى المال أو المزيد من الطلبات المباشرة، التي تحث المؤيدين والأتباع على التبرع فورا إما عن طريق تقديم تفاصيل الحساب المصرفي، أو عن طريق بوابة الدفع الإلكتروني.

كما تقوم باستغلال أدوات وهيئات التجارة الإلكترونية، حيث تنشئ الهيئات والأفراد المرتبطون بالإرهاب جبهات أعمال مرتبطة بالإنترنت، أو قائمة على الإنترنت كوسيلة لجمع الأموال لدعم أنشطتهم، أو إنشاء وتأسيس الجمعيات الخيرية لأغراض إنسانية، في إشارة إلى استخدام الجمعيات الخيرية كأدوات لجمع الأموال بشكل سري، إما عن طريق التسلل إلى فروع المنظمات الحالية لجمع

الأموال بشكل سري، أو عن طريق إنشاء جمعيات خيرية جديدة يُزعم أنها تدّعي تحقيق أهداف وأغراض إنسانية.[5]

ثالثا: إثبات الوجود وتعزيز التواصل الشبكي

يشير إلى الجهود التي تبذلها الجماعات الإرهابية لتسوية بناها التنظيمية، والعمل بطريقة أكثر لامركزية من خلال الاستفادة من البنى الوسيطة، بما من شأنه السماح للفواعل المشتتة بالتواصل بسرعة مع بعضها البعض وتنسيق الأنشطة وتنفيذ عمليات فعالة بتكلفة منخفض.[6] وتجدر الإشارة أن الهيكل الحالي للإنترنت لا يسمح بالاتصال السريع داخل المجموعة فحسب، بل يتيح أيضًا إنشاء روابط دائمة بين المجموعات.

وبالتالي، تعزز الإنترنت قدرات الإرهابيين على تحويل التسلسلات الهرمية الداخلية لمنظماتهم، وبناء روابط عالمية ضمن المساحات البديلة التي توفرها للتواصل والمناقشة والتفاعل القائم على الوسائط الإعلامية الثرية.[7] كما توفر الإنترنت للجماعات الإرهابية وسيلة يمكن أن يتفاعلوا بها بحرية، ودون الكشف عن هويتهم، بالإضافة إلى فرصة التطور واللامركزية.

رابعا: التجنيد والتدريب

تشتهر المنظمات الإرهابية بالتجنيد عبر الإنترنت على نطاق واسع ومتكرر، إذ تتوفر شبكة الإنترنت بصفة خاصة على طرق عديدة يمكن من خلالها للمجموعات والمنظمات الإرهابية أن توظفها لكي تعبئ بفعالية المتعاطفين من عامة الناس، وتجنيد أعضاء جدد يدعمون بنشاط أكثر أفكار التنظيم، أو النشاط الإرهابي المعني.

وفي هذا السياق، تعمل تقنيات الاتصالات الرقمية الجديدة والأنظمة المرتبطة بها على تسهيل عملية جمع المعلومات الكاملة عن المجندين المحتملين للوصول إلى المعلومات وفهمها. في حين أن الوصول والتفاعل العالميين على الويب يتيحان للمجموعات الإرهابية نشر الأحداث لعدد أكبر من الناس، مع إمكانية الاتصال بهم بشكل مباشر وسري. علاوة على ذلك، ومن من خلال استخدام منتديات النقاش والمنصات التفاعلية الأخرى، يمكن أيضًا لأفراد الجمهور - سواء كانوا مؤيدين أو معارضين لجماعة أو قضية معينة- الدخول في نقاش نشط مع بعضهم البعض.[8]

خامسا: استخراج البيانات ومشاركة المعلومات

يتمثل الاستخدام الرئيسي الآخر للإنترنت، والتكنولوجيات والتطبيقات ذات الصلة من قبل الإرهابيين، والمنظمات الإرهابية في استخدام وجمع البيانات والبحث عن المعلومات. وهذا التوظيف يشير إلى قدرة مستخدمي الإنترنت من جميع الفئات السكانية على الوصول إلى كميات هائلة من المعلومات، والتي كان من الصعب للغاية استرجاعها كنتيجة لتخزينها في تنسيقات ومواقع مختلفة على نطاق واسع. على عكس الاستخدامات الأخرى التي ذكرت سابقًا، فإن أنشطة جمع المعلومات من قبل الإرهابيين لا تعتمد فقط على تشغيل، وتطوير مواقع الويب الخاصة بهم كأدوات لإنشاء ونشر الدعاية، ولكن أيضًا تتضمن جمع وتقييم البيانات التي ساهم بها الآخرون في المكتبة الرقمية الهائلة أو الشبكة العالمية.[9]

كما قد يتخذ جمع الشبكات الإرهابية للمعلومات شكل استخراج البيانات، أو البحث عن المعلومات الذي يتضمن الاستخدام المتعمق، والواسع للإنترنت والموارد المستندة إلى الويب من قبل الإرهابيين، من أجل جمع وتجميع معلومات مفصلة حول قضايا موضعية محددة، أو فرص التمويل أو الأهداف المحتملة، أو مشاركة مباشرة للمعلومات، والتي تشير إلى إجمالي استخدام ممارسات جمع المعلومات العامة على الإنترنت من قبل الإرهابيين[10].

المحور الثاني: تطور الاستخبارات في الفضاء السيبراني

"ليست أقوى الأنواع التي تعيش، ولا هي الأكثر ذكاءًا التي تعيش. إنها الأكثر قدرة على التغيير"[11]، تشير هذه العبارة لـ "تشارلز داروين" (*Charles Darwin*) إلى وصفه لما يمكن أن يحصل عندما تحدث تغييرات سريعة في المكانة المتخصصة، التي أصبحت من خلالها الأنواع مرتاحة، مما يشكل تحديًا لبقائها. في الوقت نفسه ومن قبيل الصدفة، شهدت السنوات العشرين الماضية عدة تغييرات ثورية في بيئة وكالات الاستخبارات الغربية.

يصف هذا التغيير السريع بالتأكيد المتطلبات الاستخباراتية الجديدة بعد نهاية الحرب الباردة، وحل معاهدة وارسو، وإدماج أوروبا الوسطى في مجتمع الدول الغربية. والأكثر من ذلك، بعد هجمات تنظيم القاعدة على واشنطن ونيويورك في 2001/11/9 فإن الحاجة الملحة لمطالب الاستخبارات لمواجهة الإرهاب الدولي، وعدم الاستقرار تسببت في ضغط هائل على مجتمعات الاستخبارات في جميع أنحاء العالم.

ولكن خلال نفس الفترة، كان على جميع وكالات الاستخبارات أن تحاول في وقت واحد تكييف أنشطتها مع التغيرات العميقة التي أحدثتها الثورة الرقمية في بيئتها التكنولوجية. فنظرا لشعبية الإنترنت كوسيلة اتصالية، واختراع شبكة الويب العالمية والقدرة الرخيصة على تخزين البيانات الرقمية، فقد عملت على تغيير فرص الحصول على المعلومات الاستخباراتية، ولم تتوقف الفرص عن النمو منذ ذلك الحين خصوصا مع التطورات الحاصلة على مستوى المجال السيبراني.

ترتبط المجموعة الأخرى من التغييرات الحاصلة بالهياكل القانونية والسياسية التي تعمل ضمنها الآن معظم وكالات الأمن والمخابرات في النظم الديمقراطية، والمتعلقة بوجودها المعلن، وأنشطتها الخاضعة للقانون، ومواقع الويب التي توضح الغرض منها، وتوظيف الجيل التالي من الموظفين بما يتماشى مع مختلف التحديات والتهديدات السيبرانية.

وبحلول نهاية العقد الأول من القرن الحادي والعشرين، تمكنت مجتمعات الاستخبارات الأكثر تقدماً على الأقل من التكيف مع هذه التغييرات الحاصلة. إذ بدأت أجهزة استخبارات الإشارات على وجه الخصوص تتجه نحو الاستقرار بشكل مريح في مكان جديد ذو إنتاجية عالية، مستغلة بنشاط الوصول غير المسبوق إلى المعلومات الرقمية والاستخباراتية حول التنظيمات الإرهابية وأهدافها، لتقديمها لعملائها العسكريين والمكلفين بإنفاذ القانون، وغالبًا ما يتم ذلك في الوقت شبه الحقيقي ومع بدل القليل من الجهد.

ومع ذلك، فإن الكشف عن قضية "سنودن"* قد أظهر نظرة وطنية، ودولية غير مريحة ولم يسبق لها مثيل بخصوص النجاح الذي حققته وكالات المخابرات الأمريكية وحلفاؤها المقربون - بما في ذلك المملكة المتحدة- في التكيف مع العالم السيبراني. إذ أصبحت حماية المعلومات الشخصية من الاستغلال غير القانوني، ومشروعية وتناسب وكفاية تنظيم الوصول إلى الاستخبارات الرقمية وتبادل المعلومات الاستخباراتية، من القضايا الرئيسية على الصعيد الدولي. كما أن مدى ملاءمة التغييرات السابقة أصبحت تواجه تحديا خطيرا مرتبطا بالصلاحيات القانونية وترتيبات الحكم.

وفي هذا الاتجاه، تعيد العديد من الحكومات تقييم اعتمادها على شركات الإنترنت الأمريكية الكبرى، وكذلك اعتمادها على موردي تكنولوجيا المعلومات الصينيين، على غرار ما قامت به الحكومة البريطانية بشأن خطط شبكتها للجيل الخامس، حيث يجري التحقق من سلامة وأمن معدات شركة هواوي الصينية للجيل الخامس.[12] إذ أصبحت بعض أساليب الاستخبارات الرقمية

معروفة بشكل عام. كما أن شركات الإنترنت والتكنولوجيا الأمريكية نفسها مشغولة في طمأنة عملائها بأن بياناتهم ستصبح معرضة لخطر القرصنة وبهذا تشمل وكالات الاستخبارات التابعة لحكومتهم.

وبالتالي، يكمن وراء هذا الموقف الواقع التجاري المتمثل في أنه بالرغم من أن ما يقرب من 40٪ من سكان العالم لديهم إمكانية الوصول إلى الإنترنت، فإن معظمهم في العالم المتقدم. والنمو المستقبلي في الأعمال سيكون في الصين، وأماكن أخرى في آسيا وجنوب آسيا وأمريكا الجنوبية وأفريقيا. حيث يوجد اشتباه في هيمنة شركات المعلومات والتكنولوجيا الأمريكية، وعلاقاتها بالحكومة، وكذلك رغبة طبيعية لرؤية تنمية القدرات المحلية. في الوقت نفسه، لا شك أن معظم وكالات الاستخبارات والأمن في جميع أنحاء العالم تحاول تحديد كيفية سد فجوة واضحة في القدرات الإلكترونية مع الولايات المتحدة. وفي الوقت نفسه يشكو تطبيق القانون الغربي من أنهم لم يعودوا قادرين على جمع الأدلة كما كان من قبل وأن المخاطر على الجمهور آخذة في الازدياد.[13]

المحور الثالث: تحليل الاستخبارات السيبرانية لمواقع ومنتديات الجماعات الإرهابية الجهادية

أصبح الفضاء السيبراني يمثل القلب الحقيقي للجهاد العالمي، باعتباره المكان الذي يتم فيه تبادل الأفكار أو تحييد المعارضة أو استيعابها. علاوة على مناقشة الاستراتيجيات والتكتيكات. ومع أنه لا نتوقع العثور على مناقشات عبر الإنترنت للتخطيط الفعلي للهجمات الإرهابية، ولكن يمكننا أن نتعلم كيف تتشكل الأيديولوجيات والآراء في المجتمعات التي تشكل الدائرة الرئيسية للجهاد العالمي من حيث عدد المجنّدين.

فلجوء تنظيم القاعدة إلى الفضاء الإلكتروني ارتبط بتدمير معسكرات التدريب الجهادية في أعقاب هجمات 11 سبتمبر. مما اضطر قادة الحركة اللّجوء إلى الفضاء الإلكتروني كوسيلة للحفاظ على الاتصال في بيئة مشتتة جغرافيا. ومع ذلك، فإن استخدام الويب كموقع رئيسي للمناقشة لم يكن أمرًا ضروريًا فحسب، بل كان أيضًا مسألة اختيار. باعتبار أن حركة الجهاد العالمي ومنذ نشأتها اعتمدت اعتمادًا كبيرًا على مجتمعات الإنترنت لتعزيز أهدافها. لذلك كان لزاما على مجتمع الاستخبارات السيبرانية مواكبة هذه التغيرات من أجل ضمان متابعة ومراقبة وتحليل

المواقع والمنتديات الجهادية لفهم الأبعاد الأيديولوجية والإستراتيجية والتكتيكية المرتبطة بنشاط الجماعات الإرهابية والاستفادة من ذلك في عملية المواجهة.

أولا: تحليل البعد الأيديولوجي للإرهاب السيبراني

يعتبر وجود الحركة الجهادية على الإنترنت عنصرا أكثر وضوحا في النقاش الأيديولوجي. لأن شبكة الإنترنت ضرورية للتطور الإيديولوجي للحركة، وكذلك للنشر الفعلي لهذه الإيديولوجية على المجندين والمؤيدين المحتملين. إذ تتيح مثل هذه المناقشات -التي يمكن الوصول إليها بحرية- للمحللين نافذة على حركة الجهاد على مستوى "القاعدة الشعبية" ومستوى القادة (المستوى الأعلى). باعتبار أن كل من كبار الأيديولوجيين، وكذلك العملاء من المستوى المتوسط، والباحثين الجدد يكتبون على هذه المواقع الإلكترونية الجهادية.

وفي هذا الصدد، أشار كل من "داونينج"(*Downing*) "وميس"(*Meese*) من مركز مكافحة الإرهاب** *CTC* إلى وجود قدر لا بأس به من الأدبيات العقائدية الرئيسية للجهاد على شبكة الإنترنت، بالإضافة إلى الوثائق التي استولت عليها وكالات الاستخبارات في مختلف البلدان. إذ تتمثل إحدى أفضل الطرق للتعرف على تنظيم القاعدة في قراءة الأوراق والأدلة والمستندات الأخرى التي كتبها قادة التنظيم لتوجيه وضبط مشاريعهم. وقد تم الحصول على العديد من هذه الوثائق من قبل القوات العسكرية وقوات إنفاذ القانون. وبالتالي يمكنها أن توفر نظرة ثاقبة على الطريقة التي يعمل بها التنظيم. علاوة على ذلك، تعتبر المراجع الرئيسية الأخرى لتنظيم القاعدة متاحة بسهولة على شبكة الإنترنت العالمية.[14]

وهناك تشديد على أنه كلما تم توفير إمكانية الوصول إلى هذه المستندات، زادت الفوائد التي تعود على مجتمع مكافحة الإرهاب نتيجة لذلك. ونظرًا لأن أرشيف الوثائق الجهادية المترجمة أصبح متاحًا للمحللين، فإنها توفر نظرة ثاقبة على نقاط التنافر والتقاطع الاستراتيجي والإيديولوجي بين كبار القادة، والتي يجب فهمها بشكل أفضل من أجل استغلالها.[15] وما يثير الاهتمام هو أن مثل هذا التحليل يأتي بشكل متزايد من القطاعين الخاص والأكاديمي. من خلال جهود الباحثين المختصين في مجال دراسات الأمن السيبراني والحركات الإرهابية.

كما أوضح كل من "جاريت براكمان"(*Jarrett Brachman*) و"ويليام ماكانتس" (*William McCants*) في تقريرهما بعنوان: "سرقة قواعد لعبة تنظيم القاعدة" كيف يمكن استخدام

الدراسات الإستراتيجية الجهادية لتحديد واستغلال نقاط الضعف في الحركة الجهادية المتطرفة.[16] إذ يشير المؤلفان إلى أن مفتاح هزيمة الجهاد العالمي من وجهة نظر أيديولوجية هو فهم أيديولوجيتها من الداخل إلى الخارج من خلال تحديد: من هم الأيديولوجيون الرئيسيون، والقضايا المهمة التي توحد الحركة وتقسيمها. علاوة على ذلك، يلاحظ الباحثان أن القادة الجهاديين منفتحون وصريحون بشكل ملحوظ عند مناقشة من هم أكبر منافسين لهم، وما هي نقاط الضعف في علاقاتهم العامة.[17]

بمعنى آخر، قام أعضاء الحركة الجهادية المتطرفة بوضع قواعد اللعبة لفريقهم ومؤيديهم على شبكة الإنترنت. ومن خلال تنقيب وتحليل هذه النصوص التي تكشف عن رؤاهم التكتيكية والإستراتيجية، ستكون الولايات المتحدة قادرة على صياغة أساليب وتقنيات وإجراءات فعالة لهزيمة أتباع هذه الحركات.[18]

ثانيا: تحليل البعد الاستراتيجي للإرهاب السيبراني

تمت صياغة مصطلح "الدراسات الإستراتيجية الجهادية" من "قبل توماس هيغامر"(*Thomas Hegghammer*) و"برينجار ليا"(*Brynjar Lia*)، من مؤسسة الأبحاث الدفاعية النرويجية في أوسلو، للإشارة إلى كتب ومقالات عن مواطن القوة والضعف في الحركة الجهادية وتلك الخاصة بأعدائها.[19] حيث أشار "هيغهامر" إلى أن الإنترنت أصبح مكانًا حيويًا للخلايا الإرهابية لتنظيم وتبادل الأفكار حول التكتيكات بطريقة لا مركزية. إذ يسمح هذا المجال الافتراضي للخلايا النائمة بالعمل بشكل مستقل تقريبًا مستمدًا من إلهامها وتوجيهها التشغيلي من النصوص المنشورة عبر الإنترنت من قبل الأفراد في قارات أخرى.[20]

فمن خلال شبكة الإنترنت يمكن حقًا الحصول على المعلومات المفيدة من أجل التعرف على العلامات المبكرة للتطورات الإيديولوجية للجماعات الجهادية المتطرفة، والتي ستؤثر علينا لاحقًا عندما تنتقل من العالم الافتراضي إلى العالم الحقيقي عن طريق القيام بعمليات وهجمات ميدانية قد تؤثر علينا جسديًا.

وفي الوقت نفسه، أدى الاستخدام المتزايد للإنترنت كعقل مركزي للحركة الجهادية المتطرفة إلى جعل الحركة أكثر شفافية أمام المشاهدين والمتصفحين. باعتبار أن الفكر الإرهابي/الجهادي أصبح علنيا، وأكثر عرضة لعمليات القرصنة الإلكترونية. وبالتالي فمن الضروري قيام وكالات مكافحة

الإرهاب بجهود لخلق مناخ من الإرتياب على هذه المواقع من خلال نشر النصوص الاحتيالية وتخريب ثقة القراء والمتصفحين لمنشوراتها الجهادية المتطرفة.

ثالثا: تحليل البعد التكتيكي للإرهاب السيبراني

مثلما يستخدم الجهاد شبكة الإنترنت للمناقشة الأيديولوجية ونشر الأفكار، فإن المناقشات التكتيكية والمواد التدريبية متاحة أيضًا مجانًا على شبكة الإنترنت. ومن بين المعلومات الاستخباراتية التي يمكن الحصول عليها من هذه الوثائق المعلومات المرتبطة بالتكتيكات التي يرون أنها فعالة، والأسلحة التي يفضلونها ولماذا يستعملونها، وربما الأهم من ذلك، افتراضاتهم فيما يتعلق بفعالية هذه الأسلحة.

من بين الأمثلة على هذه الوثائق المتاحة على الإنترنت، الدراسة التي قام بها أبو مصعب السوري بتشخيصه لأسباب فشل الجهاد في العالم المعاصر، حيث أرجع هذا الإخفاق للأسباب التالية:[21]

- تعاون الحكومات المحلية في مواجهة الجهاد، وفشل الجهاديين في تنظيم هجمات متزامنة في البلدان المجاورة. يذكر السوري أنها عملت مع الأجهزة الأمنية في الأردن والعراق ودول الشرق الأوسط الأخرى لشل الحركة من منتصف الستينيات وحتى الثمانينيات.

- الفشل في النظر لتأثير الأقليات والقبائل الإثنية، أو احتمال أن تختار الدولة هؤلاء السكان.

- الفشل في تزويد المقاتلين الجهاديين بشعور بالارتباط الشخصي بقادتهم، أو بالرؤية القائلة بأنهم أيضًا قد يصبحون قادة.

- الفشل في الحصول على دعم شعبي من الأغلبية المسلمة، إذ يحدد السوري دور الدعاية باعتبارها حاسمة في هذا الصدد.

- عدم كفاية مشاركة رجال الدين المسلمين. إذ يقول السوري في هذا الصدد أن مشاركة رجال الدين ضرورية لتطوير جماعات الجهاد المحلية الجديدة.

* الدروس المستفادة من هذه الوثيقة بالنسبة لمجتمع الاستخبارات:

تتمثل إحدى طرق مواجهة تكتيك الجهاديين في مساعدة البدائل المحلية على إنشاء معاقلهم الخاصة في تلك المناطق التي تركتها قوات الأمن دون حماية. كما يمكن للجماعات العرقية المحلية أن تلعب دوراً في منع الفراغات الأمنية من التشكيل. وباعتبار أن الجهاديين ومجتمع مكافحة

الإرهاب يتنافسون على نفس الجمهور، ومع ذلك فإن الرأي العام أكثر أهمية للجانب غير النظامي في صراع منخفض الحدة. لهذا السبب، يجب التركيز بشكل أكبر على العمليات النفسية، والإعلامية في مجال التأثير من أجل تقويض الدعم الشعبي الذي تعتمد عليه الحركة الجهادية المتطرفة.

المحور الرابع: الهجمات المضادة للاستخبارات السيبرانية ضد الإرهاب السيبراني

تعتبر المساعي التحليلية لنشاط الجماعات الإرهابية على شبكة الإنترنت من قبل مجتمع الاستخبارات عاملا مساعدا على تحديد استراتيجيات، وآليات المواجهة من أجل كبح مختلف الأنشطة الجهادية المتطرفة.

أولا: المواقع الإلكترونية الإرهابية كمفتاح للفعالية التحليلية الاستخباراتية

يعد جمع المعلومات الاستخباراتية مكونًا رئيسيًا لأنشطة مكافحة الإرهاب السيبراني حيث أن المعلومات التي يتم الحصول عليها من خلال هذه القنوات غالبًا ما تؤدي إلى التحقيقات التي تؤدي إلى محاكمة المشتبه فيهم، أو تُستخدم كدليل في المحاكمة إلى الحد الذي يسمح به القانون الداخلي والقواعد الإجرائية.[22]

إذ يتم جمع المعلومات الاستخباراتية مفتوحة المصدر باستخدام تقنيات المراقبة المتخصصة عبر الإنترنت من مواقع الشبكات الاجتماعية، وغرف الدردشة، والمواقع الإلكترونية ونشرات الإنترنت التي تكشف عن أنشطة الجماعات الإرهابية (من بين العديد من العناصر الإجرامية الأخرى). ويمكن وضع هذه الوظيفة ضمن اختصاص وحدات مكافحة الإرهاب حيث يحصل الأفراد على تدريب وخبرة كافيتين للقيام بهذه المهمة.

ولكن يُنظر إلى التدريب المتخصص في بيئة الجرائم الإلكترونية على أنه تدريب أساسي لهذا الدور. كما تتطلب وظيفة جمع المعلومات الاستخباراتية أيضًا التقييم والتحليل لدعم تطوير الإستراتيجية في مواجهة التهديد الذي يمثله استخدام الإرهابيين للإنترنت. ومع ذلك، قد يؤدي تضارب المسؤوليات أو الأهداف بين وكالات الاستخبارات الوطنية إلى عرقلة التنسيق وترجمة المعلومات الاستخباراتية إلى خطط عملياتية فعالة.[23]

كما ذكرنا سابقا، يعتمد الإرهاب بشكل كبير على شبكة الإنترنت لنشر المعلومات من المستويات العليا، وكذلك للمناقشة على جميع المستويات. إذ يمكن اعتبار بيانات قادة الحركات الإرهابية مدخلاً مفيدًا للتحليل الاستخباراتي. فقد يعطي تحليل محتوى هذه العبارات بعض النوايا على

الرغم من وجود قدر كبير من الوعيد والمبالغة والتضليل في الكثير من هذه العبارات. لذلك قد يكون تحليل السياق ذو فائدة أكبر. إذ يمكن لهذا النوع من التحليل تحديد ما يعتقد الشخص الذي يدلي بالبيان أن متابعيه يريدون سماعه. وبالتالي، يمكن أن يوفر تحليل السياق قياس بعض اتجاهات الشارع. لذلك يعتبر مدخلا مفيدا للمؤسسات الاستخباراتية، فضلا عن المساعدة في تحديد تركيز جمع الاستخبارات التكتيكية.

في هذا الصدد يجب إيلاء اهتمام خاص للغة وتركيز وتصميم المواقع الجهادية. لإذ يمكن أن تخبرنا اللغات المستخدمة من الذي يعتبره الجهاديون جمهورهم الأساسي للمجندين. وفي بعض الحالات، يشير هذا الأمر إلى نقاط الضعف الملحوظة بين المجموعة المستهدفة. لكنه يمكن أن يخبرنا أيضًا من يريد الجهاديون أن يكونوا مجندين (من هم الأكثر استخدامًا لهم).

علاوة على ذلك، هناك نقطة أخرى جديرة بأخذها بعين الاعتبار متمثلة في الصور وتصميم المواقع. وكثيراً ما تكون هذه المواقع من عمل بعض أفضل وألمع عناصر الجيل الجديد من الجهاديين المتطرفين. لأنهم يعرفون جمهورهم، ويعرفون التقنيات التي من المحتمل أن تكون فعالة. ومع وضع هذا في الاعتبار يمكن القول أن التقليد هو أصدق أشكال مكافحة الإرهاب.

ولكن ليس فقط أسلوب التواصل هو الذي يمكن استنساخه. فهنا أيضًا، يمكن أن ينتج عن النهج التصاعدي فوائد لا يمكن التفكير فيها للاستجابات المؤسسية من القمة إلى القاعدة. إذ يمكن تجنيد مصممي الويب من الجمهور المستهدف للجهاديين المتطرفين من قبل مجتمع مكافحة الإرهاب لبناء هجوم مضاد. ويعتمد نجاح هذا النوع من الحملات المضادة على العمل في القواعد الشعبية على مستوى المجتمعات المحلية. فالحلفاء الرئيسيون لمجتمع مكافحة الإرهاب هم أولئك الذين تم اختيارهم للتجنيد من قبل الجهاديين أنفسهم، وبالتالي يتنافس الإرهابيون و مجتمع مكافحة الإرهاب على نفس الجمهور.

ثانيا: العمليات النفسية

أدى توسيع الفضاء الإلكتروني إلى إمكانية وجود مجموعات ليست جزءًا من الفرع العسكري الرسمي لأية دولة لتنفيذ هذه العمليات، على غرار دعاية التنظيمات الإرهابية على الإنترنت مثل "داعش" بالإضافة إلى مجموعات القرصنة مثل الأنشطة المجهولة عبر الإنترنت.

ويتضمن تطبيق العمليات النفسية باستخدام الفضاء السيبراني عدة طرق كاستخدام الفضاء الإلكتروني والقرصنة، بما في ذلك تشويه المواقع الإلكترونية، ونشر البيانات الحساسة أو المخترقة عبر الإنترنت من خلال منصات وسائل التواصل الاجتماعي وإمكانية استخدام الويب المظلم للكشف عن البيانات الحساسة التي يمكن نشرها بعد ذلك في الشبكة السطحية، واستخدام وسائل التواصل الاجتماعي للدعاية والتجنيد، وللتنديد بأسباب مختلفة، والتلاعب بالمعلومات كوسيلة لنشر كل من الأخبار الحقيقية والمزيفة، وكذلك لتفريق المحتويات المزيفة الأخرى (بما في ذلك الصور، والصوت والفيديو). لذا في الوقت الحاضر تعتبر العمليات النفسية جزءًا لا يتجزأ من الحرب الهجينة في ما يشكل العمليات النفسية السيبرانية.[24]

لقد عمل المحلل "ستيفن أولف"(*Stephen Ulph*) من مؤسسة "جيمستاون" (*Jamestown Foundation*) على مراقبة المنتديات الجهادية، مع التركيز بشكل خاص على أولئك الذين يتعاملون مع الوضع في العراق، باعتبارها ساحة التدريب الجديدة للحركة الجهادية. ففي جويلية 2005، لاحظ "أولف" كيف أن أخبار المناقشات الجارية بين الجيش الأمريكي، والمسلحين العراقيين تؤثر على عمليات التواصل، والتعليقات في المنتديات الجهادية.[25]

إذ أثارت الأخبار ملاحظات كبيرة بخصوص الضيق والاضطراب على المنتديات الجهادية. ففي المنتدى الالكتروني "قلعتي" (*www.qal3ati.net*) أين وقّع أحد الأعضاء على نفسه باسم الشريف الإدريسي، والذي أشار في 28 جوان، إلى تشابه هذا التطور المحتمل مع الوضع في أفغانستان، بقوله: "عندما استقبل الباكستانيون الإرهابيين الفارين من كهوف تورا بورا، لم يكن ذلك بقصد مساعدتهم ولكن من أجل بيعهم للأمريكيين. نسأل الله أن لا يحدث هذا لإخواننا في العراق".

يسلط هذا النوع من التعليقات الضوء على نقطة ضعف رئيسية كما يراها المتشددون الجهاديون أنفسهم، وهي تعرضهم للخيانة من قبل المجتمع الأوسع نطاقا الذي ينشطون فيه. وبطبيعة الحال، هذه المخاوف يمكن اللعب عليها بسهولة. ومن الحيل الواضحة لاستغلال هذا الشعور بالشك والارتياب يتمثل في تغذية وسائل الإعلام المحلية بأخبار الخيانات، ثم إلقاء اللوم في المنتديات ذات الصلة على عناصر داخل المنظمة، أو في المنظمات المنافسة.

وأشار "أولف" أيضًا إلى أن أنباء الاجتماعات بين قادة التحالف والمتمردين قوبلت بإنكار الكثير. وفي الوقت نفسه، تم نشر إنكار صارم على منتديات الإنترنت عن أي اجتماع من هذا القبيل بما في

ذلك من مجموعات قيل أنها شاركت في المحادثات. إذ ظهر أحد المنشورات في 30 جوان في المنتدى الالكتروني "قلعتي" الذي وقعه الجيش الإسلامي في العراق، وجيش المجاهدين، وجيش أنصار السنة. حيث أعرب "أيهم السامرائي" عن سخطه من أكاذيب وألاعيب أمريكا، وأشار بسرعة إلى الخطر الوشيك للمجاهدين الإسلاميين في العراق بقوله: "نواياها هي تقسيم صفوف المجاهدين ... لتقسيم العراقيين عن غير العراقيين .. لسحب البساط من تحت المجاهدين ... كيف يمكن أن يكون الأخ المسلم البطولي المجاهد في أي بلد أجنبي؟".[26]

وبالتالي، يمكن للمرء الحصول على قدر كبير من البصيرة في حالة انعدام الأمن للخصم من هذا النوع من المنشورات. من الواضح أن نشر منتدى واحد أو بيان عبر الإنترنت لا يعطي إشارة إلى علم النفس لمنظمة بأكملها. ومع ذلك، إذا تم رصدها بشكل مستمر، يمكن أن توفر الخلاصة الكاملة لهذه التصريحات إحساسًا حقيقيًا بالحالة النفسية للخصم.

لذلك، فالعمليات السيبرانية تعتبر كأدوات مهمة يمكن من خلالها توليد الآثار النفسية من خلال نقل معلومات ومؤشرات مختارة لتنظيمات الإرهاب السيبراني للتأثير على عواطفهم، ودوافعهم، والتفكير الموضوعي، وفي نهاية المطاف تغيير السلوك، فيصبح عناصر التنظيمات الجهادية المتطرفة أقل كفاءة وفعالية في أداء مهامهم السيبرانية الخاصة بهم.[27]

ثالثا: مكافحة التجنيد والدعاية

تعتمد حركة الجهاد العالمي مثل أية حركة اجتماعية كبرى على قاعدة واسعة من الدعم، باعتبار أن الرأي العام الإيجابي من داخل دوائره أمر لا بد منه ليس فقط لجلب المجندين الجدد إلى كوادره، ولكن أيضًا لحشد الدعم لأنشطته الأقل وضوحًا التي تحركها الأهداف.

وإذ تمثل الوحدة والانسجام الاجتماعي إحدى القيم الرئيسية للمجتمعات المتشبعة بالفكر الجهادي. فمن المحتمل أن يُنظر إلى أي شخص بأنه عدو الصالح العام لأنه يزرع الخلاف، أو يعرض النظام العام للخطر بغض النظر عن قيمة ونبل أهدافه. كما لاحظ "براكمان" (*Brackman*) و"ماكانتس" (*McCants*) أن الرأي العام الإيجابي ضروري لجذب الناس للانضمام إلى الحركة أو دعمها.

وبالتالي فإن الدعاية الفعالة أمر حاسم لنجاح الحركة الجهادية. وعلى العكس من ذلك، تنخفض شعبية الحركة عندما يُنظر إليها على أنها تهاجم إخوانها المسلمين، مما يتسبب في اضطراب

عام، أو إتلاف الصناعات الوطنية الحيوية، أو الانخراط في الطائفية.[28] ويشيرون إلى أن إحدى نقاط الهجوم المضاد الفعالة لمجتمع الاستخبارات تتمثل في تسخير قوة تأثير صور الهجمات الجهادية المتطرفة التي قتلت أطفالا مسلمين، من أجل تحويل الرأي العام الإسلامي ضد الجهاديين بطريقة غير مباشرة.[29]

ومع ذلك، يشير الباحثان إلى أن أي حملة من هذا القبيل يجب أن تدار بشكل كبير من الخلف وبالوكالة. وقد يضاف إلى ذلك أن الحملة المؤسسية لا يمكن أن تتمتع بنفس القوة أو الوصول إلى حملة "القاعدة الشعبية" الحقيقية بين الجهات المستهدفة المحتملة للخصم. وبالتالي عندما نكون قادرين فقط على إلهام الفاعلين المحليين للانضمام إلى المعركة سيكون مثل هذا الهجوم الإعلامي المضاد فعالًا حقًا. فالحملة التي ترعاها الحكومة بغض النظر عن مدى إدارتها بمهارة، لا يمكن اعتبارها بديلاً عن مشاركة المدونين المحليين والإعلاميين والمعلقين.

رابعا: تقويض الثقة

من خلال المقالات المتوفرة على الإنترنت فيما يتعلق بتدريب الناشطين، يمكن التعرف على المجالات التي تعتبرها الحركة الجهادية نفسها نقاط ضعف، ومن الأفضل استغلالها. على سبيل المثال، تم نشر عدد من المقالات كملصقات في منتدى إحدى الجماعات الجهادية محذرة من اعتراض رقمي محتمل، واقتراح طرق للتغلب على المشكلة واحتوائها.

وفي حالات أخرى، يمكن أن يشير الجدل الداخلي إلى انقسامات محتملة داخل الحركة الإرهابية، أو إلى نقص أو افتقار ملحوظ للقيادة. بالإضافة إلى ذلك، يمكن لهذه الأنواع من الجدل أن تُظهر القضايا الأكثر أهمية للجهاديين أنفسهم.

في الواقع، أدى اختراق أجهزة مكافحة الإرهاب للمنتديات الجهادية المتطرفة إلى اعتقال عدد من الشخصيات الرئيسية، على غرار ما حدث في السعودية بعد الهجوم الإرهابي لتنظيم القاعدة ضد منشأة "أبقيق" النفطية***، إذ شنت قوات الأمن السعودية غارات في جميع أنحاء البلاد واعتقلت متشددين إسلاميين. وفي 29 مارس 2006 تم القبض على 40 شخصاً يشتبه في أنهم أعضاء في تنظيم القاعدة في اعتقالات متزامنة، ونصف هؤلاء يشتبه في أنهم ساعدوا مالياً في الهجمات الإرهابية ونشر مواد أيديولوجية جهادية على الإنترنت.[30] من المؤكد أن اعتقال جهادي الإنترنت

سيئي السمعة كان بسبب الافتقار الشائع إلى حد ما للاهتمام بالإجراءات الأمنية الأساسية على الإنترنت من قبل الإرهابيين.

ومن النتائج المهمة لهذه الأحداث هو عدم الثقة والارتباك الذي يكثر في المنتديات الجهادية في أعقابها. فخلال النصف الأول من عام 2005، لاحظ "ستيفن أولف" وباحثون آخرون في معهد جيمستاون سلسلة من التحذيرات والنقاشات التي ظهرت في المنتديات الجهادية، مفادها أنه لا ينبغي للمشاركين في المنتدى دخول مواقع معينة، ولا حتى كزائر خوفًا من أن يتم التعرف عليهم من قبل المخابرات. وتناولت المناقشات صحة بعض المنتديات الجهادية، أو مديري الموقع أو المشاركين الذين يشتبه في أنهم جواسيس مخابرات مضادون.[31]

والنتيجة النهائية هي أن ثقة الجهاديين في قدرتهم على تفادي سيطرة الدولة عن طريق استخدام منتديات الإنترنت قد انخفضت بشكل كبير في الأعوام القليلة الماضية. على الرغم من الجهود الكبيرة المبذولة من طرف مديري المنتديات الجهادية لاستخدام الوكلاء وإخفاء هويات المشاركين، فقد لا يمكن استعادة هذا النوع من الثقة بكل سهولة.

خاتـــمة

من خلال العرض السابق تم التوصل للنتائج التالية:

- بالنسبة لاستعمال الجهاديين المتطرفين للإنترنت فهو سلاح ذو حدين، إذ كلما زاد اعتمادهم على الإنترنت،كلما زاد نطاق فعاليتهم وكفاءتهم، ولكن أيضا سيزيد مستوى ضعفهم وهشاشتهم.

- يمكن القول أن استخدام الإرهابيين للإنترنت من أجل القيادة والتحكم والدعاية وجمع المعلومات الاستخبارية ظل مهمشا من قبل المسؤولين عن إنفاذ القانون ووكالات الاستخبارات. وفي كثير من الأحيان، تم التنازل عن المجال السيبراني للإرهابيين، حيث يسعى مجتمع مكافحة الإرهاب للحاق بالركب وسط مزاعم بعدم الكفاءة، والقصور التنظيمي.

- وضّحت الأمثلة السابقة نوع الاستنتاجات التي يمكن استخلاصها من النصوص الجهادية والنقاشات بين المنظمات الإرهابية المتطرفة، وكذلك أمثلة للدروس العملية المستفادة. ففي نظر وكالات الاستخبارات، لا ينبغي الانتقاص من أهمية جمع المواد الخام للمعلومات المتاحة على الإنترنت من أجل تحليلها والاستفادة منها في عملية المواجهة.

توصيات واقتراحات:

- من أجل مواجهة الإرهاب السيبراني، ستحتاج وكالات الاستخبارات إلى تعلم الدروس التي علمها إياها الإرهابيون أنفسهم. وهذا يعني وضع نهج شعبي أساسي لمكافحة الإرهاب السيبراني، بايجاد جهاز مكافحة الإرهاب منظم بشكل أفقي ليحل محل أو على الأقل يكمّل النموذج الهرمي القديم (من أعلى إلى أسفل)، فتدفق المعلومات يجب أن يكون أقل رأسيًا وأكثر أفقيًا.

- فالمطلوب ليس فقط التحول التكنولوجي الحاصل حاليا، ولكن التحول التنظيمي أيضا ضروري لتطوير مكافحة الجماعات الجهادية المتطرفة. وفي الوقت نفسه يجب إعادة صياغة الهيكل التنظيمي لمجتمع مكافحة الإرهاب ككل للاستفادة الكاملة من الإنترنت كأداة لجمع المعلومات الاستخباراتية وكوسيلة للقيادة والسيطرة على الفضاء السيبراني.

- وبسبب طبيعة الإرهاب السيبراني كحرب نفسية، فإن القطاع الخاص هو الأكثر عرضة للخطر. في هذا السياق، من المهم أن يفهم مجتمع المخابرات المحترف هذا التحول من المبادرة الحكومية إلى المبادرة الخاصة، ويتبناها في الواقع. لأنهم بحاجة إلى التعلم للاستفادة بشكل صحيح من الجهود التي يبذلها الأكاديميون، وخبراء الإنترنت، والمحللون المستقلون.

- من المهم أيضًا أن يفهم مجتمع مكافحة الإرهاب آثار التغيير الذي أحدثته ثورة الاتصالات. إذ تُخاض معارك اليوم أكثر فأكثر في مجال الرأي العام وليس في ساحة المعركة. فمجتمع مكافحة الإرهاب يتنافس على نفس الجمهور مثل الجهاديين أنفسهم، وفي هذا النوع من الحروب، تعتبر الإنترنت ساحة قتال وسلاح في الوقت نفسه.

الهـوامش والمراجع:

[1] *Maura Conway, "Terrorism and the Internet: New Media - New Threat?", Parliamentary Affairs, Vol.59, Issue.2, 2006, p 284.*
[2] *Catherine A. Theohary and John Rollins, "Terrorist Use of the Internet: Information Operations in Cyberspace", CRS Report for Congress, Congressional Research Service, March 8, 2011, p 5.*
[3] *Francesca Bosco, "Terrorist Use of the Internet", in : Uğur Gürbüz (Edit), Capacity Building in the Fight Against Terrorism, IOS Press, Amsterdam, 2013, p 42.*
[4] *Nikos Passas and Samuel Munzele Maimbo, "The design, development, and implementation of regulatory and supervisory frameworks for informal funds transfer systems", in : Thomas J. Biersteker and Sue E. Eckert, Countering the Financing of Terrorism, Routledge Press, Oxford, 2008, p.p 177-178.*
[5] *Maura Conway, Op.cit, p.p 186-187.*
[6] *Ibid, p.p 187-188.*
[7] *Francesca Bosco, Op.cit, p 43.*
[8] *Ibid, p 41.*
[9] *Ibid, p,p 40, 43.*

[10] *Catherine A. Theohary and John Rollins, Op.cit, p 10.*

[11] للمزيد من التفاصيل حول هذه العبارة المتضمنة في نظرية أصل الأنواع "لتشارلز داروين" يرجى مراجعة:

- Charles Darwin, On the Origin of Species, The Pennsylvania State University, Pennsylvania, 2001.

* إدوارد جوزيف سنودن *Edward Joseph Snowden*: مواطن أمريكي ومتعاقد تقني وعميل موظف لدى وكالة المخابرات المركزية، عمل كمتعاقد مع وكالة الأمن القومي قبل أن يسرب تفاصيل برنامج التجسس "بريسم" إلى الصحافة. إذ سرب في يونيو 2013 مواد مصنفة على أنها سرية للغاية من وكالة الأمن القومي، منها برنامج "بريسم" إلى صحيفة الغارديان وصحيفة الواشنطن بوست.

[12] *Sam Trendall, Defence committee launches probe into Huawei and 5G security, public technology.net, 9 March 2020, see : https://www.publictechnology.net/articles/news/defence-committee-launches-probe-huawei-and-5g-security, accessed 11/03/2020.*

[13] *Intelligence and Security Committee of Parliament, Report on the Intelligence Relating to the Murder of Fusilier Lee Rigby, ISC, 2014, p 182.*

** مركز مكافحة الإرهاب CTC هو مؤسسة أكاديمية تابعة للأكاديمية العسكرية الأمريكية في ويست بوينت بنيويورك. توفر التعليم والبحث وتحليل السياسات في المجالات المتخصصة للإرهاب ومكافحة الإرهاب والأمن الداخلي والصراع الداخلي. تأسست بتمويل خاص في عام 2003، وهي تعمل تحت رعاية قسم العلوم الاجتماعية في الأكاديمية العسكرية الأمريكية.

[14] *Wayne A. Downing And Michael J. Meese, Harmony and Disharmony: Exploiting al-Qa'ida's Organizational Vulnerabilities, CTC Report, Combating Terrorism Center (CTC), New York, February 14, 2006, p 5.*

[15] *Ibid, p.p 2-3.*

[16] *Jarret M. Brachman, William F. Mccants, Stealing al-Qa'ida's Playbook, CTC Report, Combating Terrorism Center (CTC), New York , February 2006, p.p 5-6.*

[17] *Ibid, p.p 3-4.*

[18] *Ibid, p 5.*

[19] *Brynjar Lia and Thomas Hegghammer, "Jihadi Strategic Studies: The Alleged Al Qaida Policy Study Preceding the Madrid Bombings", Studies in Conflict & Terrorism, Taylor & Francis Inc, Vol.27, No.5, 2004, p 361.*

[20] *Ibid, p.p 370-371.*

[21] *Jarret M. Brachman, William F. Mccants, Op.cit, p.p 16-17.*

[22] *United Nations, The Use Of The Internet For Terrorist Purposes, United Nations, New York , 2012, p 70.*

[23] *Ibid, p 68.*

[24] *Carlos Pedro Gonçalves, Cyberspace and Artificial Intelligence: The New Face of Cyber-Enhanced Hybrid Threats, August 9th 2019, see : https://www.intechopen.com/online-first/cyberspace-and-artificial-intelligence-the-new-face-of-cyber-enhanced-hybrid-threats, accessed 24/03/2020.*

[25] *Stephen Ulph, Islamist insurgents seek to contain PR disaster: notes of defeatism, Terrorism Focus, Vo.2, Issue.13, July 13, 2005, see : https://jamestown.org/program/islamist-insurgents-seek-to-contain-pr-disaster-notes-of-defeatism/ , accessed 24/03/2020.*

[26] *Ibid.*

[27] *Herb Lin, On the Integration of Psychological Operations with Cyber Operations, January 9, 2020, see : https://www.lawfareblog.com/integration-psychological-operations-cyber-operations, accessed 24/03/2020.*

[28] *Jarret M. Brachman, William F. Mccants, Op.cit, p 19.*

[29] *Ibidem.*

*** شن تنظيم القاعدة في 24 فيفري 2006 عملية إرهابية ضد أكبر مصفاة نفط في العالم، متمثلة في منشأة أبقيق النفطية في السعودية. لكن تمكنت قوات الأمن السعودية من منع عناصر القاعدة من اختراق المحيط، وكان الهجوم فاشلاً إلى حد كبير. ومع ذلك، فإن حقيقة أن القاعدة استهدفت أكبر مصفاة نفط في العالم خلال فترة ارتفاع أسعار النفط القياسية تسببت في عدم الاستقرار في سوق الطاقة العالمية، مما أدى إلى تضخم أسعار النفط على الفور بعد الهجوم بـ 2 دولار للبرميل.

[30] *Michael Scheuer and all, Saudi Arabian Oil Facilities: The Achilles Heel of the Western Economy, Washington : The Jamestown Foundation, May 2006, p22, see : https://jamestown.org/wp-content/uploads/2006/05/Jamestown-SaudiOil_02.pdf?x60208, accessed 26/03/2020.*

[31] *Stephen Ulph, Op.cit.*