Cybrarians Journal
journal.cybrarians.org
E-ISSN 1687-2215

CC BY

Issue 63, September 2021 العدد 63، سبتمبر 2021

بناء واختبار بوابة معلوماتية لجمع وتحليل المحتوى ذي العلاقة بالإرهاب على الويب المظلم

إعداد

أحمد حسن الموكلي

قسم علم المعلومات، إدارة المعرفة

جامعة الملك عبدالعزيز ، السعودية

أ.د. حسن عواد السريحي

قسم علم المعلومات، إدارة المعرفة

جامعة الملك عبدالعزيز ، السعودية

المستخلص

هدفت هذه الدراسة إلى بناء واختبار بوابة (معلوماتية) تتعلق بجمع وتحليل المحتوى ذي العلاقة بالإرهاب على الويب المظلم، للاستفادة منها في مجال مكافحة الإرهاب، يمكن تطويرها مستقبلاً بشكل أوسع لدعم القرار الأمني والعملي، نحو الحد من الإرهاب بكافة أشكاله من جهة. وتكمن أهمية هذه الدراسة –على حد علمنا– في عدم وجود دراسات على المستوى العربي تناولت مثل موضوع الدراسة. وقد استخدم البحث منهج دراسة الحالة لدراسة الموضوع من جوانبه المختلفة ، وفي مسح آراء المتخصصين تم ذلك باستخدام أسلوب المقابلة، حيث صمم البحث استمارة أسئلة لهذا الغرض، شملت مجموعة من الأسئلة بلغ عددها (19) سؤالاً بطريقة النهاية المغلقة، وجاءت على جزئين: أسئلة عامة وأسئلة، رئيسة في موضوع الدراسة، إضافة إلى سؤالين مفتوحين عن المقترحات والملاحظات حول البوابة المعلوماتية. وقد توصلت نتائج الدراسة إلى بناء بوابة معلوماتية لجمع وتحليل محتوى الجماعات والمنظمات الإرهابية على الويب المظلم، واختبار وظائفها من خلال عينة الدراسة التي أظهرت النتائج أنها مناسبة جداً لفكرة مشروع البوابة وتطويرها. كما انتهت الدراسة إلى عدد من التوصيات، من أبرزها التوصية بتبني فكرة الدراسة، وذلك بتطوير نظام بوابة (المعلوماتية – معرفية) أوسع وأشمل، بحيث تصبح مشروعًا مؤسساتيًّا، تتبناه المؤسسات العلمية والأمنية على غرار مختبر أبحاث الذكاء الاصطناعي في جامعة اريزونا.

الكلمات المفتاحية: الويب المظلم– الويب العميق– الزاحف الإلكتروني.

Building and testing an information portal to collect and analyze terrorism-related content on the dark web

Ahmed Hassan Mawkili
Information Science Dept.,
King Abdulaziz University, Saudi Arabia

Prof. Hassan A. Alsereihy
Information Science Dept.,
King Abdulaziz University, Saudi Arabia

Abstract

This study aimed to build and test an information portal related to the collection and analysis of content related to terrorism on the dark web, to benefit from it in the field of combating terrorism, which could be developed in the future more broadly to support the security and practical decision, towards reducing terrorism in all its forms on the one hand. The importance of this study lies - to our knowledge - in the absence of studies at the Arab level that dealt with such a subject. The research used the case study method to study the topic from its various aspects, and in surveying the opinions of specialists this was done using the interview tool, as the research designed a questionnaire for this purpose, which included a group of (19) questions in the closed end method, and it came in two parts: and the main questions on the subject of the study, in addition to two open-ended questions about the suggestions and observations on the information portal. The results of the study concluded that an information portal was built to collect and analyze the content of terrorist groups and organizations on the dark web, and to test their functions through the study sample, which the results showed that it is very suitable for the idea of the portal project and its development. The study also concluded with a number of recommendations, the most prominent of which is the recommendation to adopt the idea of the study, by developing a broader and comprehensive (informational - knowledge) portal system, so that it becomes an institutional project, adopted by scientific and security institutions, such as the Artificial Intelligence Research Laboratory at the University of Arizona.

المقدّمة

ظلّت الجماعات والمنظّمات الإرهابية لسنوات طويلة تبحث عن وسيلة تستطيع من خلالها الوصول إلى الجماهير في كافة أنحاء العالم، وحينما ظهرت شبكة الإنترنت كانت هذه الجماعات والمنظمات كتنظيم القاعدة من أوائل التنظيمات التي استخدمتها ليس للترويج لرسالتها فحسب، وإنما استخدمتها لتحقيق مآرب أخرى تخدم مشاريعها الكبرى، فاستخدمتها في التجنيد والتمويل والتدريب وصناعة المتفجرات...، حيث استفادت هذه الجماعات والمنظمات من كلّ مرحلة من مراحل تطور الويب (الويب1، والويب2). ولأن الإرهاب الحديث بكافة أشكاله وتعدد مصادره يتفاعل وينصهر مع المتغيرات التقنية، حتى أصبح في حركة ديناميكية مستمرة ومتطورة وفق المستحدثات التقنية الحديثة التي فتحت المجال واسعًا أمام هذه الآفة الخطيرة، فبعد أن كانت الإنترنت بشكلها التقليدي تشكّل مصدر قلق لهذه الجماعات، بات بإمكان الأجهزة الاستخبارية في دول العالم مراقبتها وتتبُّع اتصالاتها، فاتجهت إلى الخيارات الأخرى المتاحة التي من شأنها أن تضلل هذه الأجهزة؛ فاستخدمت بعض البرامج والتقنيات التي تمكّنها من إخفاء هويتها مثل استخدام البروكسي (proxy) أو (vpn)، وحينما استطاعت بعض الأجهزة الاستخبارية ملاحقتها وتعقُّبها فإنها بدأت في الآونة الأخيرة بالهجرة نحو ما يُعرَف بالويب العميق (deep web) والويب المظلم (dark web)، واللذين يمتازان بعدد من الخصائص جعلت منهما بيئة جذب لهذه الجماعات، وأهم هذه الخصائص الأمان العالي الذي توفّره لمستخدميهما إجمالًا، واللذين يصعب معهما تعقُّب مستخدميهما فنيًا. ورغم التداخل بين المصطلحين أعلاه فإن موضوع هذا البحث يركِّز بشكل كبير على الويب المظلم (dark web)، والذي تحدث داخله الممارسات والنشاطات غير الشرعية. فقد وصف جيمي بارتلت، مدير مركز تحليل وسائل التواصل الاجتماعي والمتخصص في الحركات الاجتماعية في كتابه الشبكة المظلمة: داخل العالم الرقمي الصادر في 2015م ما يحدث داخل هذه الشبكات بالتهديدات، وأنها [أي: الشبكات المظلمة] "أدت إلى تزايد أنماط التهديدات، ومن أبرز التهديدات التي أشار إليها: عمليات الاغتيال السياسي: وهي المهمة التي يقوم بها البعض في الشبكة المظلمة مقابل أجر مادي...والاستغلال الجنسي للقاصرين: حيث يعتبر نشر الصور والمقاطع الإباحية هي النشاط أو التطبيق الأبرز للشبكة المظلمة...ونشر التطرف والإرهاب: فهناك صفحات متخصصة في نشر الأفكار العنصرية المتطرفة... والمواد المخدرة حيث إن هناك عديد من الأسواق التي تقوم بالترويج للمواد المخدرة، ويأتي على رأسها موقع طريق الحرير" (صحيفة الاقتصادية، 2016). ولا شك أن غموض هذه الشبكات دفع ببعض المختصين والمهتمين إلى محاولة سبر أغوارها رغم الصعوبات والتحديات التي فرضتها طبيعتها الفنية والتقنية.

ونظرًا لأهمية هذا الموضوع، فإن هذه الدراسة جاءت لبحث واقع استخدام الجماعات والمنظمات الإرهابية للويب المظلم من خلال التركيز على بناء نموذج مُصغَّر لبوابة معلوماتية في مجال الإرهاب لتكون أساساً لبوابة (معرفية) أوسع وأشمل ، يمكن تطويرها مستقبلًا لدعم القرار الأمني والعلمي نحو الحدّ من الإرهاب بكافة أشكاله.

مشكلة الدراسة

ما إن ظهرت الإنترنت إلا وكانت الجماعات والمنظمات الإرهابية كتنظيم القاعدة وداعش من أوائل التنظيمات التي استخدمتها ليس للترويج فقط لرسالتها، وإنما استخدمتها لتحقيق مآرب أخرى تخدم مشاريعها الكبرى كالتجنيد والتمويل والتدريب وصناعة المتفجرات... ولأن هذه الشبكة السطحية من الإنترنت أصبحت تشكِّل تهديدًا لهذه الجماعات بعد أن استطاعت كثير من الأجهزة الأمنية ذات العلاقة في بعض دول العالم تتبُّع هؤلاء وكشف هويات البعض منهم، وفك طلاسمهم الشبكية وتقديمهم للعدالة، فبدأ بعض من هؤلاء بالهجرة باتجاه ما يُعرَف بالويب المظلم (dark web)، والذي يمتاز بعدد من الخصائص جعلت منه بيئة جذب لهم، ولعل أهم ميزة وخاصية لمثل هذه الشبكات تكمن في الأمان العالي الذي توفّره لمستخدميها إجمالًا، والذي يصعب معه تعقُّب مستخدميها فنيًا. وما يهم في هذه الجزئية هو موضوع الويب المظلم (dark web)، والذي تحدث داخله الممارسات والنشاطات غير الشرعية، ومن بينها دعم الإرهاب والتطرف. وهذه الدراسة ستركز بشكل كبير على بناء نظام معلوماتي خاص بجمع وتحليل محتوى الجماعات والمنظمات الإرهابية على الويب المظلم من خلال الأدوات والتقنيات ذات العلاقة؛ للاستفادة منها في بناء نموذج مُصغَّر لبوابة (معلوماتية) كأساس لبوابة (معرفية) أوسع وأشمل في مجال الإرهاب، يمكن تطويرها مستقبلًا؛ لدعم القرار الأمني والعلمي نحو الحدّ من الإرهاب بكافة أشكاله من جهة. وبناءً عليه يمكن صياغة مشكلة البحث بشكل منهجي في السؤال الآتي:

ما هو النموذج المصغر لبوابة معلوماتية كأساس لبوابة معرفية أوسع وأشمل يمكن تطويرها مستقبلاً لدعم القرار الأمني والعلمي؟

أهمية الدراسة

تتطور التحدّيات الناجمة عن المستحدثات التقنية يومًا بعد يوم، وهذه التحدّيات تتطلب العمل على مواجهتها بشتى الطرق، ويُعَدُّ الإرهاب أحد التهديدات التي تطورت بتطور التقنية، فكلما وجدت هذه التنظيمات تقنيات حديثة تمنحها الأمان لممارسة أنشطتها الإرهابية هاجرت إليها، وآخر تلك المحطات بل وأهمها هي

(الويب المظلم). ولمواجهة هذه التهديدات سواء من قبل الجهات الأمنية، أو المؤسسات البحثية التي تهتم بدراسة ظاهرة الإرهاب، فإن ذلك يتطلب وجود أدوات وتقنيات متقدمة تعمل على جمع وتحليل المحتوى داخل هذه الشبكات، حيث يمكن من خلالها معرفة سلوكهم ومواقعهم وعلاقاتهم وآلية أعمالهم ونشاطهم ومصادر تمويلهم... ولا شك فإن بناء (نظام متكامل) والمتمثل في البوابة (المعلوماتية) قائمة على أنظمة دعم القرار ستساعد على اتخاذ الإجراءات الاستباقية، والمساعدة في الحصول على الأدلة الإلكترونية، والتنبؤ بالمخططات المستقبلية لهذه المنظمات والجماعات.

هدف الدراسة:

بناء واختبار نموذج مصغر لبوابة (معلوماتية) لجمع وتحليل محتوى الويب المظلم ذات الصلة بالإرهاب والتعرف على احتياجات هذا النظام.

التعريفات الإجرائية :

الويب المظلم (Dark Web) : يُعرَّف بأنه: "ذلك الجزء من الشبكة العميقة الذي أُخفي بشكل مقصود ولا يمكن الوصول إليه عبر محركات البحث التقليدية مثل قوقل، وهي النقطة الأعمق داخل شبكة الإنترنت" (المركز الوطني للابحاث واستطلاع الرأي، 2015).

وتُعرَّف تقنيات وأدوات تحليل محتوى الويب المظلم إجرائيًا بأنها: مجموعة من الأدوات والتقنيات المختلفة التي تساعد على الوصول إلى الويب المظلم، وجمع البيانات منه وتصنيفها وتحليلها، من خلال بناء نظام معلوماتي لهذا الغرض.

بوابة (معلوماتية) لجمع وتحليل المحتوى ذي العلاقة بالإرهاب على الويب المظلم

يُعرَّف الإرهاب (terrorism) بأنه: "كل فعل من أفعال العنف أو التهديد أيًّا كانت بواعثه أو أغراضه، يقع تنفيذًا لمشروع إجرامي فردي أو جماعي، ويهدف إلى إلقاء الرعب بين الناس، أو ترويعهم بإيذائهم، أو تعريض حياتهم أو أمنهم للخطر، أو إلحاق الضرر بالبيئة أو بأحد المرافق أو الأملاك العامة أو الخاصة، أو اختلاسها أو الاستيلاء عليها، أو تعريض أحد الموارد الوطنية للخطر (مجلس وزراء الداخلية العرب، 1998). كما يُعرَّف الإرهاب الإلكتروني (electronic terrorism) بأنه: "هو العدوان أو التخويف ماديًا أو معنويًا للإنسان، وذلك باستخدام الوسائل الإلكترونية، سواء كان هذا التهديد صادرًا من دول أو من منظمات وجماعات إرهابية" (جندل، 2014، 45).

وبناءً عليه يمكن تعريف تطوير بوابة (معلوماتية) ذي علاقة بالارهاب على الويب المظلم إجرائيًا بأنها: بوابة معلوماتية قابلة للتطوير، بهدف جمع وتصـــنيف وتحليل محتوى الويب المظلم ذي العلاقة بالجماعات والمنظمات الإرهابية.

الإطار النظري للدراسة

وجدت الجماعات والمنظمات الإرهابية في شبكة الإنترنت ملاذًا آمنًا وبيئة استثنائية لممارسة نشاطاتها المختلفة نحو تحقيق أهدافها، حيث تنوّعت وتعدّدت هذه الأنشطة والممارسات من خلالها ما بين عمليات التجنيد والتدريب والتواصل وتبادل المعلومات والدعائية الإعلامية والتمويل... ولأن البيئة الإلكترونية بطبيعتها بيئة معقّدة ومتطوّرة، يصعب السيطرة عليها في المجمل، فقد استطاعت هذه الجماعات والمنظّمات خلال السنوات الماضية أن تتماهى مع هذه التقنيات، فتطوّرت أعمالها وفقًا للتطورات التقنية المتوالية، ومارســـت هذه الجماعات من خلالها كافة أعمالها الإرهابية، بدءًا من استخدام مواقع الويب1 والويب2 والشبكات المظلمة، فتم استغلالها أسوأ استغلال، وحقّقت بعضًا من أهدافها في الإخلال بالأمن والسلم الدوليين. وبدأت الجهود الدولية تتضافر لمواجهة هذا الإرهاب الناشئ غير التقليدي، حتى ظهرت مصطلحات تتماهى مع هذا النوع الجديد من الإرهاب، ومن تلك المصطلحات مصطلح: "الإرهاب الإلكتروني"، و"الإرهاب السيراني أو الافتراضي"، "والإرهاب الشبكي"... وبين هذا وذاك ظلّت وما زالت الجماعات والمنظمات الإرهابية تستثمر وتستغل كافة إمكاناتها وطاقتها؛ للاستفادة من العالم الافتراضي في تنفيذ أجندتها المختلفة، وقد استطاعت خلال السنوات الماضية أن تتصهر في هذه العوالم وتتطور بتطوراتها المختلفة.

الويب المظلم

يشير مصطلح الويب العميق لفئة من المحتوى على شبكة الإنترنت، لأسباب تقنية مختلفة لم يتم فهرستها من قبل محركات البحث التقليدية، وبالتالي لن تكون المعلومات في المتناول من خلالها، ويشـــمل محتوى الويب العميق الشـــبكات الداخلية كتلك الموجودة في الشـــركات والوكالات الحكومية، والجامعات، وقواعد البيانات التجارية، مثل: Lexis Nexis أو WESTLAW ... بينما الويب المظلم هو جزء من الويب العميق تم إخفاؤه عمدًا، وهو مصطلح عام يصف مواقع الإنترنت الخفية التي لا يمكن للمستخدمين الوصول إليها دون استخدام برنامج خاص... (Finklea, 2017,2). وتكاد تنحصـــر الفروقات بينهما في إطار الجزء من الكل أي: الويب المظلم جزء من العميق، وهذا –بحسب ما نرى – ليس كل شيء، فهناك جانب آخر يتعلّق بمشروعية نشاط كل منهما، وهو ما أشارت إليه إحدى الدراسات التي ذكرت أن غالبية صفحات الإنترنت العميق غير المفهرسة هي

مشـــروعة لكنها مخفية من محركات البحث، بينما صـــفحات الويب المظلم على الأغلب هي لنشـــاطات غير مشـــروعة (Recorded future and Brookcourtsolutions, 2017,4). أما الويب المظلم كمصـــطلح فقد تفاوتت تعريفاته بين الجانب الفني المتعلق بالوصـــول إلى الويب المظلم، وبعضـــها ركزت على محتوياته غير القانونية؛ فقاموس (Decryptionary) يُعرِّف الويب المظلم بأنه: جزء من الإنترنت الذي لا يمكن رؤيته إلا بواســـطة برامج خاصـة تسـمح بإخفاء الهوية، ويوفر معلومات وخدمات غير قانونية (Decryptionary,2000). كما عرَّفه قاموس (Your Dictionary) بأنه: مجموعة من مواقع الويب التي يمكن عرضها بشكل عام على الرغم من إخفاء عنوان (IP) لخادم موقع الويب... كما أضـاف القاموس تعريفًا أكثر خصـوصـية أُطلِق عليه تعريف الكمبيوتر، ووصـفه بأنه: مجموعة من البرامج والخوادم المسـتخدمة لتوزيع الموسـيقا والفيديو وغيرها من المواد المحمية بحقوق الطبع والنشـر بشـكل غير قانوني (Your Dictionary, 2018). وهذا التعريف –بحسـب ما نرى – ضـيق جدًا، فجل ما يوجد على الويب المظلم غير قانوني من خدمات وسـلع وانتهاكات أخلاقية وسـرقات... وليس حكرًا فقط على ما يتعلق بحقوق النشـر والملكية الفكرية. وهناك من يصـف الويب المظلم بأنه: مجموعة من المواقع التي هي مرئية علنًا ، لكن يتم إخفاء عناوين بروتوكول الإنترنت من الخوادم التي تعمل عليها. وهذا يعني أن أي شـخص يمكنه زيارة موقع ويب داكن، ولكن قد يكون من الصـعب جدًا معرفة مكان اسـتضـافته (GREENBERG, 2014). ومن هنا فإن الويب المظلم لا يخرج في مفهومه العام عن المحتوى المتوفر داخل هذا العالم المظلم، ومشـــروعية هذا المحتوى من عدمه، إضـــافة إلى آلية الوصـــول إلى هذا المحتوى التي تتطلب برامج غير تلك المســـتخدمة في الويب السطحي.

استخدام الويب المظلم من قبل الجماعات والمنظمات الإرهابية

الجماعات والمنظمات والمتعاطفين معهم لا تتوانى البتة في اسـتخدام كل ما يحقّق لها أهدافها وطموحاتها عبر الشبكات والوسائط التقنية الحديثة، لذلك يعدّ الويب المظلم من أفضـل الخيارات وأكثرها أمنًا لممارسـة بعض أنشطتهم، خصوصًا تلك التي تتعلق بتأمين اتصالاتهم، وتمويل أنشطتهم وشراء احتياجاتهم، فـ "لم يعد الإرهابيون في الوقت الحالي بحاجة إلى خدمات وســـائل الإعلام التقليدية؛ لتوثيق وبث جرائمهم التي تغذّيها الكراهية، بل إنهم بمســـاعدة الإنترنت وأدوات بث الفيديو المباشـــر يمكنهم بأنفســـهم القيام بذلك، وهذا ما فعله منفذ هجوم كرايسـتشـيرش، من خلال اسـتخدام شـبكات الإنترنت المظلم" (مركز المسـتقبل، 2019). وفي الوقت الراهن يكاد يقتصـر اسـتخدام الجماعات والمنظمات الإرهابية للويب المظلم في أنشـطة بعينها بعيدًا عن الأنشـطة التفاعلية التي تتعلق بالجماهير، والتي تؤدي إلى اســـتقطاب وتجنيد أتباعهم، فالإرهابيون عندما يبحثون عن الدعاية،

والدخول في جدول أعمال وسائل الإعلام والأجندة العامة، فإنها لن تذهب عميقًا في شبكة الإنترنت المظلمة، وسوف تذهب إلى شبكة الإنترنت السطحي، أما إذا كانوا مهتمين بما يريدون استهلاكه، واتصالاتهم الداخلية، وتنسيق الإجراءات، وجمع التبرعات باستخدام العملة الافتراضية كالبيتكوين، وشراء الذخيرة والأسلحة والمتفجرات، فذلك سيتم القيام به من خلال الويب المظلم (Hanson and Weimann, 2018).

وتشير كثير من التقارير التي رصدتها الأجهزة الاستخبارية الدولية إلى هجرة بعض هؤلاء إلى الويب المظلم، حيث الأمان الذي يبحثون عنه حتى وإن اقتصرت أهدافهم في الوقت الراهن على عمليات التواصل والتمويل، وكانت دراسة نشرت في عام 2011 ورد فيها أن شبكة Darknet لديها أكثر من (50000) موقع و(300) منتدى للمنظمات الإرهابية (Rosner,London, and Mendelboim, 2013). الجدير بالذكر أن الدلائل والمؤشرات حول استخدام هذه الجماعات للويب المظلم بدأت في عام 2013م. حينما وجد مكتب التحقيقات الفيدرالية محادثات مسجلة مع أحد الإرهابيين الذين تم القبض عليهم، وقد كانت هذه المحادثات بين كل من "أيمن الظواهري" زعيم تنظيم القاعدة، و"ناصر الوحيشي" زعيم تنظيم القاعدة في اليمن، على الشبكة المظلمة، حيث أعلنت وزارة الخارجية الأمريكية عن إغلاق عشرين سفارة أمريكية في دول مختلفة، تبعتها دول غربية بإغلاق سفاراتها مثل: فرنسا، وبريطانيا، وألمانيا (Rosner,London, and Mendelboim, 2013).

كما أعربت القيادة الأمريكية عن قلقها إزاء التغلغل المتزايد للمنظمات الإرهابية فيما يُسمَّى بالويب المظلم، حيث صرّحت قيادة الأمن السيبراني في الولايات المتحدة الامريكية من أن أنشطة داعش على شبكة الإنترنت المظلمة تعزّز قدرتها على الحفاظ على نفسها ماليًا، وكذلك تحسين فاعليتها التشغيلية على أرض الواقع Berton, (2015,1). لذلك بادرت هذه الجماعات سواءً التنظيمات أو المتعاطفين معها إلى استخدام الويب المظلم حتى وإن لم يكن بالفاعلية نفسها التي كانت عليها في الويب السطحي خصوصًا شبكات التواصل الاجتماعي، فبعد هجمات باريس في نوفمبر 2015 تحول تنظيم داعش إلى الويب المظلم؛ لنشر أخباره ودعايته في محاولة منه لحماية أتباعه... كما قامت مجموعة تابعة لتنظيم القاعدة تُسمَّى (فريق الأقصى لتكنولوجيا المعلومات) في ديسمبر 2015 بتوزيع دليل بعنوان: إرشادات أمان متصفح (TOR)؛ لضمان الاتصال بالإنترنت (Weimann, 2016,41). والمعروف أن متصفح (تور TOR) هو المتصفح المستخدم في الوصول إلى الويب المظلم، وقد دأبت هذه الجماعات والمتعاطفين معها إلى إرشاد أتباعهم نحو الاستخدام الآمن حتى في الإنترنت السطحي، بل إنها تجاوزت في ذلك إلى إنشاء برامج اتصال آمنة خاصة بهذه الجماعات، كما هو الحال مع برنامج (أسرار المجاهدين) للتراسل الآمن الذي أنشأته الجبهة الإعلامية الإسلامية العالمية، وهي إحدى الأذرع الإعلامية لتنظيم القاعدة. ولأنها مصدر الأمان لهذه الجماعات فقد بدأت تتقاطر عليها، وقد تصبح في يوم من الأيام

المرتع الخصـــب لها. أما اســـتخدام الويب المظلم أو الشـــبكة المظلمة أيًا كان مســـماها من قبل الجماعات والمنظمات الإرهابية والمتعاطفين معهم، فهي لا تختلف كثيرًا عن أغراض وأهداف استخدامهم للشبكة السطحية، وهذا الاســـتخدام يكاد يتمحور في عمليات الاســـتقطاب والتجنيد، والدعاية والتدريب والتواصـــل وجمع الأموال، وإجمالًا فإن هناك عدد من الاتجاهات بهذا الشأن، وهي على النحو الآتي:

- الإرهابيون الذين يســتخدمون التشــفير من أجل التخفي: حيث تشــير الدلائل إلى أن المجندين يســتخدمون شـبكة الإنترنت الخفية؛ للتخطيط لشـن هجمات إرهابية؛ لأن الكشـف عن طريق وكالات إنفاذ القانون يكون أقل احتمالًا.

- الإرهابيون الذين يســتخدمون شــبكة الإنترنت الخفية لأغراض التجنيد: قد تهدف الدولة الإســلامية (داعش) إلى جذب المتعاطفين المهتمين من الشــبكة الخارجية ومواقع التواصــل الاجتماعية إلى الخبايا الأكثر أمانًا في شبكة الإنترنت الخفية؛ لمزيد من التفاعل والتلقين.

- الإرهابيون الذين يستخدمون شبكة الإنترنت الخفية كمستودع للدعاية: إن إزالة المحتوى المتطرف والإرهابي من شــبكة الإنترنت الســطحية والخفية –خاصــة في ظل وجود برامج الذكاء الاصــطناعي التي تؤدي إلى عمليات إزالة جماعية يزيد من خطر خسارة الأدلة اللازمة لمحاكمة الأفراد الذين ينشرون المحتوى، أو الذين يقومون بتقديم دعم مـادي للمنظمـات الإرهابيـة، والكثير من المواد تعود للظهور مرة أخرى على شـــبكة الإنترنت الخفية.

- الإرهابيون الذين يستخدمون العملة المشفرة؛ للتهرُّب من الكشف وجمع الأموال:

يستخدم الإرهابيون عملات افتراضية لتجنُّب الكشف، ولجمع الأموال: يستخدم الإرهابيون مثل المجرمين العملة المشـفرة؛ لأنها توفر عدم الكشـف عن هويته في الإعداد المالي كما يفعل التشـفير لأنظمة الاتصـالات (Malik, 2018,IV).

الدراسات السابقة

حتى يقف البحث بشكل دقيق على الأدب المنشور المتعلق بموضوع الدراسة، فقد تم مسح عدد من قواعد البيانات ومحركات البحث ذات العلاقة، ولأن موضـوع الويب المظلم من المواضـيع الحديثة، فهناك الكثير حتى من المتخصصين لا يعرف عنه إلا الشيء القليل، فهو لا يزال في بداياته، خصوصًا على المستوى العربي، ولم يتم الوصول الى أي دراسة متخصصة تناولت موضوع الويب المظلم على المستوى العربي من قبل الجماعات

والمنظمات الإرهابية، بينما على مستوى الدارسات الأجنبية (الإنجليزية) فهناك بعض الدراسات التي تناولت موضوع الويب بشكل عام، ودراسات قليلة أخرى متخصصة حول موضوع هذا البحث المتعلق بتقنيات وأدوات تحليل محتوى الويب المظلم دراسة لتطوير بوابة معرفية في مجال الإرهاب، وكثير من هذه الدراسات قام بها الفريق المتخصص في هذا الشأن بمختبر الذكاء الاصطناعي بجامعة أريزونا. لذلك سوف يقدِّم البحث ما تمَّ التوصل إليه من الدراسات الأجنبية (الإنجليزية) التي تتعلق بموضوع البحث وفقًا للترتيب الزمني الأحدث ومناقشتها.

وفي دراسة أعدّها كل من Patil Manwade and Landge (2012):

هدفت هذه الدراسة إلى بناء نظام خصائص الويب المظلم (dark web attribute system)، وقد ركّز هذا العمل المقترح على تحديد وتحليل سمات صفحة الويب الجديدة. ويهدف إلى مقارنة مواقع إرهابية/متطرفة مختلفة بمواقع حقيقية، وبالتالي إعداد مقاييس يمكن استخدامها كذلك لتحديد المواقع الأخرى للجماعات الإرهابية/المتطرفة... كما يساعد هذا النظام على تحديد الجماعات التي تعتبرها مصادر موثوقة جماعات إرهابية/متطرفة. ومن أهم الاستنتاجات التي تم التوصل إليها بعد القيام بعمل تجريبي، بعد أن تم تحديد بيانات للمنظمات الإرهابية من تقارير الحكومة، مثل: مكتب التحقيقات الفدرالي، ووزارة الخارجية الأمريكية، ومراكز البحوث MEMRI وATC وما إلى ذلك. والزحف كذلك إلى URLS لتحليل الارتباط، وتحديد التشابه بينهما؛ تم تحديد سبعة وعشرين نوعًا من السمات لأغراض التحليل، وقد شكّلت خمس مجموعات السمة الرئيسة، وهي: سمة التطور التقني من خلال (قائمة التجميع، والنمط، والشكل، وإطار وجدول السمات...)، والتطور التقني المتقدّم من خلال (التجميع في الجافا سكربت، والسمات في السكربت). والبرمجة الديناميكية على شبكة الإنترنت (من خلال لغات البرمجة java وPHP وASP). وثراء المحتوى (من خلال الفلاش، صورة، الصوت، الفيديو ...)، والسمات التفاعلية على شبكة الإنترنت (حسب قائمة التجميع، والاتصال، والبريد الإلكتروني، والتعليق، والمؤتمرات المرئية، والتوظيف عبر الإنترنت...). كما وجدت الدراسة أن تحليل المحتوى يعطي المزيد من البصيرة عما هو في التطور التقني، وثراء المحتوى، في حين أن تحليل الارتباط يركّز على التفاعل في شبكة الإنترنت... كما أن استخدام الإرهابيين/المتطرفين للويب أكثر تركيزًا على ثراء المحتوى. كذلك فإن سمات أخرى مثل التفاعل على شبكة الإنترنت ... (Patil, Manwade and Landge, 2012,1816-1825).

كما قدم Abbasi, Fu and Chen (2010) دراسة بعنوان (A Focused Crawler for Dark Web Forums وفيها يقترح تصميم نظام زحف إلكتروني لجمع محتويات الويب المظلم بمساعدة الإنسان؛ للوصول إلى منتديات

الويب المظلم مع مميزات أخرى؛ كاسترجاع المعلومات، وتحديث المحتوى، وسهولة الوصول، ويخدم لغات متعددة، كما يشمل النظام على بروكسيات تساعد على الوصول إلى منتديات الويب المظلم. وقد أظهرت النتائج أن النظام حقق الوصول إلى الويب المظلم بنسبة (90%). (Abbasi, Fu and Chen, 2010, 1213-1231).

كما قدم Zhang, at el (2010) في مؤتمر (IEEE International Conference on Intelligence and Security Informatics) **دراسة** هي امتداد لدراسة سابقة في أرشفة الويب المظلم للجماعات الإرهابية والمتطرفة، وتوفير البنية التحتية البحثية للاستخدام من قبل علماء الاجتماع والمعلومات والكمبيوتر والمحللين السياسيين والأمنيين، وكان يحتوي هذا الأرشيف في وقته على ثلاثة عشر مليون منشور، وتسعة وعشرين من المنتديات الجهادية الدولية التي تستضيف ثلاثة مائة وأربعين ألف عضو، وتغطي مجموعة واسعة من المواضيع الاجتماعية والسياسية والثقافية والإيديولوجية والدينية، وهذه المنتديات التي جمعت لهذا المشروع هي باللغة العربية والإنجليزية والفرنسية والألمانية والروسية. ... (Zhang, at el, 2010,1-5).

كما أعد Qin,et al (2008) دراسة والدراسة منشورة عبر السلسلة المتكاملة لنظم المعلومات (IS2)، وقد حاول الباحثون من خلال هذه الدراسة الحصول على فهم شامل للويب المظلم، من خلال تطوير واستكشاف نهج شامل؛ لجمع ومراقبة محتويات الويب المظلم، وذلك بتوظيف تقنيات الزحف التلقائي لبناء مجموعات خاصة بالويب المظلم تغطي مواقع أنشأتها أكثر من (200) منظمة متطرفة دولية ومحلية، كما قاموا بتطبيق منهجية لتحليل محتوى هذه المواقع تسمى منهجية نظام سمات الويب المظلم؛ لتمكين التقييم الكمي للتطور التقني وفاعلية استخدام هذه المنظمات للإنترنت، وقد أثبتت النتائج فاعلية نظام تحليل الويب المظلم في دراسة استخدام المنظمات المتطرفة للإنترنت، فقد تم جمع أكثر من (1.7) مليون وثيقة ويب للوسائط المتعددة من حوالي (224) موقعًا أنشأتها الجماعات المتطرفة في كل من أمريكا الشمالية واللاتينية وبلدان الشرق الأوسط. (Qin,et al, 2008, 237).

كما نشر Abbasi and Chen (2007) دراسة أخرى في السلسلة نفسها والتي تهدف إلى دراسة تأثير المحتوى المنشور على منتديات الجماعات المتطرفة من خلال عينة من هذه المنتديات في كل من أمريكا والشرق الأوسط، كما شمل التحليل قياس وتصور أثر كثافة العنف والكراهية عبر هذه المنتديات، وعرضت الدراسة تصميم النظام المستخدم لتنفيذ تقنيات التحليل المؤثرة، كما قدمت وصفًا لأساليب التقييم والفرضيات المقترحة. أظهرت النتائج أن هناك مستويات متماثلة من التأثيرات ذات العلاقة بالكراهية، وعلى النقيض كثافة التأثير ذو العلاقة بالعنف، حيث أظهرت الدراسة ضعف كثافة تأثيره في منتديات الشرق الأوسط منها على المنتديات الأمريكية موضوع الدراسة. كما أظهرت الدراسة

أن منتديات الشرق الأوسط لها تأثير قوي على العلاقة بين العنف والعنصرية (Abbasi and Chen, 2007,285).

ومن الدراسات المبتكرة في هذا المجال الدراسة التي أجراها Zhou, Yilu, et al (2005) حيث اقترحوا في هذه الدراسة نظام إدارة المعرفة الذكي؛ لدعم اكتشاف وتحليل بيانات الويب المظلم التي أنشأتها الجماعات الإرهابية وبلغات متعددة، فقاموا بتطوير أسلوب منهجي؛ لتحديد جمع وتخزين تلك البيانات، كما اقترحوا بناء بوابة معرفية متكاملة من النص المتقدم وتقنيات التعدين، مثل: التلخيص، والتصنيف، والاسترجاع؛ وذلك لتسهيل اكتشاف المعرفة من مصادر الويب المظلم، وقد انتهت الدراسة إلى تأسيس مجموعة تجريبية عالية الجودة من مواقع الويب المظلم، غطت (444) موقعًا أنشأتها الجماعات الإرهابية في كل من أمريكا اللاتينية والشرق الأوسط والولايات المتحدة الأمريكية، إضافة إلى تنفيذ البوابة الإلكترونية على شبكة الإنترنت، والتي تسمح للباحثين والخبراء بالبحث والتصفح والتحليل بعدد من اللغات(Zhou, Yilu, et al,2005,1-14).

الإطار المنهجي للدراسة

منهج الدراسة

منهج الدراسة هو منهج دراسة الحالة لدراسة الموضوع من جوانبه المختلفة ولتطوير البوابة في مجال مكافحة الإرهاب على الويب المظلم كنموذج مُصغَّر لنظام جمع وتحليل محتوى الويب المظلم، التي تم بناء البوابة كأحد مخرجات الدراسة، واختبارها كحالة تستحق التطبيق والتطوير على مستوى أكبر وأشمل، وتم اختبارها عبر عرضها على مجموعة من الخبراء المتخصصين ومسح آرائهم عبر أداة المقابلة وقائمة الأسئلة، وهؤلاء الخبراء يُمثِّلون القطاع الأمني المعلوماتي، وتشتمل عناصر تقييم البوابة (المعلوماتية) على الآتي:

- سهولة إنشاء قاعدة بيانات متخصصة تتعلق بموضوع الإرهاب على الويب المظلم.
- دعم اللغتين (العربية، والإنجليزية).
- أدوات متنوعة لتحليل المحتوى.
- أدوات استرجاع.
- طرق متنوعة لعرض النتائج.
- مشاركة المعرفة.
- بحث مباشر في الويب المظلم.

مجتمع وعينة الدراسة

تنوُّع مجتمع الدراسة بتنوع أهداف البحث والمناهج العلمية لتحقيقها، حيث سيتم التركيز في هذه الدراسة على الممارسين والمتخصصين من العاملين في المجال الأمني والمعلوماتي ذوي العلاقة بمكافحة الإرهاب بوجه عام والإرهاب على الإنترنت برئاسة أمن الدولة في المملكة. أما عينة الدراسة المتعلقة باختبار البوابة (المعلوماتية) التي تم بناؤها بهذا الخصوص، فقد تم اختيار عينة (قصدية) صغيرة تتكون من عدد (16) من الممارسين للعمل الأمني والمعلوماتي بمهام مختلفة في مجالات مشابهة لموضوع الدراسة الحالية، حيث تم اختيار هذه المجموعة وفق مواصفات محددة مستوحاة من طبيعة عملهم ذات العلاقة بمكافحة هذا النوع من الإرهاب، عبر جمع وتحليل وتقييم هذا المحتوى الخاص بهذه الجماعات.

أدوات جمع البيانات

تم استخدم **استمارة أسئلة مقابلة:** وذلك لاختبار البوابة (المعلوماتية) وفق الآتي:

- استمارة الأسئلة الخاصة باختبار (البوابة المعلوماتية) التي صممت كنموذج مُصغَّر يمكن الاستفادة منها في مكافحة الجماعات والمنظمات الإرهابية، من خلال جمع وتحليل محتواها على الويب المظلم، فقد استخدمت أداة المقابلة (interview)؛ لجمع المعلومات حول النموذج المصغر للبوابة المعلوماتية التي تم بناؤها ذات العلاقة بمحتوى الجماعات والمنظمات على الويب المظلم، فأداة المقابلة هي الأنسب لتجميع آراء الممارسين والمتخصصين ممن لهم علاقة بموضوع الدراسة الحالية سواء على مستوى جمع المعلومات أو تحليلها؛ للوقوف على فعاليتها وجوانب القصور فيها. وقد اعتمد على أسلوب المقابلات غير المنظمة، من خلال بنائه استمارة تحتوي على مجموعة من الأسئلة (ذات النهايات المغلقة) مع سؤالين بـ(نهاية مفتوحة) عن الملاحظات والمقترحات حول البوابة (المعلوماتية)؛ لتخدم أهدافها بشكل أفضل، أو أي مشاكل تقنية إن وجدت في البوابة بشكل عام. وقد روعي عند إعداد الأسئلة أن تكون مباشرة ذات صلة بالهدف من الدراسة، كما تم صياغة الأسئلة بطريقة سهلة وواضحة تتناسب مع من تم مقابلتهم من المختصين. وقد تم إعداد الاستمارة أولا بإعداد مسودة استمارة؛ من أجل جمع المعلومات، ثم تم إجراء دراسة استطلاعية؛ للوقوف على وضوح الأسئلة وسهولتها وموضوعيتها. بعد ذلك تعديل الاستمارة وفق الملاحظات الواردة من عينة الدراسة. وأخيرا تم البدء في مقابلة من تم اختيارهم وجهًا لوجه.

الجدير بالإشارة هنا أن الاستمارة اشتملت على ثلاثة أجزاء رئيسة، هي:

أ- الجزء الأول: عبارة عن معلومات عامة، حيث اشتملت الاستمارة على عبارات تتعلق بـــ (الجنس، العمر، المؤهل العلمي، عدد سنوات الخبرة، طبيعة العمل)، وتم استخدام أسلوب الاختيار من متعدد.

ب- الجزء الثاني: اشتمل على (5) عبارات، ركّزت على واقع أفراد مجتمع الدراسة بالنسبة للويب المظلم.

ت- الجزء الثالث: اشتمل على (8) عبارات، ركّزت على تقييم البوابة المعلوماتية (راصد)، من حيث سهولة إنشاء قاعدة بيانات، والصلاحيات المعطاة للمستخدم، وسهولة أدوات البحث، وأدوات التحليل، والنتائج وطرق عرضها.

ث- الجزء الرابع: تكون من سؤالين مفتوحين، ركّز السؤال الأول على الاقتراحات التي يمكن إضافتها للبوابة؛ لتحقيق هدفها بشكل أفضل، وركّز السؤال الثاني على الملاحظات والمقترحات التقنية التي من شأنها أن تحسن أداء البوابة وترفع فاعليتها.

صدق أدوات الدراسة وثباتها

للتحقق من الصدق الظاهري الخاص باستمارة المقابلة تم عرض الاستمارة على ثلاثة من الخبراء المتخصصين؛ أحدهم متخصص في تقنية المعلومات، والآخران متخصصان في جمع وتحليل المعلومات؛ إذ طلب منهم تحديد وضوح الفقرات، وانتمائها للبعد المنتمية إليه، وسلامتها لغويًا، ومناسبتها لعينة الدراسة، وقد انتهى ذلك إلى حذف وإضافة ودمج بعض الفقرات، لتصبح الاستمارة في شكلها النهائي.

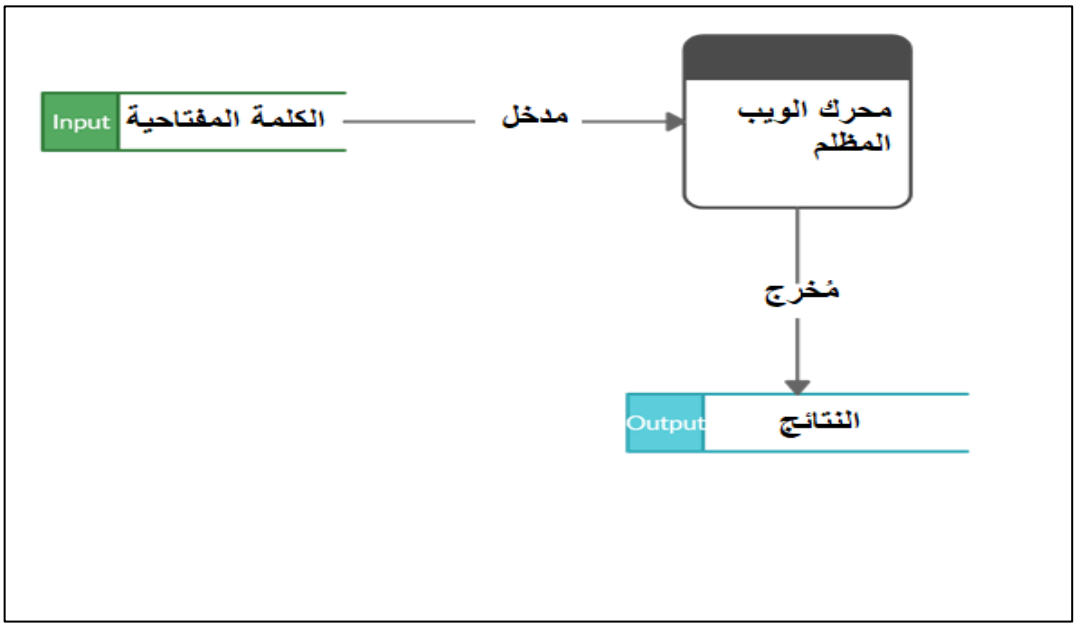
بناء البوابة المعلوماتية

بعد مراجعة الدراسات السابقة، والاطلاع على عدد من التقارير الاستخبارية في هذا المجال، كون الباحث الرئيسي فكرة كاملة عن مشروع البوابة معلوماتية التي أطلق عليها اسم (راصد) يمكن من خلالها، جمع وتحليل محتوى الجماعات والمنظمات الإرهابية على الويب المظلم. ولتنفيذ مشروع البوابة الاستعانة بمبرمج تقني لتنفيذه. حيث تم ذلك على مرحلتين وفق الآتي:

1- المرحلة الأولى طريقة عمل نظام البوابة المعلوماتية

بعد مناقشة مستفيضة مع المبرمج وبناء مسودات أولية لآلية نظام البوابة (المعلوماتية) تم تحديد عدة عمليات للنظام؛ للعمل على أكمل وجه، وهي على النحو الآتي:

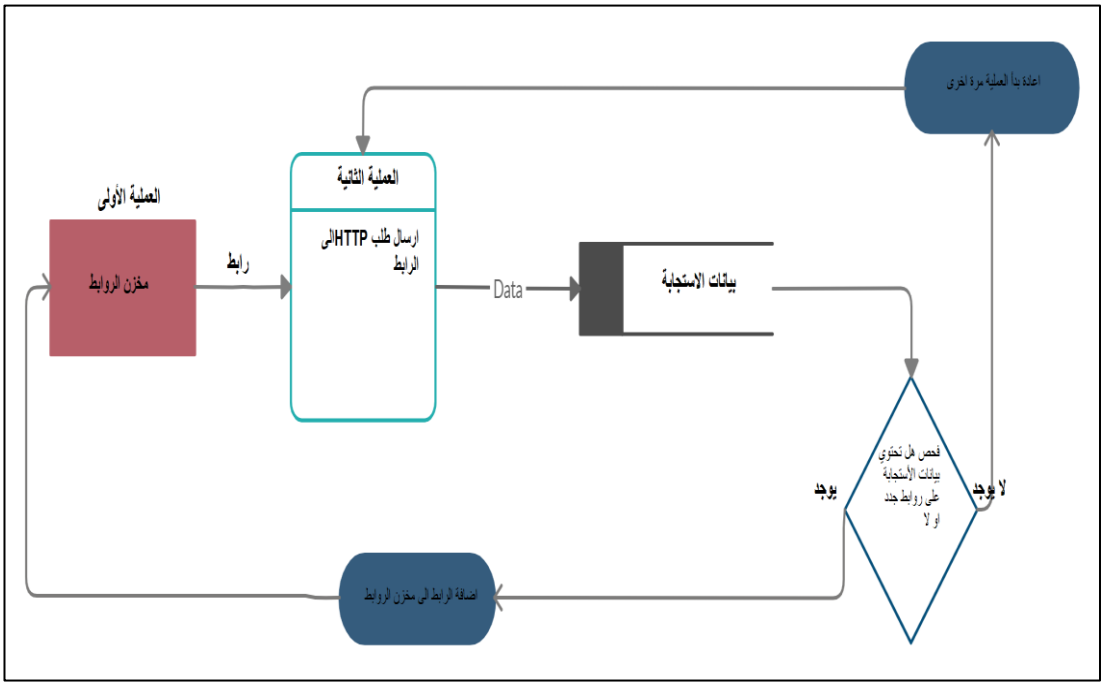
- **جمع المعلومات:** وفي هذه المرحلة يقوم الزاحف بالبحث عن الروابط، وتجميع كل البيانات الموجودة فيها، كما أنه يقوم في الوقت ذاته بالبحث عن البيانات الوصـــفية، حيث تتم عملية البحث عن الكلمة المفتاحية، وتجميع أكبر قدر من النتائج المتعلقة بها.



شكل رقم (1) عملية البحث

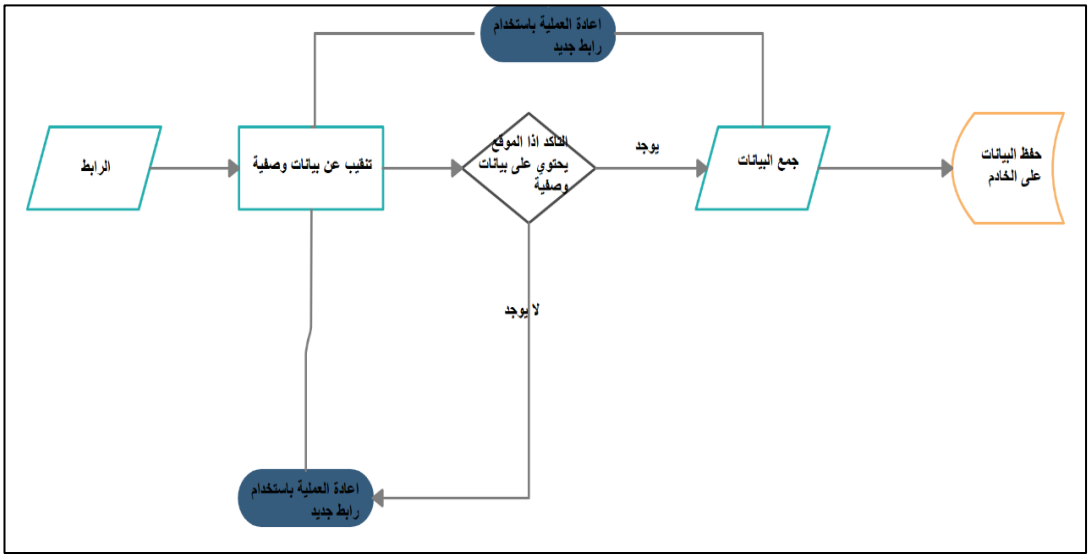
- **جمع المصـادر:** عندما تبدأ عملية البحث في محرك البحث الخاص بالويب المظلم، تكون النتائج في شـكل بسيط، وهو: (1.عنوان الموقع.، 2.رابط الموقع. ، 3. وصف الموقع).

ففي حال انتهاء عملية تجميع الروابط تبدأ عملية الزحف وهي أكبر من ســـابقتها، حيث ترتكز عملية الـزحـف عـلـى الـروابـط الـمـوجـودة فـي نـتـائـج عـمـلـيـة الـبـحـث الأولـى؛ فـطـبـيـعـة طـلـب (HTTP) هو طلب من مرسـل، واسـتجابة من المسـتقبل، والبيانات المطلوبة هي الاسـتجابة وعادة ما تكون كود (HTML) متعددة المضـــامين، أهمها روابط أخرى، وبيانات متعلقة بالكلمة المفتاحية، وفي مصـــدر الصـــفحة (HTML) تتم عملية التنقيب عن بيانات معينة مثل: صـــور، فيديو، عناوين بريد إلكتروني، عناوين محفظة إلكترونية وروابط أخرى.



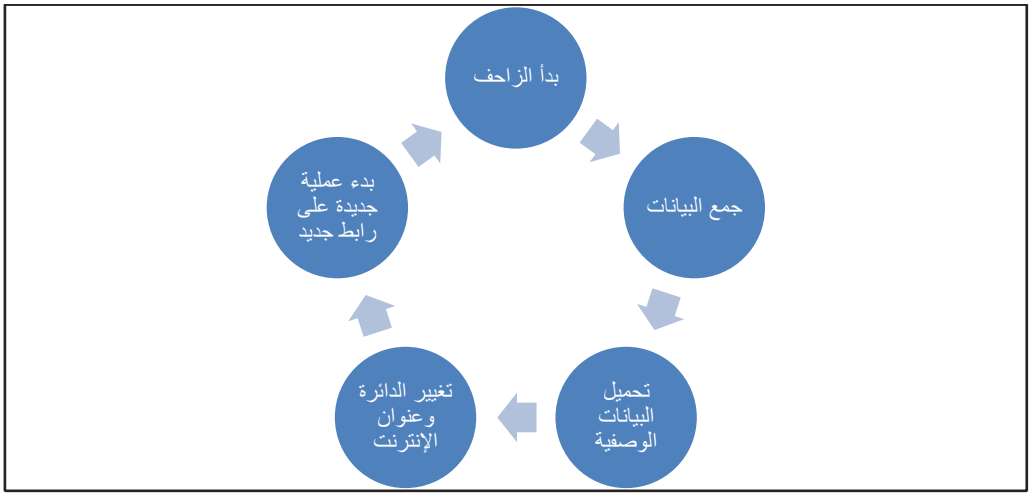
شكل رقم (2) عملية تعامل الزاحف مع الروابط

- **تحميل المصادر**: بعد العملية أعلاه، تأتي في وقت لاحق عملية تحميل المصادر وفق الشكل أدناه.



شكل رقم (3) عملية البحث عن البيانات الوصفية

الأمان: كما أشـرنا آنفًا في أثناء هذا البحث أن تصـفح الويب المظلم ليس آمنًا على الإطلاق، وهذا مرده إلى عدم وجود رقابة على المحتوى أو إدارة للمواقع من قبل هيئة معينة؛ هذا بدوره قد يقود إلى عمليات الاختراق أو تحديد مواقع المسـتخدمين بكل سـهولة. ولتفادي ذلك يمكن تغيير الدائرة الخاصـة بمتصـفح (Tor)، وتغيير عنوان الإنترنت (IP) بعد كل طلب (HTTP).



شكل شكل رقم (4) تغيير متصفح (Tor) لعنوان الإنترنت (IP) بعد كل طلب(HTTP)

– معالجة الأخطاء: نظرًا لضعف شبكة الويب المظلم، فإن حدوث الأخطاء وارد بشكل كبير جدًا، ولعل أكثر هذه الأخطاء وأشهرها هو انتهاء وقت الحزمة (TTL Expired)، وهذا يعني أن مهلة الطلب انتهت دون الوصول إلى الهدف، ولتجاوز هذه المشكلة: يجب إنشاء الطلب مرة أخرى وأخرى إلى أن يتم الطلب بنجاح.

تحليل البيانات: خلال جمع العمليات يحفظ الزاحف بيانات تساعد على التحليل، وتنبئ بتوجه الموقع. والبيانات التي يتم جمعها هي الآتي:

1. عدد الروابط المستخرجة من عملية البحث.
2. عدد الفيديوهات المجمعة خلال عملية جمع المصادر.
3. عدد الهواتف المجمعة خلال عملية جمع المصادر.
4. عدد الأبردة الإلكترونية المجمعة خلال عملية جمع المصادر.
5. عدد المحافظ الإلكترونية المجمعة خلال عملية جمع المصادر.

هذه البيانات تُستخدَم في التحليل؛ لإيجاد العلاقة بين الكلمة المفتاحية والمحتوى الخاص بالمواقع، على سبيل المثال: لإيجاد نسبة التواصل عبر الهاتف الخاصة بالكلمة المفتاحية تستخدم المعادلة التالية:

نسبة التواصل عبر الهاتف = عدد أرقام الهواتف / عدد الروابط * 100%

لإيجاد نسبة التواصل عبر البريد الإلكتروني: تستخدم المعادلة نفسها بتغيير بعض المعطيات، على سبيل المثال:

نسبة التواصل عبر البريد الإلكتروني = عدد عناوين البريد الإلكتروني / عدد الروابط * 100%

لإيجاد إجمالي نسبة التواصل: تستخدم مخرجات المعادلتين السابقتين، على سبيل المثال:

نسبة التواصل = نسبة التواصل عبر البريد الإلكتروني + نسبة التواصل عبر الهاتف.

المعادلات السابقة هي لإيجاد نسبة التواصل الخاصة بنتائج الكلمة المفتاحية المستخدمة في البحث.

ولإيجاد نسبة البيع والشراء الخاصة بالكلمة المفتاحية: يعتمد ذلك على عناوين المحفظة الإلكترونية Bitcoin

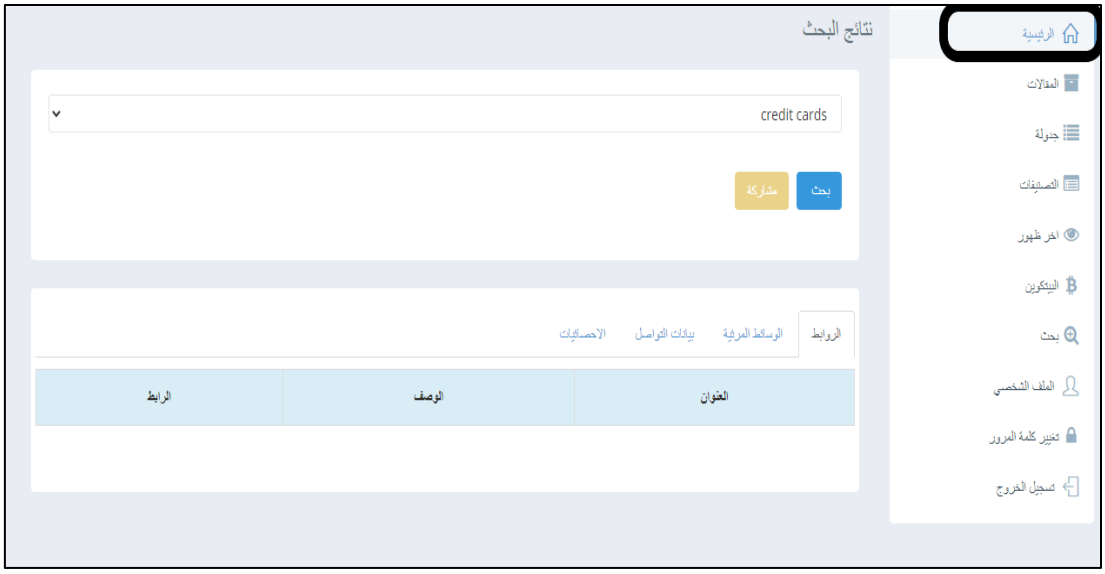
ومعادلة نسبة الشراء والبيع ترتكز على عدد عناوين المحافظ الإلكترونية:

نسبة الشراء والبيع = عدد المحافظ الإلكترونية / عدد المواقع الكلي * 100%

وبعد الحصول على هذه النسب يمكن تحديد توجه الموقع إذا كان خاصًا بالتواصل أم التجارة والبيع أو أي أغراض أخرى. وهذه النسب يمكن قراءتها تلقائيًا، من خلال البوابة المعلوماتية التي صُمِّمت على هذا الأساس.

2- **المرحلة الثانية التنفيذ العملي لبناء النموذج المصغر للبوابة المعلوماتية، بحسب الوظائف والمهام الآتية:**

الشاشة الرئيسة : حيث تتمثل وظيفة الشاشة الرئيسة في عرض النتائج التي قد تم الانتهاء من البحث عنها، وأيضًا مشاركة النتائج.

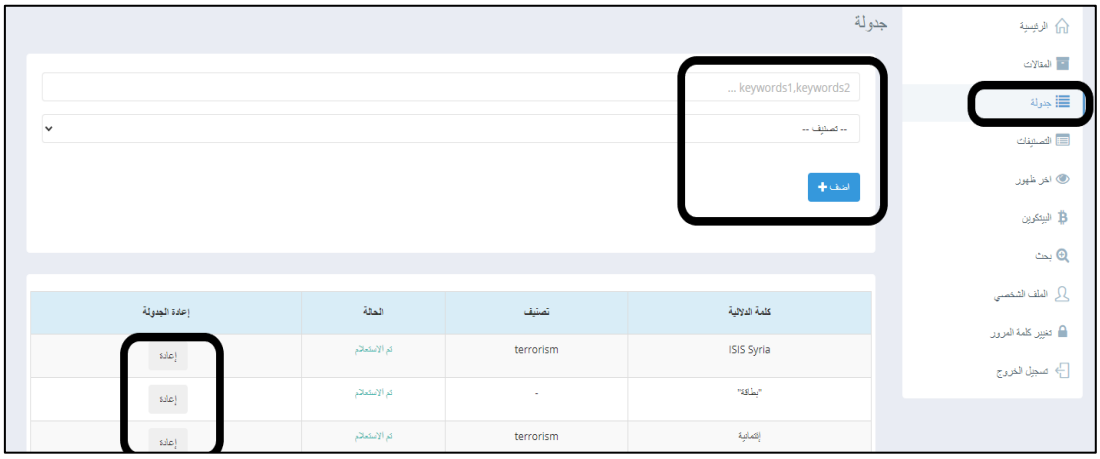


شكل رقم (5) وظيفة الشاشة الرئيسة

شاشة المقالات:يوجد في شاشة المقالات عدة خيارات، مثل: إضافة، حذف، تعديل، أو عرض مقال.

شكل رقم (6) الخيارات الموجودة في شاشة المقالات

شاشة الجدولة: يوجد العديد من الخيارات في شاشة الجدولة، مثل: إضافة كلمة دلالية وإرفاقها إلى تصنيف معين، وأيضًا إعادة البحث عن كلمة دلالية بعد انتهاء البحث عنها سابقًا. في حال كانت عملية البحث جارية حاليًا وتريد إجهاض العملية يظهر خيار إجهاض العملية، ويظهر هذا الخيار على شكل مفتاح باللون الأحمر بداخله كلمة قتل العملية باللغة الإنجليزية.

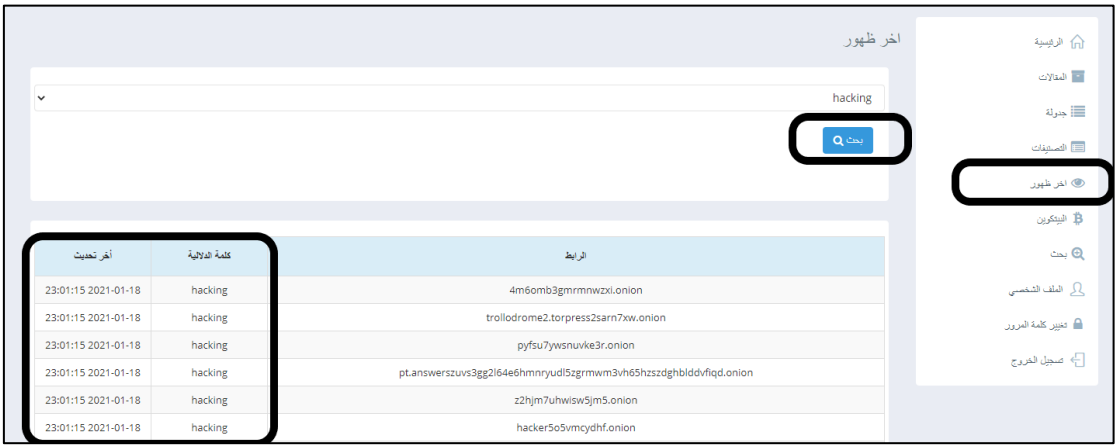


شكل رقم (7) وظيفة الجدولة

شاشة التصنيفات: من خلال شاشة التصنيفات يتم إضافة تصنيف أو تعديل آخر، وأيضًا عرض تقرير مفصل عن تصنيف معين.

شكل رقم (8) وظيفة التصنيفات

شاشة آخر ظهور: في شاشة آخر ظهور يتم تعقُّب المواقع عن آخر ظهور لها من خلال الزاحف، حيث يتم تشغيل فحص آخر ظهور كل ثمانية ساعات، ويتم عرض آخر استجابة للموقع في شبكة الويب المظلم.

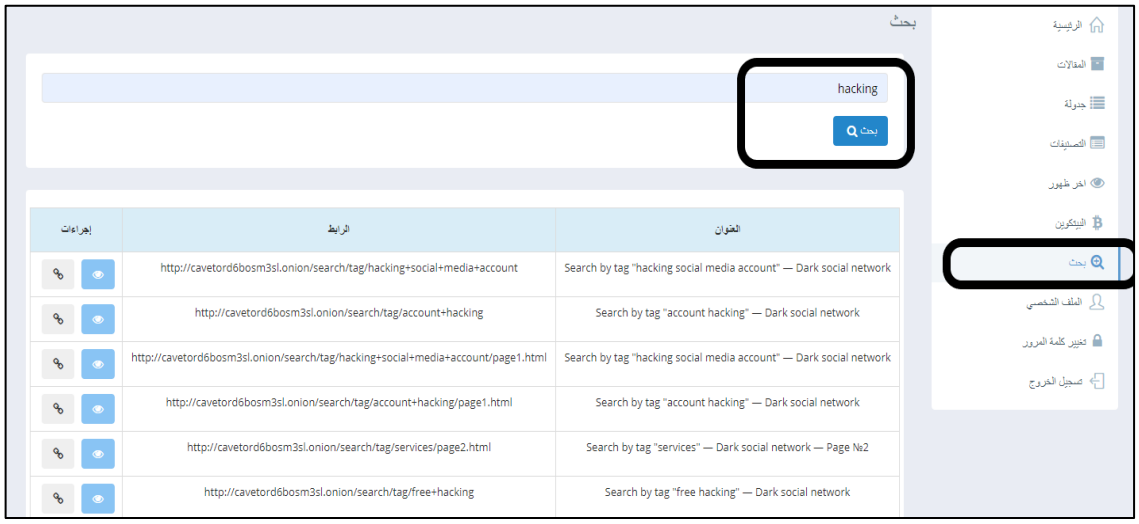


شكل رقم (9) وظيفة شاشة آخر ظهور

شاشة البيتكوين: في هذه الشاشة يتم عرض بيانات المحفظة الإلكترونية البيتكوين، التي تم استخراجها باستخدام الزاحف، ويتم فحص المحافظ كل ثماني ساعات من خلال الزاحف. وكما هو موضح عند استخراج عنوان محفظة يتم الحصول على البيانات الموضحة في الصورة أدناه.

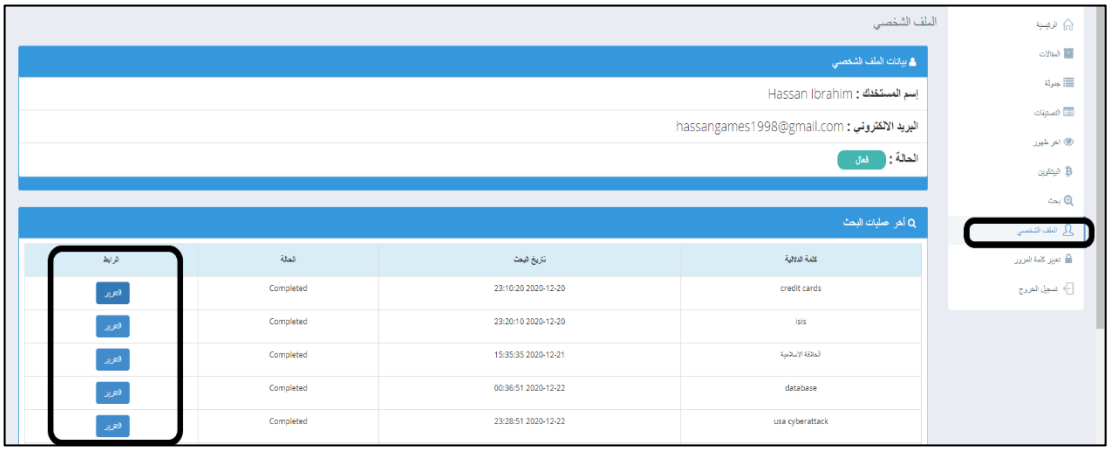
شكل رقم (10) وظيفة شاشة البيتكوين

شاشة البحث المباشر: تمكن شاشة البحث المباشر المستخدم من البحث في الويب المظلم بشكل مباشر دون أي أدوات وسيطة، وأيضًا تتيح للمستخدم عرض محتوى الويب المظلم دون برامج وسيطة، إلا أن هذه الميزة تتطلب الحذر من خطورة الويب المظلم، لذلك قبل عرض المحتوى للمستخدم يتم حذف جميع الروابط الخارجية؛ حفاظًا على أمن المستخدم.



شكل رقم (11) وظيفة شاشة البحث المباشر

شاشة الملف الشخصي: في هذه الشاشة يتم عرض بيانات المستخدم الشخصية بجانب جميع الكلمات الدلالية الخاصة به، والتقرير في حال انتهاء البحث عنها.



شكل رقم (12) وظيفة شاشة الملف الشخصي

كما تحقّقت هذه النتائج في استخدام الأدوات المتاحة عليها، من حيث: سهولة الاستخدام، وإنشاء قواعد البيانات، ونتائج البحث والتحليل، وآلية عرضها، والصلاحيات المعطاة للمستخدم... ولعل من أهم هذه النتائج أن (90.06) من العينة المبحوثة وجدوا سهولة إنشاء قاعدة بيانات باستخدام البوابة المعلوماتية، و(89.06) من العينة المبحوثة وجدوا سهولة في أدوات البحث، والنسبة ذاتها في تقييم المخاطر الأمنية على استخدام الجماعات والمنظمات الإرهابية للويب المظلم، كذلك أوضحت نتائج السؤالين المفتوحين بعض الملاحظات والمقترحات التي من شأنها أن تخدم أهداف البوابة مستقبلًا، مثل: تطوير أدوات البحث، والإحصائيات العميقة، وحفظ محتوى الصفحات في قواعد البيانات.

التحليل الإحصائي للبيانات ذات الصلة باختبار البوابة (المعلوماتية)

لاختبار مخرجات النموذج المُصغَّر للبوابة (معلوماتية)، لجمع وتحليل محتوى الويب المظلم ذي الصلة بالإرهاب، فإن هذا الجزء يقدم التحليل الإحصائي للبيانات ذات الصلة بالأسئلة ذات النهاية المغلقة لاختبار البوابة وفق الآتي:

جدول رقم (1) توزيع أفراد عينة الدراسة تبعًا للمتغيرات الديموغرافية (ن=16)

المتغيرات	المجموعات	ن	%
الجنس	ذكر	16	100.0
المجال الوظيفي	مدني	11	68.8
	عسكري	5	31.3

الخبرة	5 سنوات فأقل	1	6.3
	عشر سنوات فأكثر	15	93.8
المؤهل العلمي	ثانوي	1	6.3
	دبلوم عالي	3	18.8
	بكالوريوس	10	62.5
	دراسات عليا	2	12.5
طبيعة العمل	معالج معلومات	3	18.8
	محلل معلومات	7	43.8
	مقيّم معلومات	11	68.8
	أخرى	2	12.5

ويوضح جدول رقم (1) أن عينة الدراسة كانت ذكورًا بنسبة (100%)، حيث كان (68.8%) من إجمالي عينة الدراسة مدنيين، وكان (31.3%) عسكريين، وبالنسبة للخبرة كانت ما نسبته (93.8%) لديهم عشر سنوات فأكثر خبرة في العمل، وبالنسبة للتعليم كانت أعلى نسبة (62.5%) حاصلين على البكالوريوس، وبالنسبة لطبيعة العمل كان مقيّم المعلومات الأعلى بنسبة (68.8%) من إجمالي الدراسة.

والنسبة المئوية الكاملة لعينة (الذكور) تعزى إلى أن غالبية المتخصصين في الأعمال ذات العلاقة بمكافحة الإرهاب بما في ذلك مكافحته في العالم الافتراضي ليس على مستوى المملكة فحسب، بل على مستوى العالم هم من فئة الذكور؛ نظرًا لطبيعة مثل هذه الأعمال التي تتطلب ربما قدرات خاصة يتمتع بها الذكور أكثر من الإناث، إضافة إلى أن المرأة في المملكة لم تخض حتى الآن العمل بشكل كبير في مثل هذا النوع من الأعمال، بينما يعزو البحث النسبة المئوية الأعلى لطبيعة العمل لمقيّم المعلومات، ربما لأنها أكثر شمولية، فعملية التقييم تقوم على الجمع والتحليل والتي في بعض الجهات قد يقوم بها المقيّم نفسه.

تحليل استجابات المشاركين حول أسئلة الدراسة

المحور الثاني: يقيس هذا المحور واقع أفراد مجتمع الدراسة بالنسبة للويب المظلم، من حيث الدخول إلى الويب، واستخدام الخدمات القانونية وغير القانونية المتوفرة عليه، وتقييم استخدام الجماعات والمنظمات الإرهابية للويب المظلم، وتقييم المخاطر الأمنية المترتبة على هذا الاستخدام، والتوقعات المستقبلية لذلك.

جدول رقم (2) يوضح واقع أفراد مجتمع الدراسة بالنسبة للدخول للويب المظلم

دخولك إلى الويب المظلم	التكرار	النسبة المئوية
أبدًا	11	68.8
أحيانًا	4	25.0
دائمًا	1	6.3
المجموع	16	100.0

يوضح جدول رقم (2) استجابات عينة الدراسة حول الفقرة (دخولك إلى الويب المظلم)، حيث جاءت (أبدًا) بأعلى نسبة (68.8%)، ويليها (أحيانًا) بنسبة (25%)، يليها (دائمًا) بأقل نسبة (6.3%) من إجمالي عينة الدراسة، ويوضح الشكل البياني التالي هذه النتائج.

ومجيء (أبدًا) كأعلى نسبة في استجابات عينة الدراسة حول الفقرة (دخولك إلى الويب المظلم) يمكن ارجاعه إلى أن الويب المظلم نفسه غير معروف بشكل كبير على مستوى العالم كما هو الحال للإنترنت (السطحي)، وقد يكون معروفًا ومتداولًا بين المختصين التقنيين، وهو ما أكدته النسبتان (أحيانًا) و(دائمًا)، اللتان تعطيان مؤشرًا على دخول المختصين، وعلى الأرجح أن يكون هذا الدخول مرتبطًا بمجال العمل.

جدول رقم (3) استخدام الخدمات القانونية وغير القانونية على الويب المظلم

استخدامك الخدمات القانونية وغير القانونية على الويب المظلم	التكرار	النسبة المئوية
أبدًا	12	75.0
أحيانًا	4	25.0
المجموع	16	100.0

يوضح جدول رقم (3) استجابات عينة الدراسة حول الفقرة (استخدامك الخدمات القانونية وغير القانونية على الويب المظلم)، حيث جاءت (أبدًا) بأعلى نسبة وهي (75%)، يليها (أحيانًا) بنسبة (25%) كأقل نسبة من إجمالي عينة الدراسة ويوضح الشكل البياني التالي هذه النتائج.

جدول رقم (4) تقييم استخدام الأفراد والجماعات والمنظمات الإرهابية للويب المظلم

تقييمك لاستخدام الأفراد والجماعات والمنظمات الإرهابية للويب المظلم	التكرار	النسبة المئوية
أبدًا	3	18.8
أحيانًا	8	50.0
دائمًا	5	31.3
المجموع	16	100.0

يوضح جدول رقم (4) استجابات عينة الدراسة حول الفقرة (تقييمك لاستخدام الأفراد والجماعات والمنظمات الإرهابية للويب المظلم)، حيث (أحيانًا) بنسبة (50%) كأعلى نسبة، يليها (دائمًا) بنسبة (31.3%)، ويليها (أبدًا) بأقل نسبة وهي (18.8%) من إجمالي عينة الدراسة ويوضح الشكل البياني التالي هذه النتائج.

ويعزى ارتفاع النسبة المئوية من خلال (أحيانًا) و(دائمًا) إلى إدراك عينة الدراسة إلى أساليب الجماعات والمنظمات الإرهابية في البحث عن تأمين أعمالها في العالم الافتراضي.

جدول رقم (5) تقييم المخاطر الأمنية من استخدام الأفراد والجماعات والمنظمات الإرهابية للويب المظلم

تقييمك للمخاطر الأمنية من استخدام الأفراد والجماعات والمنظمات الإرهابية للويب المظلم	التكرار	النسبة المئوية
لا توجد	1	6.3
عالية	4	25.0
عالية جدًا	11	68.8
المجموع	16	100.0

يوضح جدول رقم (5) استجابات عينة الدراسة حول الفقرة (تقييمك للمخاطر الأمنية من استخدام الأفراد والجماعات والمنظمات الإرهابية للويب المظلم)، حيث جاءت (عالية جدًا) بنسبة (68.8%) كأعلى نسبة، يليها (عالية) بنسبة (25%)، ثم (لا توجد) بأقل نسبة وهي (6.3%) من إجمالي عينة الدراسة ويوضح الشكل البياني التالي هذه النتائج.

وارتفاع النسبة المئوية لـــ (عالية جدًا) و(عالية) لتقييم المخاطر الأمنية من استخدام الأفراد والجماعات والمنظمات الإرهابية للويب المظلم، يعزز ما أُشير إليه في الفقرة السابقة إلى إدراك عينة الدراسة لاستخدام الجماعات والمنظمات الإرهابية بشكل كبير في المستقبل.

جدول رقم (6) التوقعات المستقبلية لاستخدام الويب المظلم من قبل الأفراد والجماعات والمنظمات الإرهابية

التوقعات المستقبلية لاستخدام الويب المظلم من قبل الافراد والجماعات والمنظمات الإرهابية	التكرار	النسبة المئوية
عدم الاستخدام	1	6.3
استخدام جزئي	5	31.3
استخدام كلي	10	62.5
المجموع	16	100.0

يوضح جدول رقم (6) استجابات عينة الدراسة حول الفقرة (التوقعات المستقبلية لاستخدام الويب المظلم من قبل الأفراد والجماعات والمنظمات الإرهابية)، حيث إن (الاستخدام الكلي) جاء بنسبة (62.5%) كأعلى نسبة، يليها (الاستخدام الجزئي) بنسبة (31.3%)، ثم (عدم الاستخدام) بأقل نسبة وهي (6.3%) من إجمالي عينة الدراسة، ويوضح الشكل البياني التالي هذه النتائج.

وبحسب ما يرى البحث فإن ارتفاع النسبة المئوية للاستخدام كلي، وكذلك الاستخدام الجزئي هو امتداد للفقرتين السابقتين وتأكيد لهما.

المحور الثالث: يقيس هذا المحور واقع تجربة مجتمع الدراسة للبوابة المعلوماتية (راصد)، من حيث سهولة إنشاء قاعدة بيانات من خلالها، والصلاحيات المعطاة للمستخدم، وسهولة أدوات البحث، وأدوات تحليل النتائج، والرضا عن نتائج البحث، ونتائج التحليل، والرضا عن عرض النتائج، ووسائل مشاركة المعرفة عبر البوابة.

جدول رقم (7) سهولة إنشاء قاعدة بيانات عبر البوابة (المعلوماتية) ذات العلاقة بموضوع البوابة

سهولة إنشاء قاعدة بيانات عبر البوابة (المعلوماتية) ذات العلاقة بموضوع البوابة	التكرار	النسبة المئوية

سهلة	6	37.5
سهلة جدًا	10	62.5
المجموع	16	100.0

يوضح جدول رقم (4) استجابات عينة الدراسة حول الفقرة (سهولة إنشاء قاعدة بيانات عبر البوابة (المعلوماتية) ذات العلاقة بموضوع البوابة)، حيث جاءت (سهلة جدًا) بنسبة (62.5%) كأعلى نسبة، يليها (سهلة) بنسبة (37.5%) كأقل نسبة من إجمالي عينة الدراسة، ويوضح الشكل البياني التالي هذه النتائج.

جدول رقم (8) الصلاحيات المعطاة للمستخدم عبر البوابة (المعلوماتية) ذات العلاقة بموضوع البوابة

الصلاحيات المعطاة للمستخدم عبر البوابة (المعلوماتية) ذات العلاقة بموضوع البوابة	التكرار	النسبة المئوية
إلى حدّ ما	2	12.5
مناسبة	11	68.8
مناسبة جدًا	3	18.8
المجموع	16	100.0

يوضح جدول رقم (8) استجابات عينة الدراسة حول الفقرة (الصلاحيات المعطاة للمستخدم عبر البوابة (المعلوماتية) ذات العلاقة بموضوع البوابة)، حيث جاءت (مناسبة) بنسبة (68.8%) كأعلى نسبة، يليها (مناسبة جدًا) بنسبة (18.8%)، ثم (إلى حد ما) بأقل نسبة وهي (12.5%) من إجمالي عينة الدراسة، ويوضح الشكل البياني التالي هذه النتائج.

جدول رقم (9) سهولة أدوات البحث عبر البوابة (المعلوماتية) باستخدام الكلمات المفتاحية ذات العلاقة

سهولة أدوات البحث عبر البوابة (المعلوماتية) باستخدام الكلمات المفتاحية ذات العلاقة بموضوع البوابة	التكرار	النسبة المئوية
سهلة	7	43.8

سهلة جدًا	9	56.3
المجموع	16	100.0

يوضح جدول رقم (9) استجابات عينة الدراسة حول الفقرة (سهولة أدوات البحث عبر البوابة (المعلوماتية) باستخدام الكلمات المفتاحية ذات العلاقة بموضوع البوابة)، حيث جاءت (سهلة جدًا) بنسبة (56.3%) كأعلى نسبة، يليها (سهلة) بنسبة (43,8%) كأقل نسبة من إجمالي عينة الدراسة، ويوضح الشكل البياني التالي هذه النتائج.

جدول رقم (4-10) أدوات التحليل لنتائج البحث عبر البوابة المعلوماتية باستخدام الكلمات المفتاحية ذات العلاقة بموضوع البوابة

أدوات التحليل لنتائج البحث عبر البوابة المعلوماتية باستخدام الكلمات المفتاحية ذات العلاقة بموضوع البوابة	التكرار	النسبة المئوية
إلى حد ما	2	12.5
مناسبة	10	62.5
مناسبة جدًا	4	25.0
المجموع	16	100.0

يوضح جدول رقم (10) استجابات عينة الدراسة حول الفقرة (أدوات التحليل لنتائج البحث عبر البوابة المعلوماتية باستخدام الكلمات المفتاحية ذات العلاقة بموضوع البوابة 3)، حيث جاءت (مناسبة) بنسبة (62.5%) كأعلى نسبة، يليها (مناسبة جدًا) بنسبة (25%)، ثم (إلى حد ما) بأقل نسبة وهي (12.5%) من إجمالي عينة الدراسة، ويوضح الشكل البياني التالي هذه النتائج.

جدول رقم (11) الرضا عن نتائج البحث عبر البوابة المعلوماتية باستخدام الكلمات المفتاحية ذات العلاقة

رضاك عن نتائج البحث عبر البوابة المعلوماتية باستخدام الكلمات المفتاحية ذات العلاقة بموضوع البوابة	التكرار	النسبة المئوية
إلى حد ما	5	31.3
راضٍ	4	25.0

راضٍ جدًا	7	43.8
المجموع	16	100.0

يوضـــح جدول رقم (11) اســـتجابات عينة الدراســـة حول الفقرة (رضـــاك عن نتائج البحث عبر البوابة المعلوماتية باستخدام الكلمات المفتاحية ذات العلاقة بموضوع البوابة)، حيث جاء (راضٍ جدًا) بنسبة (43.8%) كأعلى نسـبة، يليها (إلى حد ما) بنسـبة (31.3%)، ثم (راضٍ) بنسـبة (25%) كأقل نسـبة من إجمالي عينة الدراسة، ويوضح الشكل البياني التالي هذه النتائج.

جدول رقم (12) الرضا عن تحليل النتائج عبر البوابة المعلوماتية باستخدام الكلمات المفتاحية ذات العلاقة

رضـاك عن تحليل النتائج عبر البوابة المعلوماتية باستخدام الكلمات المفتاحية ذات العلاقة بموضوع البوابة	التكرار	النسبة المئوية
إلى حد ما	3	18.8
راضٍ	7	43.8
راضٍ جدًا	6	37.5
المجموع	16	100.0

يوضـــح جدول رقم (12) اســـتجابات عينة الدراســـة حول الفقرة (رضـــاك عن تحليل النتائج عبر البوابة المعلوماتية باســـتخدام الكلمات المفتاحية ذات العلاقة بموضـــوع البوابة)، حيث جاء (راضٍ) بنســـبة (43.8%) كأعلى نسـبة، يليها (راضٍ جدًا) بنسـبة (37.5%)، يليها (إلى حد ما) بأقل نسـبة وهي (18.8%) من إجمالي عينة الدراسة، ويوضح الشكل البياني التالي هذه النتائج.

جدول رقم (13) الرضا عن عرض النتائج عبر البوابة المعلوماتية باستخدام الكلمات المفتاحية ذات العلاقة

رضـاك عن عرض النتائج التحليلية عبر البوابة المعلوماتية باســـتخدام الكلمات المفتاحية ذات العلاقة بموضوع البوابة	التكرار	النسبة المئوية
إلى حد ما	4	25.0

راضٍ	7	43.8
راضٍ جدًا	5	31.3
المجموع	16	100.0

يوضح جدول رقم (13) استجابات عينة الدراسة حول الفقرة (رضاك عن عرض النتائج التحليلية عبر البوابة المعلوماتية باستخدام الكلمات المفتاحية ذات العلاقة بموضوع البوابة)، حيث جاء (راضٍ) بنسبة (43.8%) كأعلى نسبة، يليها (راضٍ جدًا) بنسبة (31.3%)، يليها (إلى حد ما) بأقل نسبة وهي (25%) من إجمالي عينة الدراسة، ويوضح الشكل البياني التالي هذه النتائج.

جدول رقم (14) الرضا عن عرض النتائج عبر البوابة المعلوماتية باستخدام الكلمات المفتاحية ذات العلاقة

رضاك عن وسائل مشاركة المعرفة المتاحة عبر البوابة (المعلوماتية)	التكرار	النسبة المئوية
إلى حد ما	3	18.8
راضٍ	4	25.0
راضٍ جدًا	9	56.3
المجموع	16	100.0

يوضح جدول رقم (14) استجابات عينة الدراسة حول الفقرة (رضاك عن عرض النتائج التحليلية عبر البوابة المعلوماتية باستخدام الكلمات المفتاحية ذات العلاقة بموضوع البوابة)، حيث جاء (راضٍ جدًا) بنسبة (56.3%) كأعلى نسبة، يليها (راضٍ) بنسبة (25%)، ثم (إلى حد ما) بأقل نسبة وهي (18.8%) من إجمالي عينة الدراسة، ويوضح الشكل البياني التالي هذه النتائج.

وفي ختام هذا الجزء الخاص بتحليل النتائج، وبعد عرض الإحصاء الوصفي؛ قامت الدراسة بتحليل آراء أفراد عينة الدراسة حول فقرات الاستمارة، حيث تم استخدام مقياس ليكرت الثلاثي لأول ثلاث فقرات، ومقياس ليكرت الرباعي لباقي فقرات الاستمارة، ولتحويل المتوسطات الحسابية إلى نسب مئوية: نقوم بضرب المتوسط الحسابي في (100 /3 =33.33) لفقرات المقياس الثلاثي، وبضرب المتوسط الحسابي في (100 / 4 =25) لفقرات المقياس الرباعي، كما أشار إلى ذلك (Pimentel, J. L ; 2010).

وعليه تم تحليل أفراد عينة الدراسة، من خلال حساب العدد وأقل قيمة وأكبر قيمة، والمتوسطات الحسابية، والانحرافات المعيارية، ودرجة المتوسطات تبعًا لمقياس ليكرت الخماسي، والترتيب التنازلي للفقرات تبعًا للمتوسطات الحسابية بأقل قيمة للانحراف المعياري.

جدول رقم (15) الإحصاءات الوصفية لمتغيرات الدراسة الرتبية

الفقرات	ن	أقل قيمة	أكبر قيمة	المتوسط الحسابي	الانحراف المعياري	النسبة المئوية	الترتيب
دخولك إلى الويب المظلم.	16	1.00	3.00	1.3750	61914.	45.83	12
استخدامك الخدمات القانونية وغير القانونية على الويب المظلم.	16	1.00	2.00	1.2500	44721.	41.66	13
تقييمك لاستخدام الأفراد والجماعات والمنظمات الإرهابية للويب المظلم.	16	1.00	3.00	2.1250	71880.	70.83	10
تقييمك للمخاطر الأمنية من استخدام الأفراد والجماعات والمنظمات الإرهابية للويب المظلم.	16	1.00	4.00	3.5625	81394.	89.06	3
التوقعات المستقبلية لاستخدام الويب المظلم من قبل الأفراد والجماعات والمنظمات الإرهابية.	16	1.00	3.00	2.5625	62915.	64.06	11
سهولة إنشاء قاعدة بيانات عبر البوابة (المعلوماتية) ذات العلاقة بموضوع البوابة.	16	3.00	4.00	3.6250	50000.	90.63	1

الفقرات	ن	أقل قيمة	أكبر قيمة	المتوسط الحسابي	الانحراف المعياري	النسبة المئوية	الترتيب
الصلاحيات المعطاة للمستخدم عبر البوابة (المعلوماتية) ذات العلاقة بموضوع البوابة.	16	2.00	4.00	3.0625	57373.	76.56	8
سهولة أدوات البحث عبر البوابة (المعلوماتية) باستخدام الكلمات المفتاحية ذات العلاقة بموضوع البوابة.	16	3.00	4.00	3.5625	51235.	89.06	2
3 أدوات لتحليل لنتائج البحث عبر البوابة المعلوماتية باستخدام الكلمات المفتاحية ذات العلاقة بموضوع البوابة.	16	2.00	4.00	3.1250	61914.	78.13	6
رضاك عن نتائج البحث عبر البوابة المعلوماتية باستخدام الكلمات المفتاحية ذات العلاقة بموضوع البوابة.	16	2.00	4.00	3.1250	88506.	78.13	7
رضاك عن تحليل النتائج عبر البوابة المعلوماتية باستخدام الكلمات المفتاحية ذات العلاقة بموضوع البوابة.	16	2.00	4.00	3.1875	75000.	79.69	5

الفقرات	ن	أقل قيمة	أكبر قيمة	المتوسط الحسابي	الانحراف المعياري	النسبة المئوية	الترتيب
رضاك عن وسائل مشاركة المعرفة المتاحة عبر البوابة (المعلوماتية).	16	2.00	4.00	3.3750	80623.	84.38	4
رضاك عن عرض النتائج التحليلية عبر البوابة المعلوماتية باستخدام الكلمات المفتاحية ذات العلاقة بموضوع البوابة.	16	2.00	4.00	3.0625	77190.	76.56	9

يوضح الجدول السابق ما يأتي:

- جاء في المرتبة الأولى: (سهولة إنشاء قاعدة بيانات عبر البوابة) المعلوماتية (ذات العلاقة بموضوع البوابة) بمتوسط حسابي (3.6250) من أصل (4) درجات، وانحراف معياري (50000.)، وهو ما يقابل موافقة كبيرة جدًا لما نسبته (90.63%) من إجمالي عينة الدراسة.
- جاء في المرتبة الثانية: (سهولة أدوات البحث عبر البوابة) المعلوماتية (باستخدام الكلمات المفتاحية ذات العلاقة بموضوع البوابة) بمتوسط حسابي (3.5625) من أصل (4) درجات، وانحراف معياري (51235.)، وهو ما يقابل موافقة كبيرة جدًا لما نسبته (89.06%) من إجمالي عينة الدراسة.
- بينما جاء في المرتبة الأخيرة: (استخدامك الخدمات القانونية وغير القانونية على الويب المظلم) بمتوسط ح
- سابي (1.2500) من أصل (3)، وانحراف معياري (44721.)، وهو ما يقابل أقل نسبة موافقة وهي (41.66%) من إجمالي عينة الدراسة، ويوضح الشكل التالي هذه النتائج.

شكل رقم (16) نتائج الأسئلة المفتوحة في هذا القسم التحليلي ذي العلاقة باختبار البوابة (المعلوماتية)

أما فيما يخص نتائج الأسـئلة المفتوحة في هذا القسـم التحليلي ذي العلاقة باختبار البوابة (المعلوماتية)، وهي عبارة عن سؤالين؛ ركّزت بشكل كبير على المقترحات التي من شأنها أن تخدم أهداف البوابة بشكل أفضل، وكذلك المقترحات والملاحظات والمشـــاكل التقنية من خلال تجربة البوابة المعلوماتية، وقد جاءت النتائج وفق الآتي:

- بلغ عدد الذين أجابوا عن السؤالين المفتوحين (9) من عينة الدراسة، أي: ما يُمثِّل نسبة (56%) منها.
- بلغ عدد الذين أجابوا عن السؤال الأول (5) من أصل (9)، أي: ما يُمثِّل نسبة (55.5%) ممن أجابوا عن السؤالين.

- عدد من أجابوا عن السؤال الثاني فقط عدد (2) من أصل (9)، أي: ما يُمثِّل نسبة (22.2%) ممن أجابوا عن السؤالين.
- عدد الذين أجابوا عن السؤالين معًا عدد (2) من أصل (9)، أي: ما يُمثِّل نسبة (22.2%)ممن أجابوا عن السؤالين.
- ركّزت إجابات السؤال الأول على بعض المقترحات التي من شأنها أن تخدم معطيات البوابة بشكل أفضل، مثل: السعي نحو فلترة الصور بشكل أدق، حيث إن نظام البوابة يسحب فقط الصور التي لها علاقة بالموضوع. ومن المقترحات كذلك: العمل على تطوير أداوت البحث بشكل أفضل؛ كعملية البحث المتقدم، مما يخدم البوابة بشكل أفضل. ومن المقترحات التي وردت حول هذا السؤال: هو العمل على إظهار الإحصائيات بشكل أعمق، بحيث يمكن إدخال تحليل البيانات الإحصائية لإظهار التغيير في المنحنيات، وإتاحة البوابة المعلوماتية للمستخدمين بشكل آمن؛ وذلك نظرًا لخطورة الويب المظلم، وليس كل مستخدم قادر على حماية نفسه فيه. ومن المقترحات: الاحتفاظ بمحتوى الصفحات؛ لسهولة الرجوع إليها عند الحاجة، والعمل على توفير أداة يمكن من خلالها مقارنة نتائج البحث الخاصة بالشبكة المظلمة مع نتائج الإنترنت السطحي بشكل تلقائي، وبناء متصفح عبر تور (tor)؛ لتصفح الدارك ويب بدون استخدام متصفح تور نفسه.
- بينما ركّزت إجابة السؤال الثاني على العمل على تقديم حلول تقنية أفضل فيما يتعلق بالتحليل الإحصائي، بينما ركّزت إحدى المقترحات بالسعي نحو تطوير البوابة لتكون مشروع دولة، بحيث تصبح مرجعًا معلوماتيًا وبحثيًا كبيرًا.

وفي هذا السياق ترى الدراسة أن هذه المقترحات والملاحظات مهمة، ويمكن الاستفادة منها في تطوير البوابة المعلوماتية بما يخدم المؤسسات الأمنية والأكاديمية في مكافحة ظاهرة الإرهاب، وربما بعضًا من هذه المقترحات لم تخف على الباحث الرئيسي المتخصص في المجال، إلا أن هناك عوائق تتعلق بالدعم المالي في الوقت الراهن، ومن جهة أخرى لا يوجد إدراك كامل حتى اللحظة للمخاطر المترتبة على استخدام الويب المظلم بشكل عام في انتشار الجرائم بما في ذلك جريمة الإرهاب.

التوصيات

وفقًا للنتائج أعلاه، وما خلص إليه؛ فإن البحث الحالي يقدِّم عددًا من التوصيات التي يمكن أن تكون أساسًا لتطوير تقنيات وأدوات تحليل محتوى الويب المظلم من خلال البوابة (المعلوماتية – المعرفية)، وذلك على النحو الآتي:

1. توصي الدراسة بتبنّي فكرة البحث، وذلك بتطوير نظام البوابة المعلوماتية إلى بوابة معرفية أوسع وأشمل، بحيث تصبح مشروعًا مؤسساتيًا تتبناه المؤسسات العلمية والأمنية على غرار مختبر أبحاث الذكاء الاصطناعي في جامعة أريزونا، الذي هو عبارة عن برنامج بحثي علمي طويل الأمد يهدف إلى دراسة وفهم ظاهرة الجماعات الإرهابية على الإنترنت إجمالًا والويب المظلم على وجه التحديد، والذي يسعى إلى اكتشاف المعرفة حول الإرهاب والمنهجيات المتقدمة لتحليل بحوث الإرهاب، وإنشاء بنية أساسية بحثية لاستخدامها من قبل علماء الكمبيوتر والمعلومات، وكذلك علماء الاجتماع الذين يدرسون مجموعة واسعة من المشكلات الحسابية والظواهر الاجتماعية والتنظيمية.

قائمة المراجع

المراجع العربية:

1. جندل، جاسم محمد (2014م) الإرهاب الإلكتروني، دار البداية ناشرون وموزعون.
2. صحيفة الاقتصادية (2016) الشبكة المظلمة.. ما لا يرى من جبل جليد الإنترنت، من موقع http://www.aleqt.com/2016/02/15/article_1030312.html
3. مجلس وزراء الداخلية العرب (1998) الاتفاقية العربية لمكافحة الإرهاب، المركز العربي للبحوث.
4. مركز المستقبل (2019م) ملاذات المتعصبين: دور شبكات "الإنترنت المظلم" في الهجوم الإرهابي بنيوزيلندا، تاريخ الدخول 2020/6/7م من موقع https://2u.pw/DCajA
5. المركز الوطني للابحاث واستطلاع الرأي (2015) الأعماق المظلمة للإنترنت "الشبكة العميقة"، تاريخ الدخول 9 أيار 2015م من موقع http://ncro.sy/?p=1889

المراجع الأجنبية:

1. Abbasi, Ahmed and Chen, Hsinchun. (2007) Analysis Of Affect Intensities In Extremist Group Forums. Available In: Terrorism Informatics Knowledge Management And Data Mining For Homeland Security, Edit By: Hsinchun Chen Edna Reid Joshua Sinai Andrew Silke Boaz Ganor, Its published by Springer Science + Business Media, Accesses date 18/9/2020 from: http://antiterrortoday.com/images/docs/Hsinchun_Chen_Hsinchun_Chen_Edna_Reid_Joshua_SBookFi.org.pdf
2. Decryptionary. (2020) Dark Web, Accesses date 23/7/2020 from: https://decryptionary.com/dictionary/dark-web/
3. Finklea, Kristin. (2017) Dark Web.P.P.2-10, Access date 14/02/2020 from: https://fas.org/sgp/crs/misc/R44101.pdf

4. Fu, Tianjun., Abbasi,ahmed and Chen, Hsinchun. (2010) A Focused Crawler for Dark Web Forums: 1219-1220, Journal of the American Society for Information Science and Technology, Vol 61, Number 6: 1213-1231, Accesses date 29/9/2020 from: https://www.researchgate.net/publication/302459792_Forum_Spidering.
5. Greenberg, Andy.(2014) Hacker Lexicon: What Is the Dark Web? Accesses date 23/7/2020 from: https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/#:~:text=The%20Dark%20Web%20is%20a,users%20from%20surveillance%20and%20censorship.
6. Hanson, B. and Weimann, G. (2018) Deep Dish: Terrorism in Cyberspace, Chicago Council on Global Affairs, Accesses date 5/6/2020 from: https://fas.org/sgp/crs/misc/R44101.pdf
7. Patil, G. A., Manwade, K. B and Landge, P. S. (2012) A Novel Approach for Social Network Analysis & Web Mining for Counter Terrorism, International Journal on Computer Science and Engineering (IJCSE),Vol. 4, No. 11 : 1816-1825, Accesses date 18/6/2020 from: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.637.2040&rep=rep1&type=pdf
8. Qin,et al. (2008) Studying Global Extremist Organizations' Internet Presence Using The Dark Web Attribute System. Available In: Terrorism Informatics Knowledge Management And Data Mining For Homeland Security, Edit By: Hsinchun Chen Edna Reid Joshua Sinai Andrew Silke Boaz Ganor, Its Published By Springer Science + Business Media Available Accesses date 16/6/2020 from: http://antiterrortoday.com/images/docs/Hsinchun_Chen_Hsinchun_Chen_Edna_Reid_Joshua_SBookFi.org.pdf
9. Zhang, at el. (2010) Developing a Dark Web Collection and Infrastructure for Computational and Social Sciences, Proceedings of 2010 IEEE International Conference on Intelligence and Security Informatics, ISI 2010, Vancouver, Canada, May 2010: 1-5 , Accesses date 18/6/2020 from: https://calhoun.nps.edu/bitstream/handle/10945/37179/Zhang-DevelopingDarkWebCollection-isi2010_final.pdf;jsessionid=C78E1FC694065FA4859088C0E240C397?sequence=1
10. Zhou, Yilu, et al.(2005). Building Knowledge Management System for Researching Terrorist Groups on the Web, Proceedings of the AIS Americas Conference on Information Systems (AMCIS 2005) , Omaha, NE, USA, August 11-14, Accesses date 18/6/2020 from: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.92.2834&rep=rep1&type=pdf