اتجاهات الخبراء المصريين في مجالات التشريع والتقنيّات والإعلام الرقمي نحو تطبيقات الشبكات المظلمة The Dark Web على الإنترنت

د. علا عبد القوى عامر محمد*

ملخص الدراسة:

سعت الدراسة الحالية للتعرف على اتجاهات الخبراء المصريين في مجالات التشريع والتقنيّات والإعلام الرقمي نحو تطبيقات الشبكات المظلمة على الإنترنت واعتمدت الدراسة على المنهج الوصفى واستخدام استمارة الاستبيان التى تم تطبيقها من خلال المقابلة المتعمقة حيث شملت الاستمارة مجموعة من الأسئلة المفتوحة هدفت إلى تحليل الدراسة بشكل كيفي ، وطبقت الدراسة على عينة عمدية مكونة من ٣٠ خبيرًا تم توزيعهم بالتساوى على المجالات الثلاثة، وأظهرت نتائج الدراسة اتفاق الخبراء فى المجالات الثلاثة على خطورة الأثار المسقبلية للشبكات المظلمة سواء من الناحية الإعلامية أو التقنية أو القانونية وقد جاءت تلك التوقعات استنادًا إلى اتفاق الخبراء فى المجالات الثلاثة على زيادة استخدام الشبكات المظلمة فى الأنشطة غير القانونية وجاء ابرزها على المستوى القانونى العمليات الإرهابية وعلى المستوى التقنى السرقات الإلكترونية وعلى مستوى الإعلام الرقمى نقل مواد إعلامية لا يرغب المشاهد فى رؤيتها ، وفيما يتعلق بأساليب مواجهة مخاطر الشبكات المظلمة اتفق الخبراء لا سيما فى المجال التقني والقانوني بأن هناك صعوبة فى تتبع مجرمى شبكات الدارك نتيجة الفجوة الرقمية، حيث يستحيل اختراقها تكنولوجيا، مما يجعل من الصعب تعقبهم من قبل السلطات القانونية وتطبيق القانون عليهم.

الكلمات المفتاحية: الاتجاهات ، الخبراء المصريين ، الشبكات المظلمة، الإعلام الرقمى

* الأستاذ المساعد بقسم الإذاعة والتليفزيون بكلية الإعلام وتكنولوجيا الاتصال-جامعة السويس

Attitudes of Egyptian Experts in the Fields of Legislation, Technology and Digital Media Towards the Applications of the Dark Web on the Internet

Abstract:

The current study aimed to identify the perspectives of Egyptian experts in the fields of legislation, technology, and digital media regarding the applications of dark networks on the internet. The study adopted a descriptive approach and utilized a questionnaire that was applied through in-depth interviews. The questionnaire included a set of open-ended questions that aimed to analyze the study qualitatively. The study was conducted on a purposive sample consisting of 30 experts, evenly distributed among the three fields. The results of the study revealed the consensus among experts in the three fields regarding the potential risks of dark networks, whether from a media, technological, or legal perspective. These expectations were based on the agreement among experts in the three fields regarding the increased use of dark networks in illegal activities. Notably, the study highlighted terrorist operations as a major concern from a legal standpoint, electronic thefts from a technological standpoint, and the transmission of undesirable media content from a digital media standpoint. Regarding the methods of confronting the risks of dark networks, experts, especially in the technological and legal fields, agreed that there are difficulties in tracking down criminals involved in dark networks due to the digital divide, making it technologically impossible to penetrate them and challenging for legal authorities to track and enforce the law upon them.

Keywords:Trends, Egyptian experts, dark webs, digital media

مقدمة:

فى الفترة الأخيرة تحديدًا فى عام ٢٠١٩ انتشرت خدمات جديدة لشبكة الإنترت تعرف بإسم شبكات الويب المظلمة ، فلم يعد الأمر يقتصر فقط على استخدام الإنترنت للمواقع المتعارف عليها بين جميع مستخدمى شبكة الإنترنت والتى تقتصر على مواقع البحث ومواقع وسائل التواصل الاجتماعى وهى المواقع الأشهر استخداماً عالمياً وفقًا لما أشارت إليه معظم الدراسات، ولكن يوجد عالم أخر غير مرئى لا سيما لفئة قليلة من المستخدمين نظرًا لطبيعة أستخدامها التى تحتاج لبرامج متخصصة حتى يمكن الدخول عليها هذا العالم يطلق عليها الشبكات العميقة أو الشبكات المظلمة ، والتى تقدم ما يقرب من ٢٢ خدمة لمستخدميها والتى تهدف معظمها إلى إفساد ليس فقط الأفراد المستخدمين لتلك النوعية من المواقع ولكن إفساد دول بأكملها ، وتركزت تلك الخدمات بين القرصنة، والقمار، والتزوير، والإباحية (*)، وغيرها من الخدمات التي تعكس الكثير من الأثار السلبية على الفرد والمجتمع. وأصبحت الشبكة المظلمة بيئة رقمية تلتقي فيها العديد من العناصر والجهات، التي تمثل تهديدًا للواقع، لا سيما أن تلك البيئة الرقمية تكاد تكون بمنأى من سلطات إنفاذ القانون. ولا يمكن الوصول إلى محتوى الويب المظلم إلا عبر برنامج خاصTOR ، لتشفير عنوان الـ IP للمستخدم وحزم مرور البيانات.

ونتيجة لظهور تلك النوعية من البيئات الرقمية التى من المحتمل أن تتحول إلى dark social وجب الوقوف للبحث والدراسة من الناحية التقنية والتشريعية والإعلام الرقمى ، لا سيما مع زيادة عدد مستخدمى تلك المواقع السرية باعتبارها منصات هامة لحرية لتعبير عن الرأى ليس فقط من خلال الكتابة وتبادل الأراء ولكن أيضًا التنفيذ على أرض الواقع طبقاً لمجالات إهتمام كل مستخدم فى المجالات التى تطرحها والتى تأتى فى معظمها مجالات إجرامية حسبما أشارت إلية العديد من الدراسات الأجنبية التى بحثت فى استخدامات الويب المظلم والتى قامت بتحليل الخدمات التى تقدمها الشبكات المظلمة لمستخدميها.

مشكلة الدراسة:

أثار ظهور الشبكات المظلمة العديد من التساؤلات من قبل الباحثين في شبكة الإنترنت، نظرًا لأنها تعد إحدى الشبكات الحديثة في المجال التقني إضافة إلى ذلك، أشارت نتائج الدراسات الحديثة التي أجريت على تلك الشبكات إلى المخاطر الناتجة عن استخدامها، تحديدًا من قبل الجماعات الإرهابية، حيث يتم استخدامها في التخطيط للعمليات الإرهابية وتجارة الأعضاء والسرقة الإلكترونية، نتيجة للقدر العالي من السرية والخصوصية التي توفرها تلك الشبكات لمستخدميها. ونتيجة لما سبق، تتحدد مشكلة الدراسة في التعرف على اتجاهات الخبراء في مجالات التشريع والتقنيات والإعلام الرقمي نحو الشبكات المظلمة وما قد تحدثه تلك الشبكات من تأثيرات مستقبلية على الفرد والمجتمع، وأبرز القضايا والموضوعات التي تتطرق إليها تلك الشبكات على مستوى مصر والعالم العربى.

أهمية الدراسة:-

١- يعد هذا البحث من البحوث العلمية الحديثة التى تتطرق للبحث فى هذا النوع من المواقع الذى يضمن العديد من الموضوعات والقضايا التى تشكل خطورة على المستخدمين حيث أشارت الدراسات التى أجريت حديثًا على الشبكات المظلمة إلى ارتفاع استخدام البرامج المشفرة التى تتطلب الدخول إلى الشبكات المظلمة.

٢- قلة الدراسات العربية التى تناولت مواقع الدارك ويب نظرًا لأنها تتطلب بعض التطبيقات الخاصة للدخول عليها.

٣- تفتح مجالاً جديداً للبحوث الإعلامية التى تهتم بدراسة الإعلام الرقمي.

أهداف الدراسة:-

١- استكشاف وتحليل اتجاهات الخبراء المصريين في مجالات التشريع والتقنيات والإعلام الرقمى نحو الشبكات المظلمة عبر الإنترنت.

٢- رصد العلاقة بين تعرض الخبراء فى مجالات التشريع والتقنيات والإعلام الرقمي وبين تشكيل اتجاهاتهم نحو الشبكات المظلمة عبر الإنترنت.

٣- كشف السلبيات والايجابيات التى يراها الخبراء فى مجالات التشريع والتقنيات والإعلام الرقمي للشبكات المظلمة عبر الإنترنت.

٤-تحديد الآثار المستقبلية لاستخدام الشبكات المظلمة عبر الإنترنت وتحليل التغيرات التي قد تحدث على مستوى الفرد والمجتمع، لا سيما ما أشارت إليه بعض الدراسات السابقة فيما يتعلق باستخدامها من قبل الجماعات المتطرفة في العمليات الإرهابية وربطها بالإسلام، نظرًا على لعدم القدرة على الكشف عن هوية تلك الجماعة وتأثيرها على صورة العرب والمسلمين.

٥-تحليل وتقييم الأساليب الممكنة لمواجهة ومكافحة مخاطر الدارك ويب، وذلك وفقاً لرؤية وتصور الخبراء في مجالات التشريع والتقنيات والإعلام الرقمي.

الإطار النظرى للدراسة:

تستند الدراسة الحالية إلى نموذج القيمة المتوقعة لفيشبان " Fishbine Expecting" value model لشرح عملية تشكيل اتجاهات الأفراد.

تقترح النظرية المطورة من قبل فيشباين في عام ١٩٧٥ أن الأفراد يمكنهم تطوير توقعات مستقبلية وفقًا للمنفعة المرتبطة بهذه الاتجاهات ، حيث يرى فيشباين أن الأفراد يقوموا باتجاهات ايجابية أو سلبية بناء على تلك التوقعات والتى تقوم على أساس المنفعة الناتجة عن هذا الاتجاه، [١] ، وتشير النظرية إلى أن المعتقدات والقيم تؤثر في تكوين المواقف وتعديلها، والفكرة الرئيسية للقيمة المتوقعة هي أن التوقعات والقيم والمعتقدات تؤثر في اتجاه الأفراد الذي يترجم في سلوك محدد. يحاول النموذج تحديد العوامل العقلية التي تحدث خلال تطور الموقف[٢]. ويتم قياس اتجاه الفرد في هذا النموذج بناءً على المعادلة التالية:

Attitude: اتجاه الفرد نحو الأشياء.

Beliefs: قوة الإعتقاد بالخصائص التى تمتلكها الأشياء موضع الإتجاه.

Affective : القيمة التأثيرية للشئ المتوقع.

ويشير النموذج إلى أن رغبة الفرد فى التصرف بشكل معين تعتمد بشكل كبير على النتيجة المتوقعة من قيامه بهذا السلوك، فعندما يكون هناك أكثر من سلوك يستطيع الشخص القيام به ، وأن السلوك المختار من قبل الشخص هو السلوك الذى يترتب عليه أكثر التوقعات الإيجابية الناجحة من حيث مدى تقييم الهدف بدرجة عالية ، والدرجة التي يتوقع الشخص أن ينجح بها [٣].

في هذا النموذج، يتم التأكيد على أن الأفراد يمتلكون توقعات وقيم ومعتقدات تؤثر على سلوكهم المستقبلي. التوقعات هي المعتقدات المحددة التي يحملها الأفراد بخصوص نجاحهم في مهام معينة سيقومون بتنفيذها في المستقبل، سواء كان ذلك في المدى القريب أو البعيد.

وتعتبر توقعات الأفراد عاملًا هامًا في تحديد سلوكهم المستقبلي، حيث يتأثر اختيارهم بتقييم المدى الذي يتوقعون فيه نجاح تلك المهام. بالإضافة إلى ذلك، تلعب القيم والمعتقدات الشخصية دورًا في توجيه السلوك وتحديد الأولويات والاهتمامات الشخصية. [٤]

كما يشـــير هذا النموذج إلى أن المعلومات والحقائق التى لها علاقة بمضمون أو وسيلة تختلف فى أوزانها النسبية من حيث درجة أهميتها، ويتوقف تكوين اتجاه الفرد نحو تلك المضامين أو الوسائل على إدراك الفرد للأهمية النسبية لهذه المعلومات التى تكون ذات تأثير فعال فى تكوين الاتجاه النهائى للفرد نحو الأشياء.[٥]

تطبيق النموذج فى الدراسة الحالية:

ترى الباحثة أن هذا النموذج مناسب للدراسة الحالية لعدة أسباب:

أولاً: يعتبر النموذج قادرًا على تحليل الشبكات المظلمة وفهم جوانبها الإيجابية، كما يسمح هذا النموذج بحرية التعبير وتمكين الرأي العام من تشكيل مجال عام موازٍ ويعطي الفرصة لدراسة النتائج والتأثيرات المحتملة لهذه الشبكات.

ثانيًا: يقوم النموذج المقترح بحساب الاتجاه العام بناءً على فروق الاتجاهات نحو السمات الإيجابية والسلبية لموضوع الدراسة. يتيح ذلك فهمًا أعمق للتوجهات والاهتمامات المختلفة للأفراد تجاه الموضوع، وبالتالي يمكن استخدام هذه المعلومات لتحسين الفهم والتأثير على السلوك المرغوب.

ثالثًا: باستخدام هذا النموذج، يمكن للباحثة تحليل البيانات والمعلومات المتاحة بشكل أفضل وتوجيه البحث نحو الجوانب الرئيسية التي تؤثر في السلوك والاتجاهات، كما يمكن أن يساهم هذا في تحقيق نتائج أكثر دقة وفهم أفضل للموضوع المدروس.

الدراسات السابقة:

تعرض الباحثة الدراسات السابقة التى لها علاقة مباشرة بعنوان البحث وذلك لقلة الدراسات التى أجريت في مجال الشبكات المظلمة ال Dark Web لا سيما الدراسات العربية.

فقد اهتمت بعض الدراسات بالتعرف على نوع الأنشطة التى يتم ممارستها عبر الشبكات المظلمة والفرق بينها وبين الأنشطة عبر الشبكات السطحية والتى يسهل الدخول عليها ولا تحتاج لأنواع محددة من التطبيقات، فقد بحثت دراسة (Sumeet Raghunath & Yache Vishal Shivra, 2022) فى الشبكة العميقة للوصول إلى أنواع الخدمات والأنشطة التى تقدمها وتحديد المساحة والطرق التى يمكن الدخول بها إلى تلك الشبكة وتقدير عدد مستخدميها وقد استخدمت الدراسة البرامج التى يمكن من خلالها الوصول إلى الشبكة العميقة وفى مقدمة تلك البرامج برنامج tor وتوصلت الدراسة إلى العديد من النتائج تمثل أهمها فى التقديرات إلى أن الويب العميق أكبر بنحو ٤٠٠ إلى ٥٠٠ مرة من سطح الويب العادى، لأنه لا يمكن قياس حجم شبكة الويب العميقة نظراً لأن غالبية المحتوى لا يمكن الوصول إليه ، كما أشارت النتائج أن هناك عدد كبير من مواقع الويب التي لم يتم اكتشافها بعد على شبكة الويب العميقة ، لأنه لم يتمكّن أحد من الوصول إلى هذا الموقع بدون روابط أو دعوات سرية، لأنه يجب الحفاظ على سرية الهوية أثناء الوصول إلى شبكة الويب العميقة، كما توصلت الدراسة إلى أن الخدمات التى تقدمها الويب المظلمة بشكل أساسي هى للأنشطة غير القانونية مثل السوق السوداء (سوق الشبكة المظلمة) ، والقرصنة ، والمواد الإباحية للأطفال ، والاحتيال ، والغرف الحمراء[٦]، وتساءلت دراسة Nuruddin Bin Razali , 2019)) ماذا يوجد داخل الويب المظلم ؟، حيث طبقت الدراسة استمارة تحليل مضمون للمعرفة المضامين التى تقدمها تلك النوعية من الشبكات التى ظهرت فى الألفية الجديدة وأظهرت نتائج الدراسة أن الويب المظلم يحتوي على العديد من ملفات الأنشطة غير المشروعة وفى مقدمتها المواد الإجرامية ، حيث أصبحت البيئة الأساسية لمجرمي الإنترنت التى ينضم إليها جميع مجرمي الإنترنت ويتجمعون فيه لممارسة ما أسمته الدراسة ب " قراصنة الظلام" ، كما توصلت الدراسة إلى أن أكثر الأنشطة التى تمارس بقوة عبر الشبكة المظلمة تتمثل فى (تاجر مخدرات ، إرهابي ، مبتكرو الفيروسات ، مجنونون بالجنس ، مشتهو الأطفال ، الملاحقون ، الإنترنت المتنمرون) وكل نشاط إجرامى لا يمكن تصوره يوجد عبر تلك الشبكة [٧]، وأكدت على النتائج السابقة دراسة كلاً من (Mohd Faizan and Raees Ahmad Khan,2019) حيث قامت الدراسة بتحليل محتوى ٢٥٧٤٢ نشاط عبر الدراك ويب، وأظهرت نتائج التحليل تباين تلك الأنشطة ما بين الانشطة غير القانونية وغير الأخلاقية مما يعزز من التصور السلبي للشبكات المظلمة على الرغم من ظهور ٢٣١ نشاط قانونى يتمثل فى مناقشة القضايا السياسية والموضوعات التى تتعلق بالعنصرية الدينية والطائفية فى البلدان الغربية .[٨].

وحذرت دراسة (shillito, Robert Matthew ,2019) من خطورة الشبكات المظلمة فى انتشار الجرائم الدولية لا سيما أن التقنية القائمة عليها تلك الشبكات هو حجب هوية مرتكبى الجرائم كما أوضحت نتائج الدراسة أنه لا يوجد قانون قادر على تقييد الجرائم المرتبكة عبر الويب المظلم ، وأن جميع التشريعات والهياكل التنظيمية غير قادرة على تتبع مرتكبى جرائم

الويب المظلم أو مجرد التقليل منها، [٩] وفى نفس السياق ، ألقت دراسة (رامى متولى القاضى ، ٢٠٢١) الضوء على استخدام شبكة الإنترنت المظلمة من جانب التنظيمات الإجرامية والإرهابية، وأكت النتائج على استغلال المجرمين استخدام تقنيات ً التشفير المعقدة التى تصعب عملية تعقبهم، مما يشكل عائقاً فى ملاحقة هذه العناصر وصعوبة إثبات الجرائم المرتكبة من الناحية القانونية، فقد أصبحت الشبكة المظلمة بيئة خصبة لمباشرة أنشطتهم الإجرامية، وتحقيق هذه الجماعات أرباح ضخمة من هذه الأنشطة غير المشروعة، باستخدامهم للعملات الافتراضية المشفرة.[١٠]

فى حين ركزت بعض الدراسات البحث فى علاقة الدراك ويب بالعمليات الإرهابية فقد توصلت نتائج دراسة (Natalia Grivas, 2018) التى قامت بتحليل مجموعة من العمليات الارهابية التى قامت بها داعش فى مجموعة متفرقة من الدول أن أنصار وأعضاء جماعة الدولة الإسلامية الإرهابية (ISIS) يستخدمون شبكة الويب المظلمة ليس فقط للدعاية من خلال الفيديو والصور والإعلانات ولكن أيضاً للتواصل مع بعضهم البعض أو مع الجهاديين الجدد في كل جانب من جوانب الكوكب باستخدام تطبيق الهاتف المحمول الذي يمكن الوصول إليه للتنزيل فقط من خلال الويب المظلم [١١]، بينما تطرقت دراسة (Goldman& others, 2019) إلى البحث فى كيفية تمويل العمليات الإرهابية عبر الشبكات المظلمة وأشارت نتائج الدراسة أن التمويل يتم عن طريق ما اسماه منظموا تلك العمليات " بالعملية الإفتراضية" فقد دعت بعض الجماعات الإرهابية إلى جمع تبرعات لها عبر الشبكات المظلمة "بعملة البتكوين" عن طريق محفظة إلكترونية للتبرع من خلالها للحصول علي التمويل اللازم للعمليات الإرهابية، مثل الحملة التى أُطلقت بعنوان "جهزونا"، وأكدت على النتائج السابقة دراسة (محمد على محمود ، ٢٠١٨) التى أوضحت أن عمليات التمويل للأنشطة غير القانونية عبر الشبكات المظلمة وفى مقدمتها العمليات الإرهابية تتم باستخدام العملات المشفرة المستحدثة التى تتميز بسهولة تحويلها وصعوبة تتبعها من قبل السلطات الحكومية.[١٣] ، كما ذكرت دراسة بحثية أجراها (مركز المعلومات ودعم اتخاذ القرار بمجلس الوزراء المصرى، ٢٠٢٠) بعنوان "أسواق الإنترنت المظلمة"marketplaces web Dark ؛ أن عائدات التعاملات على مواقع الإنترنت المظلم شهدت ارتفاعاً ملحوظاً لتصل إلى ٣,١ مليار دولار عام ٢٠٢٠ مقابل ١,٥ مليار دولار فى ٢٠١٩ ، وأن عمليات الشراء على تلك المواقع تتم عن طريق "العملات الرقمية المشفرة" وفى مقدمتها عملة " البيتكوين" [١٤]

واهتمت دراسة (Julia Ebner and Cécile Guerin, 2019) بالبحث فى دور الشبكات المظلمة في نشر التطرف بين الأوروبيين، وقد أجرت الدراسة تحليل للحادث الارهابى الذى وقع فى " كرايستشيرش" جنوب نيوزيلندا وتوصلت النتائج الى أن الإرهابيون، في الوقت الحالي، بحاجة إلى خدمات وسائل الإعلام التقليدية لتوثيق وبث جرائمهم التي تغذيها الكراهية، بل إنهم بمساعدة الإنترنت وأدوات بث الفيديو المباشر، يمكنهم بأنفسهم القيام بذلك، وهذا ما فعله منفذ هجوم كرايستشيرش من خلال استخدام شبكات الإنترنت المظلم، وما يُميز تلك الشبكات أنها تسمح بتدشين المواقع الإلكترونية ونشر المعلومات بدون الكشف عن هُوية الناشر أو موقعه. [١٥]

وأوضحت دراسة (Saini, Jaspal Kaur and Bansal, Divya, 2019) خطورة الشبكات المظلمة فى ربط العمليات الإرهابية بالإسلام حيث استغلت الجماعات الإرهابية المزايا التى تتمتع بها الشبكة المظلمة فى إخفاء هوية مستخدميها وتم تشويه صورة الإسلام من خلال إطلاق أسماء إسلامية على المنتديات التى قامت الدراسة بتحليلها ، نذكر منها على سبيل المثال "شبكة أنصار الجهاد" و"الإيقاظ الإسلامى" و "جواهر" و "الشبكة الإسلامية". (١٦)

وقدمت دراسة (Gabriel Weimann,2016) تقارير عن بعض الاتجاهات الحديثة في الاستخدام الإرهابي لشبكة الويب المظلمة للتواصل وجمع الأموال وتخزين المعلومات والمواد عبر الإنترنت ، وقد استخدمت الدراسة متصفح TOR للوصول للشبكة والتعرف الأساليب التى يتبعها الإرهابيين مع بعضهم البعض فى الدول المختلفة لتنفيذ العمليات الإرهابية دون الكشف عن هويتهم وقد طبقت تلك الدراسة بعد تنفيذ الارهابيين مجموعة من خدماتهم الارهابية فى باريس وتوصلت إلى مجموعة من النتائج جاء فى مقدمتها استخدام الإرهابيين شبكة الإنترنت المظلمة لتوفير المعلومات لزملائهم ، للتجنيد والتطرف ونشر الدعاية وجمع الأموال وتنسيق الأعمال والهجمات على سبيل المثال ، في ١٥ تشرين الثاني / نوفمبر ٢٠١٥ ، بعد يومين من هجمات باريس ، نشر تنظيم الدولة الإسلامية رسالة يناقش فيها موقع إسدارات الرسمي الذي يقوم بأرشفة الدعاية ، واحتوت الرسالة على روابط مخفية خدمة Tor بعنوان ".onion" ، مما يشير إلى انتقال منفذ Isdarat إلى Dark Web (١٧)، وحللت دراسة (Emily Chiang ,2020) كيفية انخراط الجناة الجدد في مجتمعات المتحرشين بالأطفال عبر الإنترنت المظلم ورصدت مجموعة من المواقع والمنتديات والشبكات الاجتماعية المشفرة بشدة التى توفر مساحات كبيرة للإتجار بالأطفال لا سيما الدول الفقيرة، وقامت الدراسة بتحليل يدوي لـ ٧١ مشاركة من ستة منتديات خاصة بالإتجار بالأطفال ، وكشفت الدراسة عن ١٢ خطوة مختلفة للمستخدمين المهتمين بالإتجار بالأطفال(١٨)، بينما رصدت دراسة (Navi Mumbai & Maharashtra 2018) المشكلات الكبرى التى واجهتها البنوك المركزية في العالم بسبب المعاملات المالية التي تمت باستخدام التشفير للعملات غير الخاضعة للضريبة، هذه العملات مهمة جدًا للويب العميق لأن جميع المعاملات على الويب المظلم تتم باستخدام العملات المشفرة فقط، هؤلاء العملات تستخدم ليس فقط لعدم الكشف عن هويتها ، ولكن هذه العملات هي أيضا لامركزية وتقدم معاملة آمنة للغاية من الدفع المنتظم للقيام بالعمليات غير القانونية (١٩) ، ونوهت دراسة (Duxbury& Haynie,2018) على خطورة الشبكات المظلمة فى تجارة الأدوية لا سيما المواد المخدرة ، فقد توصلت النتائج أن شبكة "الدارك ويب" تعد من أولى شبكات توزيع الأدوية المشفرة عبر الإنترنت ، وأشارت أن نسبة ٨٧% من تلك الأدوية تندرج تحت المواد المخدرة غير العادية والتى تهدف إلى تدمير الخلايا العصبية مما يؤكد على خطورة تلك الشبكة فى بيع المواد المخدرة المحظور استخدامها عالميًا.(٢٠)

وفى المقابل تناولت القليل من الدراسات الاستخدام المشروع للدارك ويب فقد توصلت دراسة (Carly Chatfield,2022) أن هناك أيضًا استخدامات مشروعة لشبكة Dark Web على سبيل المثال ، يمكن للأشخاص في البلدان التي تنتشر فيها الرقابة استخدام شبكات الويب المظلمة لمشاركة المعلومات ومعرفة ما يحدث في العالم مع حماية خصوصيتهم وعدم الكشف

عن هويتهم، و يمكن للصحفيين والمبلغين والأشخاص المهتمين بالخصوصية استخدام الويب المظلم لزيادة إخفاء هويتهم وتجاوز الرقاب،ة بالإضافة إلى ذلك يمكن للأفراد مثل هؤلاء استخدام تقنيات مثل متصفح Tor ليس فقط للوصول إلى Dark Web ، ولكن لتصفح الإنترنت بشكل مجهول (٢١) ، وأكدت على تلك النتائج دراسة كلاً من(Mihnea Mirea,Victoria Wang & Jeyong Jung,2019) التى بحثت فى الجانب المشرق أو غير المظلم "للدارك ويب" حيث أكدت على أنه بالرغم من السمعة السيئة التى اكتسبتها الشبكات المظلمة، إلا أن هناك جانب أخر يسمى "بالجانب المشرق" لتلك الشبكة وذلك نتيجة لاعطائها قدر كبير من الحرية لمستخدميها الذين لا يستطيعون التعبير عن أرائهم بحرية تجاه سياسات الدول التى ينتمون إليها، فالسرية التامة التى توفرها الشبكات المظلمة لبيانات مستخدميها تشجعهم وتحمسهم وتوفر لهم الأمان للدخول والتعبير عن أرائهم بحرية دون الخوف من اعتقالهم من قبل الحكومات التى ينتقدونها (٢٢)، واتفقت مع النتائج السابقة نتائج دارسة (Daniel Moore & Thomas Rid, 2016) التى أوضحت أن الشبكات المظلمة أصبحت مصدر هام لممارسة الحريات، حيث يمكن للأفراد مشاركة ملفاتهم الاجتماعية والمعتقدات السياسية وخلافاتهم مع حكوماتهم أو توقعاتهم دون الخوف من القصاص، و هذه المشاركة ضرورية بشكل خاص في البلدان التي لديها رقابة شديدة ضد النشطاء السياسيين ، ومقاتلي الحرية (٢٣)، وناقشت دراسة **(Arbër S. Beshiri ,2019 , Arsim Susuri**) تأثير شبكة الويب المظلمة فى مختلف المجالات ، ومن التأثيرات الإيجابية التى رصدتها الدراسة أن الشبكة المظلمة ساعدت بفضل الخصوصية التى تتمتع بها من اخفاء هوية مستخدميها قيام رجال الشرطة برصد أخطر المجرمين فى الأنشطة غير القانونية والتى كان لها تأثير إيجابى مجتمعى فعلى سبيل المثال ، فقد حققت نجاحًا كبيرًا في إزالة المواقع واعتقال مستخدميها والأشخاص الذين يقفون وراءها، كان أشهرها اعتقال روس أولبريشت ، الشخص الذي يقف وراء أشهر أسواق المخدرات، وفي قضية أخرى سيئة السمعة ، حُكم على مدير موقع Playpen الإباحي للأطفال على الإنترنت بالسجن لأكثر من ٣٠ عامًا، كما تم القبض على ستيفن تشيس من قبل مكتب التحقيقات الفيدرالي بعد الكشف عن غير قصد عن عنوان الإنترنت الحقيقي للموقع. وبحسب ما ورد قُبض على ٨٧٠ شخصًا آخرين على صلة بالموقع (٢٤).

ومؤخرًا رصدت دراسة حديثة أجراها مركز (Cybercrime and Dark Web Research,2022) الاستخدامات القانونية لشبكات الويب المظلمة، والتى تنوعت مابين الاستخدامات الإعلامية والمالية والأكاديمة، وجاءت أهم تلك الاستخدامات فى إتاحة شبكات الدارك ويب التعاون المجهول مع الصحفين فقد يشعر بعض الأشخاص ، مثل المبلغين عن المخالفات بالراحة في الاتصال بالصحفيين تحت ستار إخفاء الهوية، والوصول إلى البحث الأكاديمى الذى يصعب غالبًا الوصول إليه مما يتعين على الباحث دفع رسوم باهظة للوصول إلى مقال واحد، كما أشارت النتائج إلى تأمين محافظ العملات الرقمية الخاصة بالمستخدم، بينما تتمتع العملات المشفرة مثل البيتكوين بفوائد لا حصر لها ، ومن أهمها صعوبة تتبع عملة معينة (٢٥)، وفيما يتعلق بالاستخدامات المحتملة لشبكات الدارك فى المستقبل القريب اهتمت دراسة (رحاب أحمد فايز، ٢٠١٩)، بالبحث عن الاستخدامات المحتملة للويب المظلم القانوني

منها وغير القانوني، وكيف يمكن تجنب غير المشروع منها ، وتوصلت النتائج أن من أكثر الاستخدامات غير القانونية للشبكات تتمثل فى شراء المخدرات والأسلحة وتجارة الأعضاء البشرية والجماعات التخريبية ، ومواقع الاحتيال المالي التي تتضمن بيع أرقام حسابات بنكية وبطاقات إئتمانية مسروقة ، ومواقع الشبكات الروبوتية ، ومواقع مجموعات الاختراق المأجورة لتحقيق الكسب المادي بنشر البرمجيات الخبيثة ومواقع المتديات لمناقشة الموضوعات المحظورة مثل السلاح والأفكار المتطرفة ، وقد توصلت نتائج الدراسة أن من أكثر الاستخدامات القانونية للشبكات المظلمة ، توفير أكبر مكتبية افتراضية لكل الباحثين والطلاب والمدرسين لكون المحتوى المتوافر عليه غير متاحٌ فى محركات البحث التقليدية [٢٦].

التعليق على الدراسات السابقة

١- اتفقت معظم الدراسات السابقة على خطورة شبكات الدارك والمتمثلة فى ممارسة الأنشطة غير القانونية وأكدت على أن تلك الشبكات تتمتع بمميزات تساعدعلى إنتشار كافة الجرائم بأنواعها دون تعقب ممارسيها.

٢- أشارت القليل من الدراسات أن الشبكات المظلمة تتمتع ببعض الإيجابيات والتى تتمثل فى حرية التعبير عن الرأي لا سيما فى البلدان التى لها رقابة شديدة على النشطاء السياسين بالإضافة إلى التأثيرات الإيجابة للشبكات المظلمة، حيث ساعدت رجال الشرطة بتتبع وإلقاء القبض على أخطر المجرمين فى ممارسة الأنشطة غير القانونية.

٣- اعتمدت الدراسات الأجنبية على المنهج التحليلي للأنشطة الإجرامية التى تمارس عبر الشبكات المظلمة واتفقت نتائجها على أن من أبرز تلك الأنشطة العمليات الإرهابية وعمليات الاحتيال والسرقات الإلكترونية بالإضافة إلى تجارة المخدرات والإتجار بالبشر.

٤- تناولت الدراسات العربية وهم دراستان فقط تحليل الأدبيات التى تمت فى مجال الويب المظلم والجوانب القانونية لها ولم يتم التطرق إلى تحليل مضمون لتلك الشبكات.

تساؤلات الدراسة وفروضها:

التساؤلات:

اعتمدت الدراسة على مجموعة من التساؤلات الكمية والكيفية لتحقيق الأهداف التى تسعى إليها.

١- ما مدى تعرض الخبراء فى المجال التشريعى والتقني والإعلام الرقمي للشبكات المظلمة؟

٢- ما القضايا والموضوعات الأكثر إثارة للجدل في الشبكات المظلمة وما علاقتها بمصر والعالم العربي؟

٣- ما الجوانب السلبية والإيجابية التى يراها الخبراء في المجال التشريعى والتقني والإعلام الرقمي فى الشبكات المظلمة؟

٤- ما الأثار المستقبلية التى يراها الخبراء فى المجال التشريعى والتقني والإعلام الرقمي لاستخدام الشبكات المظلمة على الفرد والمجتمع؟

٥- ما الاستخدامات المستقبلية للدارك ويب القانونية وغير القانونية من وجهة نظر المبحوثين؟

٦- ما الأساليب الممكن اتباعها على المستوى الإعلامى والتشريعى والتقني لمواجهة مخاطر الدارك الويب من وجهة نظر المبحوثين ؟

الفروض:

١- توجد علاقة ارتباطية دالة احصائيًا بين حجم تعرض الخبراء فى المجالات الثلاثة وبين تشكيل اتجاهاتهم نحو الشبكات المظلمة.

٢- توجد علاقة ارتباطية دالة احصائيًا بين درجة اهتمام الخبراء فى المجالات الثلاثة بالشبكات المظلمة وبين تشكيل اتجاهاتهم نحوها.

٣- توجد فروق دالة احصائيًا بين تخصصات الخبراء فى المجالات الثلاثة وبين درجة اهتمامهم بالتعرض للشبكات المظلمة.

التصميم المنيجي للدراسة

نوع الدراسة ومنهجها:

تندرج تلك الدراسة ضمن الدراسات الوصفية التى تهتم بدراسة واقع الأحداث والظواهر فى الوقت الحاضر فهى تتناول موضوعات موجودة بالفعل وقت اجراء الدراسة وتقوم بتحليلها تحليلًا دقيقًا ويتم من خلال تلك الدراسة وصف اتجاهات الخبراء فى الثلاث مجالات المختلفة (التشريع والتقنية والاعلام الرقمى) وقياس معارفهم وتقييماتهم وتحديد اتجاهاتهم نحو تطبيقات الشبكات المظلمة ال Dark Web

عينة الدراسة وأسباب إختيارها:

تعتمد تلك الدراسة على العينة العمدية ، فقد تم تحديد العينة بناء على عنوان الدراسة وهم الخبراء فى المجال التشرعى والتقنى والإعلام الرقمى ، حيث تتيح تلك العينة للباحثة تحقيق أهداف البحث لما توفرة من خصائص وسمات مقصودة ترتبط بمشكلة البحث ، وتم مراعاة أن تكون العينة مرتبطة ارتباط مباشر بموضوع البحث وقد بلغت عينة الدراسة (٣٠) مبحوث من الخبراء تم تقسيمها بالتساوى بواقع ١٠ مبحوثين فى كل مجال من المجالات الثلاثة:

١- الخبراء فى مجال التشريع ويشمل (١٠)

٢- الخبراء فى مجال التقنيات ويشمل (١٠)

٣- الخبراء فى مجال الإعلام الرقمى ويشمل (١٠)

<u>أداة جمع البيانات:-</u>

قامت الباحثة بتصميم استمارة استبيان تم تطبيقها من خلال المقابلة المتعمقة بهدف قياس متغيرات الدراسة واختبار فروضها في إطار " نموذج فيشباين " وتم تصميمها مكونة من خمسة محاور رئيسية تضمنت مجموعة من الأسئلة التى تحدد الغرض من الدراسة **المحور**

الأول : يشمل الأسئلة الخاصة بالبيانات الشخصية لمعرفة خصائص العينة (السن- المستوى التعليمى – الدرجة الوظيفية - التخصص)، **وتناول المحور الثانى** : مدى اهتمام الخبراء بالتعرض لشبكات الدارك وأسباب التعرض إليها، بينما تضمن **المحور الثالث:** أهم القضايا والموضوعات التى تثيرها تلك النوعية من الشبكات لا سيما التى تتعلق بمصر والعالم العربى وما أكثر التطبيقات التى يعتمد عليها مستخدمى الدارك ويب للدخول إليها، وتناول **المحور الرابع** : قياس اتجاه الخبراء فى المجالات الثلاثة من خلال تحديد الجوانب السلبية والإيجابية التى يراها الخبراء فى مجالات التشريع والتقنية والإعلام الرقمى فى الشبكات المظلمة، وتضمن **المحور الخامس:** الأثار المستقبلية التى يراها الخبراء فى المجالات الثلاثة لاستخدام الشبكات المظلمة على الفرد والمجتمع، بينما تضمن **المحور السادس** : الاستخدامات المستقبلية للشبكات المظلمة التى يتوقعها الخبراء فى المجالات الثلاثة عينة الدراسة ، بينما تناول **المحور السابع:** تحديد الأساليب التى يمكن من خلالها مواجهة مخاطر تلك الشبكات من وجهة نظر الخبراء فى المجالات الثلاثة عينة الدراسة.

واعتمدت الباحثة على المقايس الثالية :-

مقياس ليكرت الخماسى (Likert Scale) الذي يقيس شدة الاتجاه لدى الرأي العام حول القضية المطروحة في وسائل الإعلام ، وتم قياس اتجاهات المبحوثيين من خلال ١٣ عبارة ، وقد وضعت خمس درجات تفضيل أمام كل عبارة لقياس الاتجاه وتحديد نوعه بـ (موافق بشدة)، و(موافق) و(محايد) ، و(معارض) ، و(معارض بشدة).

صدق الأداة وثباتها:

استخدمت الباحثة أسلوب الصدق الظاهري Face Validity ، من خلال تصميم استمارة المقابلة المتعمقة في ضوء أهداف الدراسة وتساؤلاتها وفروضها، وفي ضوء مراجعة الدراسات السابقة وتم إجراء اختبار قبلي على ١٢ مبحوث، وتم عرضها في صورتها الأولية على مجموعة من المحكمين(*) على مجموعة من المحكمين للتأكد من مدى قدرتها وصلاحيتها للتطبيق وتحقيق أهداف البحث وقد تم إجراء التعديلات بناء على أراء المحكمين قبل إعدادها في صورتها النهائية.

وللتأكد من ثبات الأداة البحثية تم إعادة التطبيق مرة أخرى بعد مرور أسبوعين من التطبيق الأول ، وبلغت نسبة الثبات ٩٥% مما يدل على الثقة فى النتائج التى أسفرت عنها الدراسة الحالية.

مفاهيم الدراسة:-

ال Dark Web:- تعد الشبكات المظلمة مجموعة من المحتويات المشفرة عبر الإنترنت والتي لا يمكن الوصول إليها عن طريق محركات البحث التقليدية، بل تتطلب استخدام برمجيات محددة مثل Tor للوصول إليها، وتُعَد الشبكة المظلمة جزءًا من الويب العميق، الذي يصف النطاق الواسع للمحتوى الذي يمكن الوصول إليه فقط من خلال أنشطة التصفح المخصصة.

وعلى الرغم من أن الشبكات المظلمة يُصوَّر بعض الأحيان على أنها بيئة مغلقة للأنشطة الإجرامية، وقد صنَّفتها العديد من الدراسات على هذا النحو، إلا أنها تُستخدم أيضًا من قبل

الأفراد الذين يحتاجون إلى الخصوصية التامة في الأعمال التجارية والاقتصادية التي تتطلب السرية والحماية الشديدة لهويتهم.

الإتجاه:- هو الرأي أو الاعتقاد الذي يحمله الفرد بشأن موضوع معين، سواء كان مؤيدًا أم معارضًا، ويتكون هذا الاعتقاد بناءً على خبرات سابقة للشخص وتفاعله مع الأفراد والبيئة المحيطة به، وإذا كان الاعتقاد يتفق مع الخبرات المسبقة والقيم والمعتقدات الشخصية والتاثيرات الاجتماعية والثقافية، فإن ذلك يعزز الاتجاه ويعزز قناعة الشخص برأيه، ومن الجدير بالذكر أن الاعتقادات الشخصية قد تتغير مع مرور الوقت نتيجة اكتساب معلومات جديدة أو تفاعل مع وجهات نظر مختلفة.

النتائج:-

سوف تعرض الباحثة نتائج الدراسة الحالية من خلال مستوين :

المستوى الأول النتائج الإحصائية للدراسة

جدول (١) مدى تعرض الخبراء فى المجالات الثلاثة للشبكات المظلمة

مدى التعرض	ك	%
يومياً	١٠	٣٣,٣
أسبوعياً	١	٣,٣
عند الحاجة للبحث عن موضوع محدد فى مجال التخصص.	١٢	٤٠
وقت التحدث عنها فى وسائل الإعلام	٧	٢٣,٣
الإجمالى	٣٠	-

تشير بيانات الجدول السابق إلى ارتفاع تعرض الخبراء فى المجالات الثلاثة للشبكات المظلمة وقد تركز وقت التعرض لها (عند الحاجة للبحث عن موضوع محدد فى مجال التخصص) وذلك بنسبة ٤٠% ، بينما جاء التعرض لها بشكل يومى بنسبة ٣٣,٣% ، وتدل تلك النسب على أن الشبكات المظلمة من المواقع التى تلقى اهتمام كبير من جانب الخبراء بالتعرض لها ويرجع ذلك لطبيعة تخصصات الخبراء التى ترتبط بتلك النوعية من شبكات الإنترنت.

جدول (٢) مدى اهتمام الخبراء فى المجالات الثلاثة بالدخول على الشبكات المظلمة

درجة الاهتمام	ك	%
كبيرة	١٢	٤٠
متوسطة	١١	٣٦,٧
ضعيفة	٧	٢٣,٣
الإجمالى	٣٠	-

يتضح من بيانات الجدول السابق اهتمام الخبراء فى المجالات الثلاثة بالدخول على الشبكات المظلمة ، حيث أشارت نسبة ٤٠% بالاهتمام بدرجة كبيرة ، ونسبة ٣٦,٧% بالاعتمام بدرجة متوسطة بينما ظهر الاهتمام بدرجة ضعيفة بنسبة ٢٣,٣% ، وتلك النسب تشير إلى أهمية تلك النوعية من شبكات الإنترنت سواء على المستوى التقني أو التشريعى أو الإعلام الرقمي.

جدول (٣) أنماط تعرض الخبراء فى المجالات الثلاثة للشبكات المظلمة

أنماط التعرض	ك	%
أنضم للمجموعات المستخدمة للشبكة للبحث عن موضوع فى مجال التخصص.	١٣	٤٣,٣
التصفح فقط.	٦	٢٠
استخدام التطبيقات التى تساعدنى على الدخول للشبكة للتعمق فى الموضوعات المطروحة.	١١	٣٦,٧
الإجمالى	٣٠	-

تظهر نتائج الجدول السابق تفاعل الخبراء فى المجالات الثلاثة مع ما تقدمة الشبكات المظلمة عبر الإنترنت حيث ظهر(الانضمام للمجموعات المستخدمة للشبكة للبحث فى موضوع التخصص) والذى يمثل درجة عالية من درجات التعرض النشط وذلك بنسبة ٤٣,٣%، وظهور (استخدام التطبيقات التى تساعدنى على الدخول للشبكة للتعمق فى الموضوعات المطروحة) بنسبة ٣٦,٧% فى حين ظهر أقل درجة للتعرض الغير نشط وهو التصفح فقط بنسبة ٢٠%.

وتتفق تلك النتائج مع نتائج التحليل الكيفى للدراسة والتى أكدت على تعرض الخبراء النشط لشبكات الدارك والتى اتضح فى اجاباتهم عن الإستخدامات والأثار المستقبلية لتلك النوعية من الشبكات.

جدول (٤) الجوانب السلبية التى يراها الخبراء فى المجالات الثلاثة للشبكات المظلمة

العبارات التى تقيس الجوانب السلبية فى الشبكات المظلمة	موافق		محايد		معارض	
	ك	%	ك	%	ك	%
التعرض للكثير من المشاكل القانونية.	١٢	٤٠	١١	٣٦,٧	٧	٢٣,٣
إمكانية شراء أو بيع الأشياء غير القانونية والحذر منها بشدة.	٢٦	٨٦,٧	-		٤	١٣,٣
مواجهة العديد من الذين يعملون في (Dark Web) من خلال استغلال المستخدمين بأي طريقة وخداعهم لإعطاء معلومات.	٢٢	٧٣,٣	-	-	٧	٢٣,٣
احتمال حدوث أضرار نفسية بسبب الأنشطة غير القانونية وإيجاد مواد مزعجة	١٧	٥٦,٧	١٠	٣٣,٣	٣	١٠
إصابة بعض مواقع الويب لأجهزة الحاسوب بالفيروسات وتتعدد بأنواعها.	٢٢	٧٣,٣	٨	٢٦,٧	-	-
يمكن العثور على العديد من منتديات القراصنة على شبكة الإنترنت	٢٤	٨٠	٣	١٠	٣	١٠
يمكن للقراصنة القيام بأنشطة غير قانونية، والاستعداد لاختراق أجهزة الحاسب	٢٨	٩٣,٣	٢	٦,٧	-	-
تساعد تلك الشبكات فى تشويه صورة العرب والمسلمين نتيجة اخفاء هوية الجماعات الارهابية الحقيقة	٢١	٧٠	٦	٢٠	٢	٦,٧
تقف تلك النوعية من الشبكات حائلًا أمام مشروعات التنمية المستدامة نتيجة استقطاب الجمهور للأعمال غير المشروعة	١٢	٤٠	١٤	٤٦,٧	٣	١٠
الوصول إلى المواد غير القانونية أو الصور غير اللائقة للأطفال أو المواقع الخطرة	٢٦	٨٦,٧	٢	٦,٧	٢	٦,٧
الإجمالى	٣٠					

تشير بيانات الجدول السابق إلى ظهور عبارة (يمكن للقراصنة القيام بأنشطة غير قانونية، والاستعداد لاختراق الأجهزة) بنسبة ٩٣,٣% يليها فى الترتيب الثانى (إمكانية شراء أو بيع الأشياء غير القانونية والحذر منها بشدة، الوصول إلى المواد غير القانونية أو الصور غير اللائقة للأطفال أو المواقع الخطرة) بنسب متساوية ٨٦,٧%، بينما ظهر فى الترتيب الأخير بنسب متساوية (التعرض للكثير من المشاكل القانونية، تقف تلك النوعية من الشبكات حائلًا أمام مشروعات التنمية المستدامة نتيجة استقطاب الجمهور للأعمال غير المشروعة) بنسبة ٤٠% وتتفق تلك النتائج مع نتائج التحليل الكيفي للخبراء فى المجالات الثلاثة والتى أسفرت عن الاستخدام غير القانونى للشبكات المظلمة مثل انتشار الجرائم لا سيما اختراق أجهزة الحاسب بغرض السرقات الالكترونية والاتجار بالبشر والعمليات الإرهابية، وهذا أيضًا ما أسفرت عنه نتائج الدراسات السابقة والتى أجمعت على توظيف شبكات الدارك فى الأعمال غير القانونية نظرًا للميزة التى تتميز بها تلك الشبكات وهى " صعوبة الكشف عن هوية مستخدميها" مما يساعدهم على استخدامها فى الأنشطة الإجرامية بكافة أنواعها.

جدول (٥) الجوانب الإيجابية التى يراها الخبراء فى المجالات الثلاثة للشبكات المظلمة

العبارات التى تقيس الجوانب الإيجابية فى الشبكات المظلمة.	موافق		محايد		معارض	
	ك	%	ك	%	ك	%
يمكن الوصول الى معلومات أو مقالات غير موجودة على مواقع الإنترنت المتعارف عليها.	٢٠	٦٦,٧	١٠	٣٣,٣	-	-
تعد من أفضل الطرق للكسب إذا ما أجيد إستخدامها.	٨	٢٦,٧	٩	٣٠	١٣	٤٣,٣
تنشر شبكة الدارك ويب فى بعض الأحيان بعض الملفات السربة أو ما يثير الدهشة أو ما يعلمك شيء جديدا.	١٩	٦٣,٣	١١	٣٦,٧	-	-
تساعد الشبكات المظلمة جميع الافراد فى التعبير عن أرائهم بحرية دون فرض قيود.	١٤	٤٦,٧	١٢	٤٠	٤	١٣,٣
يستخدمه العديد من الصحفيين والنشطاء المدنيين لنشر بعض التقارير التي تفضح ملفات الفساد.	١٩	٦٣,٣	١١	٣٦,٧	-	-
ينشر الدارك ويب العديد من الوثائق الحقيقية والتى لا يستطيع الإعلام أو الإنترنت السطحى الوصول إليها أو نشرها.	١٧	٥٦,٧	١١	٣٦,٧	٢	٦,٧
يعد الدارك ويب بيئة جيدة للكشف عن تورط لبعض الحكومات في إعمال تنتهك حقوق الإنسان مثل ما حدث مع مسلمى الروهينجا.	١٧	٥٦,٧	١٠	٣٣,٣	٣	١٠
الإجمالى	٣٠					

تشير بيانات الجدول السابق إلى ظهور عبارة (يمكن الوصول الى معلومات أو مقالات غير موجودة على مواقع الإنترنت المتعارف عليها) فى الترتيب الأول للجوانب الايجابية للشبكات المظلمة التى يراها الخبراء فى المجالات الثلاثة بنسبة ٦٦,٧% يليها فى الترتيب الثانى بنسب متساوية (تنشر شبكة الدارك ويب فى بعض الأحيان بعض الملفات السربة أو ما يثير الدهشة أو ما يعلمك شيء جديدا، يستخدمه العديد من الصحفيين والنشطاء المدنيين لنشر بعض التقارير

التي تفضح ملفات الفساد) ٦٣,٣% بينما ظهر فى الترتيب الأخير (تعد من أفضل الطرق للكسب إذا ما أجيد إستخدامها) بنسبة ٢٦,٧%.
وتتفق النتائج السابقة مع نتائج التحليل الكيفى للخبراء فى مجال الإعلام الرقمى ، حيث أكد الخبراء على إمكانية استفادة الصحفيين من تلك الشبكات التى تساعدهم فى الحصول على المعلومات على سبيل المثال أنه غالبًا ما يستخدم الصحفيون متصفح Tor للتواصل مع المخبرين للحصول على المعلومات لضمان سلامتهم من حكوماتهم، وكما تفقت النتائج السابقة مع نتائج دراسة (Daniel Moore & Thomas Rid, 2016) التى أوضحت أن الشبكات المظلمة أصبحت مصدر هام لممارسة الحريات لا سيما البلدان التى لديها رقابة شديدة ضد النشطاء السياسيين.

جدول (٦) درجة موافقة الخبراء فى المجالات الثلاثة على أبرز الأحداث التى تمت من خلال الشبكات المظلمة

أبرز الأحداث التى تمت من خلال الشبكات المظلمة.	موافق		محايد		معارض	
	ك	%	ك	%	ك	%
نجحت منظمة آوم شيريكو الإرهابية اليابانية باختراق نظام البرمجة المتحكم في مسار أعداد هائلة من سيارات الخدمة العامة، بواسطة التلاعب بأنظمة الحاسب والإنترنت من تعطيل أنظمة أكثر من خمسين شركة يابانية كبرى واختراق أنظمة عشر إدارات حكومية وتوجيهها لصالحها	١٩	٦٣,٣	٤	١٣,٣	٧	٢٣,٣
استطاعت الجماعات الارهابية الدولية بتنفيذ مجموعة من الهجمات الأخيرة التى وقعت فى فرنسا وبيلجيكا من خلال شراء الأسلحة عبر الشبكات المظلمة].	٢١	٧٠	٣	١٠	٦	٢٠
تلجأ التنظيمات الإرهابية إلى مواقع ومنصات خاصة بها على الـ "دارك ويب" لتجنيد الشباب من كافة أنحاء العالم.	٢٢	٧٣,٣	٣	١٠	٥	١٦,٧
ساعدت شبكات الدراك ويب تنظيم داعش على تنفيذ مجموعة كبيرة من العمليات الإرهابية فى سوريا والعراق منذ اندلاع ثورات الربيع العربى.	٢١	٧٠	٥	١٦,٧	٤	١٣,٣
عمليات غسيل الأموال وتمويل الإرهاب وأنشطة الجريمة المنظمة تتم من خلال النقود المشفرة عبر الشبكات المظلمة الدارك ويب.	٢٣	٧٦,٧	٣	١٠	٤	١٣,٣
الإجمالى	٣٠					

تشير بيانات الجدول السابق إلى ارتفاع درجة موافقة الخبراء فى المجالات الثلاثة على توظيف الشبكات المظلمة فى الأعمال الإرهابية حيث ظهرت عبارات (عمليات غسيل الأموال وتمويل الإرهاب وأنشطة الجريمة المنظمة تتم من خلال النقود المشفرة عبر الشبكات المظلمة الدارك ويب) بنسبة ٧٦% وبالنظر إلى درجة وعارضة الخبراء فقد ظهرت بنسب منخفضة جداً مما يدل على ان الوظيفى الأساسية للشبكات المظلمة هى تنفيذ العمليات الإرهابية بينما ظهر فى الترتيب الأخير استخدامها فى إختراق وتعطيل أنظمة الحاسب وذلك بنسبة ٦٣,٣%. وتتفق النتائج السابقة مع ما توصلت إليه نتائج الدراسات السابقة والتى أجمعت أن استخدام الشبكات

المظلمة يشكل الأولوية في الأنشطة الإرهابية تؤكد هذه النتائج أيضًا نتائج التحليل الكيفي للخبراء في المجال التشريعي.

نتائج فروض الدراسة

الفرض الأول : توجد علاقة ارتباطية دالة احصائيا بين حجم تعرض الخبراء فى المجالات الثلاثة وتشكيل اتجاهتهم نحو الشيكات المظلمة.

جدول (٧) العلاقة بين حجم تعرض الخبراء فى المجالات الثلاثة وبين تشكيل الاتجاهات نحو الشبكات المظلمة

العلاقة بين	تشكيل الاتجاهات	
حجم تعرض الخبراء للشبكات المظلمة	قيمة معامل بيرسون	مستوى المعنوية
	.٣١١**	٠,٠٠٠

تشير النتائج إلى وجود علاقة ارتباطية طردية دالة إحصائيا بين حجم تعرض الخبراء في المجالات الثلاثة للشبكات المظلمة وتشكيل اتجاهاتهم نحوها، وذلك بمستوى معنوية ٠,٠١. وتعني هذه العلاقة أن زيادة درجة تعرض الخبراء للشبكات المظلمة في المجالات الثلاثة تزيد من تشكيل اتجاهاتهم نحوها، وهذا يؤكد صحة وثبوت الفرض.

الفرض الثانى: توجد علاقة ارتباطية دالة احصائيًا بين درجة اهتمام الخبراء فى المجالات الثلاثة بالشبكات المظلمة وبين تشكيل اتجاهاتهم نحوها.

جدول (١١) العلاقة بين درجة اهتمام الخبراء فى المجالات الثلاثة بالشبكات المظلمة وبين تشكيل الاتجاهات نحوها

العلاقة بين	تشكيل الاتجاهات	
درجة اهتمام الخبراء بالشبكات المظلمة	قيمة معامل بيرسون	مستوى المعنوية
	.٣٠١**	٠,٠٠٠

تشير النتائج إلى وجود علاقة ارتباطية دالة إحصائيا بين درجة اهتمام الخبراء في المجلات الثلاثة بالشبكات وبين تشكيل اتجاهاتهم نحوها وذلك عند مستوى المعنوية ٠,٠١ وتؤكد هذه العلاقة أن كلما زادت درجة الاهتمام بالشبكات المظلمة، كلما ساعد ذلك في تشكيل الاتجاهات بأنواعها المختلفة نحو هذه الشبكات، وهذا يؤكد صحة وثبوت الفرض السابق.

الفرض الثالث:-

توجد فروق دالة احصائيًا بين تخصصات الخبراء فى المجالات الثلاثة وبين درجة اهتمامهم بالتعرض للشبكات المظلمة.

المتغير التابع	المتغيرات المستقلة	beta	قيمة ت	مستوى المعنوية	معامل التحديد	F
درجة الاهتمام	المجال التقنى	٠,٠٥٧	١,٢	٠,١٤٩	٠,٥٦	٠,٠٠٠
	المجال التشريعى	٠,٠٨٤	٣,٢	٠,٠٢٨		
	الإعلام الرقمى	٠,١٣٣	٣,٥	٠,٠٠١		

يتضح من نتائج الجدول السابق فروق دالة احصائيًا بين درجة اهتمام الخبراء وفقًا لمجال التخصص ، حيث تبين أن خبراء المجال التقنى أقل اهتمامًا

بالشبكات المظلمة ، حيث لم تثبت معنوية العلاقة مع درجة الاهتمام، بينما كانت هناك علاقة معنوية بين الخبراء فى المجاليين التشريعى والإعلام الرقمى بمستوى معنوية بلغ حوالى ٣,٢، ٣,٥ على الترتيب وتشير قيمة معامل التحديد أن ٥٦% من العوامل المؤثرة على درجة الاهتمام بالشبكات المظلمة تتمثل فى متغيرات الدراسة سالفة الذكر ، وتشير قيمة F إلى معنوية النموذج المستخدم ، وتوضح تلك النتائج دخول الشبكات المظلمة دائرة اهتمام الإعلاميين والعاملين فى المجال التشريعى حيث أشارت نتائج التحليل الكيفى إلى إمكانية استفادة الصحفيين خاصة والعاملين فى مجال الإعلامى عامة من مميزات الشبكات المظلمة فى العمل الإعلامى كما أضاف الخبراء فى المجال التقنى بأن تلك النوعية من الشبكات قد تساعد رجال القانون من تتبع القائمين بالعمليات الإرهابية والأنشطة الإجرامية نظرًا لمدى خطورتها بالمقارنة باختراق أجهزة الحاسب للتعرف على مصادر الأخبار غير الرسمية ، وهذا ما أشارت إليه نتائج الجدول رقم (٦) حيث ارتفعت درجة موافقة الخبراء على أن من أبرز الأحداث التى تم تنفيذها من خلال الشبكات المظلمة هى "عمليات غسيل الأموال وتمويل الإرهاب وأنشطة الجريمة المنظمة تتم من خلال النقود المشفرة عبر الشبكات المظلمة الدارك ويب"، وبذلك تم قبول الفرض جزئيًا حيث ثبت معنوية العلاقة بين متغيرين دون المتغير الثالث.

المستوى الثانى: النتائج الكيفية

بعد انتهاء الباحثة من عرض النتائج الاحصائية للدراسة الحالية ، قامت الباحثة بعرض إجابات الخبراء فى المجالات الثلاثة عينة الدراسة من خلال الاجابة على الأسئلة المفتوحة للدراسة ، والتى تتمثل فى السؤال الرابع والخامس والسادس، وتضمنت الاجابات مجموعة من البيانات والتحليلات قامت الباحثة بربطها بالنتائج التى توصلت إليها الدراسات السابقة.

النتائج الكيفية للدراسة:-

عرض النتائج الكيفية للدراسة الحالية من خلال المحاور الثلاثة الرئيسة:-

أولاً:- الأثار المستقبلية التى يراها الخبراء فى الاتجاهات الثلاثة لاستخدام الشبكات المظلمة على الفرد والمجتمع.

اتفق الخبراء على خطورة الأثار المسقبلية للشبكات المظلمة سواء من الناحية الإعلامية أو التقنية أو القانونية ويرجع ذلك لعدة أساب أشار إليها الخبراء بمختلف المجالات:-

فيما يتعلق بالمجال التقني ، أكد الخبراء فى المجال التقني أن من أهم الأثار المستقبلية للشبكات المظلمة هو انتشار الجرائم الإلكترونية أو ما أسماه البعض " بالجرائم المظلمة " وظهور أنماط جديدة منها فى المستقبل القريب ، وحذر الخبراء أيضاً أنه قد يكون هناك صعوبة للوصول إلى قوائم بالجرائم الإلكترونية قبل أن يتم تنفيذها على أرض الواقع ، حيث يتطلب الأمر جهود دولية للوصول لتطبيقات يمكن من خلالها رصد وتتبع مستخدمى شبكات الدارك فى جميع الانشطة غير قانونية، واتفق الخبراء أن ظاهرة الجرائم الإلكترونية ، ظاهرة عالمية وليست

محلية مما تستوجب تعاون دولى ، فقد أشار **عمرو صبحى** أن " التنظيمات الإجرامية والإرهابية تسعى إلى الاستفادة من مزايا استخدام شبكة الإنترنت المظلمة، وبصفة خاصة طابعها السرى وصعوبة تعقب مستخدميها، بما يحقق لها مباشرة أنشطتها الإجرامية بعيداً عن أية رقابة أو مسائلة قانونية، حيث يوجد على هذه الشبكة مواقع الوثائق المزورة والمسروقة وبيانات البطاقات الائتمانية والحسابات الشخصية، بالشكل الذى أصبحت به هذه الشبكة سوقاً سوداء لكافة الأنشطة غير المشروعة، ومرتعاً للمجرمين والقراصنة والقتلة المأجورين والمزورين وتجار البشر إلى غير ذلك، بحيث يمكن أن يقوم أى مستخدم على الشبكة بالتواصل معهم للحصول على هذه الخدمات فى سرية تامة من دون أن يتعرض لأية رقابة رسمية ، وتأثيرها علي الفرد والمجتمع تأثير ضار جداً". (١)

وتوقع، **عادل أبو المجد** زيادة الأثار السلبية المستقبلية لتلك الشبكات ، نتيجة لأن مواقع الانترنت المظلم تتميز باستخدام أسماء لها غير تقليدية ويصعب تتبع الاشخاص الحقيقيين. (٢)

ونوه بعض الخبراء إلى خطورة الأثار المستقبلية لارتباطها بظهور أنماط جديدة من الجرائم الإلكترونية لتلك الشبكات ، فقد أشار **مصطفى عمران أن** "خطورة ا الشبكات المظلمة تكمن فى أنها سوف تفرز انواعاً جديدة من الجرائم الإلكترونية ، مثل زيادة الانضمام للمجموعات التى تصور الجرائم بالصوت والصورة (٣) ، وأكد على ما سبق **عربى السيد كشك** قائلاً " أن هناك تعدد فى الأثار المستقبلية السلبية لتلك الشبكات،لا سيما فى مجال تجارة المخدرات والسلاح خاصة أن تلك الشبكات يصعب تتبع مستخدميها ولا يستطيع المستخدم حماية نفسه إلا من كان محترف فى مجال الإنترنت بعكس المستخدم العادة مما يؤكد على خطورة آثارها فى المستقبل" . (٤) بينما وحذر **أحمد إدريس** من " خطورة مواقع القتلة عبر تلك الشبكات والتى تهدد الأمن المجتمعى نتيجة لخطورة أثارها على الفرد، فقد رصد موقع يسمى «تأجير القتلة»، وهو أحد المواقع الموجودة على الإنترنت المظلم الخاصة بالإجرام، ويوجد فيه أشخاص مجرمون متخصصون فى القتل مقابل أجور معينة، وكل ما على الشخص هو تحديد الدولة التى يعيش فيها الشخص الذى يريد قتله" (٥) ، فى حين تناول البعض **الأثار المستقبلية النفسية** التى تتركها الشبكات المظلمة فقد أشار **توفيق اسماعيل** أن" تلك الشبكات سوف تترك العديد من الآثار النفسية السلبية لا سيما تعزيز السلوك العدوانى والانغماس فى أعمال الهاكرز والسرقات المالية". (٦) ، فى حين توقع **طارق عباس** "استمرار الهجمات الإلكترونية وأعمال القرصنة بالإضافة إلى ابتكار طرق جديدة لحماية خصوصية المستخدمين وتشجيعهم على الانضمام لتلك الشبكة". (٧)

وقد أكد على هذا التوقع **وليد حجاج** قائلاً " إن لم تتطور الأليات التى تحدد هوية مستخدميها سوف تكون هى الأكثر استخداما وستهدد أمن الدول ومعتقداتها الدينية والملكية الفكرية (٨) ، ونوه **أحمد على** " أن الأثار المستقبلية لا تتوقف فقط على الإنضمام لتلك الشبكات وإنما الدخول إلى هذه المواقع قد يتسبب في تلف أجهزة المستخدم وأضاف أنه من الممكن أن تمرير بعض الروابط إلى المستخدمين والتى تستهدف التجسس على البيانات الشخصية (٩)، وتوقع د. **أحمد بهاء الدين** " زيادة نسبة الجرائم بكافة أشكالها فى المجتمعات المتأخرة تكنولوجياً مما يمثل خطر على أمان وأستقرار المجتمع وتوقع ارتفاع الجرائم الفردية ، حيث يعد الويب

المظلم مكان للجريمة والمجرمين، وعند الدخول عليه يجب الوضع فى الاعتبار أنك سوف تتعامل مع مجرمين، وأن كل المقومات التى تساعد على انتشار الجريمة متوافرة داخل الإنترنت المظلم مما يؤدى إلى زيادة الأثار السلبية فى المستقبل لتلك النوعية من الشبكات". (١٠)

وفيما يتعلق بالمجال التشريعى، أشار فريق من الخبراء أن خطورة الأثار المستقبلية للشبكات المظلمة تتمثل فى صعوبة الوصول إلى نص قانوني يعاقب كل من يدخل على تلك الشبكة نظرًا للتطور السريع فى المجال التكنولوجى والذى أشار إليه فيما سبق خبراء المجال التقنى ، مما يساعد أسواق الويب المظلمة بربط المشترين والبائعين للسلع والمواد شبه القانونية أو غير القانونية، أو بيعها بأنفسهم مباشرة ، وأكد معظم الخبراءأن الجرائم التى تتم عبر الشبكات المظلمة سوف تزداد فى المستقبل ، مما يؤدى إلى ارتفاع عدد ضحايا تلك الشبكات حال عدم التوصل لقانون يعاقب المستخدمبن لتلك الشبكات فى الأعمال الإجرامية (١١) ، ويرى **محمد حجازى** " أن الأثار المستقبلية تختلف طبقاً لأعداد المستخدمين، والخطورة فى انضمام الشباب بهدف الكسب السريع عن طريق السرقات الإلكترونية".(١٢)، ومن وجهة نظر **أحمد سعيد** أن "الأثار المستقبلية تتحدد فى " انتشار الأعمال غير القانونية لا سيما فئة الشباب والمراهقين الذين ينساقوا وراءها، ووصفها بأنها تعد باب من أبواب جهنم" (١٣)، وأضاف **محمود الرشيدى** " أن خطورة الأثار المستقبلية تتمثل فى الخطر الخارجى الذى يهدد أمن الدول لا سيما الأعمال الإرهابية كما حدث فى فرنسا". (١٤) ، ويرى **أحمد السخاوى** أن " الأثار المستقبلية سيئة للغاية ومدى معرفه الناس ب الدارك ويب أصبح كبير

و متنامي و متزايد مما يشكل خطراً يهدد المستخدمين مِن يحاولون الدخول بدون احتياطات الأمان، بالاضافه أن العلم يجب أن يتطور ويكون هناك آليات أكثر ذكاء في تتبع المجرمين. (١٥) ، على الجانب الأخر يرى فريق من خبراء الأمن السيبرانى أن الأثار المستقبلية للشبكات المظلمة سوف تقل فى المستقبل فبالرغم من أن عالم الإنترنت المظلم يعد مستنقع ومرتع خصب لممارسة جميع أنواع الجريمة، ويعمل فيه التنظيمات الإرهابية، وأجهزة المخابرات العالمية، موضحاً أن الدخول عليه ليس سهلاً للمواطنين العاديين، ولكن يتم من خلال أكواد وشفرات معينة ، ويتم التعامل فيه بعملة البيتكوين، إلا أن نسبة المستخدمين لتلك الشفرات قليلة جداً فى مصر مما يقلل من فرص خطورة أثارها المستقبلية" . (١٦).

وحذر الخبراء فى مجال الأمن السيبرانى من خطورة الأنشطة الإجرامية، التي تتم عبر الشبكة المظلمةDark Web فى المستقبل ، وأكدوا على ضرورة تعاون حكومات العالم، للحّد من تلك الأنشطة فى المستقبل، وأن مصر مثل الكثير من دول المنطقة، تشهد نمواً في الهجمات السيبرانية الخبيثة، فقد شهدت مصر حوالي ٤٢ مليون هجمة بالبرمجيات الخبيثة فى بداية عام ٢٠٢١، بزيادة قدرها ٣٢% على أساس سنوي، وفقا لشركة الأمن السيبراني " كاسبرسكاي" ، كما شهدت منطقة الشرق الأوسط وشمال أفريقيا ككل حوالي ١٦١ مليون هجمة بزيادة قدرها ١٧% على أساس سنوي" (١٧).

ومن الناحية الإعلامية ، اتفق الخبراء فى مجال الإعلام الرقمي على أن الأثار المستقبلية للشبكات المظلمة لا سيما المجتمعات العربية تتجسد فى التأثير على الأفراد غير المدركين

لاستخدام هذه الميزة واستخدامها في أعمال غير أخلاقية أو غير قانونية وهو أمر مرفوض ولكنه للأسف الشديد ينتشر مع تزايد أعداد مستخدمي شبكة الإنترنت ونتيجة الجهل وضعف الوازع الديني والأخلاقي بالإضافة لغياب القوانين التي تجرم هذا الفعل في كثير من الدول وعدم القدرة على التحكم في الشبكة (١٨)، وعلى المستوى المجتمعي فالموضوع مرتبط بسلوك الأفراد ودرجة وعيهم مالم تتواجد توعية حقيقية وقوانين حاكمة وضابطة وهذا سيؤدي لتفشي الجرائم الإلكترونية والأعمال غير المشروعة والفساد في المجتمع (١٩).

واتفق الخبراء فى المجالات الثلاثة على أن السرعة التى تحدث فى مجال تكنولوجيا المعلومات تمثل عائق أمام تنفيذ القوانين لمعاقبة مجرمي الشبكات المظلمة، فى حين أكد خبراء الإعلام الرقمي على قصور وسائل الإعلام الرقمية فى تقديم توعية لمستخدمي شبكات الدارك ويب وأن هناك مخاوف من مجرد طرح الموضوع للنقاش عبر وسائل الإعلام الرقمية على الرغم من التطرق إليه ولكن بنسب ضئيلة فى القنوات التليفزيونة لا تتساوى مع حجم وخطورة شبكات الدارك على الفرد والمجتمع.

ثانيًا: ـ الاستخدامات المستقبلية للدارك ويب كما يراها الخبراء فى المجالات الثلاثة.

أولًا : المجال التقني : اتفق غالبية الخبراء فى المجال التقني أن الإستخدامات المستقبلية السلبية للدارك ويب سوف تتزايد نتيجة ارتفاع عدد مستخدمي الشبكات المظلمة فى المستقبل القريب، نظراً للمميزات التى تتمتع بها وعلى رأسها اخفاء هوية المستخدم، فقد أكد كل من **أحمد إدريس، عربى السيد، أحمد بهاء** " أن خطورة الاستخدامات المستقبلية تتضح بقوة من خلال مواقع متخصصة فى السحق الإباحى، وهى مجموعة من المواقع الإباحية والجنسية، التى تهدف إلى إجراء تجارب جنسية مع الحيوانات والبشر أيضاً، إلى جانب مواقع المصيدة التى يتم من خلالها إختراق أجهزة الأفراد والتجسس عليهم والحصول على المعلومات الخاصة بهم وابتزازهم س، كما حذر من مواقع تسمى " آكلى لحوم البشر" ، وهى المواقع التى تتخصص فى بيع لحوم البشر أو الأعضاء البشرية مقابل الأموال (٢٠) ، **فى حين ركز بعض الخبراء على ارتفاع الاستخدامات الاقتصادية للشبكات المظلمة والمتمثلة فى** "انتشار القرصنة والعملات الرقمية بشكل أكبر والتى تعد من أكثر الأستخدامات المرتقبة للشبكات المظلمة، وزيادة جرائم الاحتيال وسرقة البيانات البنكية لا سيما فى ظل الظروف الاقتصادية على الرغم من وجود برامج لحماية الحسابات البنكية، لكن مع الاسف تفتح شبكات الويب الظلم الباب للاستخدامات غير الشرعية التى تساعد على تكوين سوق إلكترونية غير مراقبة من قبل أجهزة الدولة الأمنية" (٢١) ، وأضاف كل **من طارق عباس و مصطفى أو جمرة وأحمد إدريس** " أن غياب الوعي والثقافة الأمنية يزيد من مخاطر مستخدمى الويب الأسود، مما يؤدى إلى ارتفاع مستخدمى تلك الشبكات وزيادة الانشطة غير القانونية نتيجة النمو بشكل متسارع مع تطور تقنيات الاتصالات من الجيل الخامس وانتشارها" (٢٢)، وأكد على الأراء السابقة كل من **مصطفى عمران ، أحمد على، عمرو صبحى** ، فتوقع كل منهما " إرتفاع الإستخدام المستقبلى للشبكات المظلمة لأن هذه الشبكات في حالة نمو سريع جداً ويزيد من خطورته لا سيما فيما يتعلق بوجود مهندسين يقوموا بإعطاء دروس حول كيفية ارتكاب الاحتيال أو اختراق الأنظمة، والخدمات غير المشروعة من إنشاء برامج ضارة مخصصة إلى نشر الهجمات الإلكترونية، وصولا

إلى الأسلحة، وعادة ما يتم الدفع مقابل السلع والخدمات في أسواق الويب المظلمة باستخدام عملات مشفرة مجهولة مثل" البيتكوين" فى المستقبل المخترق [٢٣].

وعلى النقيض من الأراء السابقة يرى **توفيق اسماعيل** أن **"**الاستخدامات المستقبلية للشبكات المظلمة **لا تمثل خطورة فى المستقبل** على مستوى مصر حيث أن عدد مستخدمى الشبكة المظلمة فى مصر قليل جداً ، والانضمام إليها يحتاج إلى سرعات كبيرة، فحجم الدارك ويب يمثل ما يقرب من ٩٦ الي ٩٧ ٪ من حجم الانترنت الكامل و ما يستخدمه المصرين يمثل من ٣ الي ٤ ٪ فقط " [٢٤].

ثانيًا:- المجال التشريعيى

اتفق غالبية خبراء العينة فى المجال التشريعى أن هناك ارتفاع فى انتشار **التجارة الإلكترونية المظلمة، وهي صناعة متنامية وتغذي طفرة الجرائم الإلكترونية ، فتوقع كل من عادل العمدة ، محمود الرشيدى "** انتشار الاستخدامات غير القانونية الحالية، ومن أبرزها ، الاتجار بالمخدرات، والأسلحة، وترويج البرمجيات الخبيثة كبرامج الفيروسات، وتجارة الأعضاء البشرية، وأدوات الجرائم الإلكترونية، والاستغلال الجنسي للأطفال، لا سيما أن تلك الشبكة تستهدف فئة اللاجئين والمشردين ممن هم أقل من ١٨ سنه والاتجار بهم [٢٥]، وأكد على الرأى السابق **هشام صبرى ، محمود حجازى وقالوا** " أن الاستخدامات المستقبلية سوف تشهد ارتفاع فى شراء العقاقير غير المشروعة والأسلحة والسلع المقَلّدة وبطاقات الإئتمان المسروقة والبيانات المخترقة، أو العملات الرقمية، أو البرامجيات الضارة وبطاقات الهوية الوطنية او جوازات السفر [٢٦].

وأضاف فريق أخر من الخبراء أن هناك تنوع فى الاستخدامات المستقبلية الأخرى غير المشروعة ، والتي يصعب حصرها، على سبيل المثال هناك مواقع متخصصة في إجراء التجارب الطبية على البشر، مثل موقع **The Human Experiment** الذي يتخصص في استغلال المشردين في إجراء التجارب الطبية عليهم، وهناك أيضًا موقع الموسوعة الخفية من أشهرها موقع" The hidden wiki" " المتخصص في تقديم إرشادات وتعليمات وخدمات متعلقة بغسيل الأموال، واتفاقات القتل، والهجمات الإلكترونية، والمواد الكيميائية المحظورة، بالإضافة إلى تعليمات صناعة القنابل والمواد المتفجرة، وتجارة الأوراق الرسمية المزورة، مثل: جوازات السفر، ورخص القيادة، وأوراق المواطنة، وشهادات الجامعات، وأوراق الهجرة، والهويات الدبلوماسية، بالاضافة إلى خدمات التجسس والاستهداف لأي شخص " [٢٧].

ثالثًا من الناحية الإعلامية:

انقسم الخبراء فى المجال الإعلامى إلى فريقين الأول يرى أن " خطورة استخدام الدارك ويب تتركز فى أنه يتم تصوير تلك الجرائم وبثها على مواقع الإنترنت العادية وفى الكثير من الأحيان يتم استخدام خاصية البث المباشر عبر موقع الفيس بوك وقت حدوثها" [٢٨].

بينما يرى الفريق الأخر" أن تلك الشبكات تساعد الإعلامين فى الحصول على المعلومات على سبيل المثال أنه غالبًا ما يستخدم الصحفيون متصفح Tor للتواصل مع المخبرين

للحصول على المعلومات لضمان سلامتهم من حكوماتهم. (٢٩) ، وأكد كل من **رضوى عبد اللطيف ، خالد البرماوى ، أحمد عصمت** على " أهمية التوظيف الايجابى لتقنيات الدارك الويب فى مجال العمل الصحفى تحديدًا، فمن المهم والضروري أن يتابع الصحفي كل ما يدور حوله وهذا يجعله مطلعاً على كل ما يحدث ولا يكتفي بالدوائر المغلقة التي توفرها منصات التواصل والانترنت ، وبالرغم من ذلك إلا أن يظل اطلاع الصحفيين العرب على الدارك ويب محدوداً ولكن إذا امتلكوا أدوات التحقق من المحتوى والتعامل بما يفيد رسالتهم في كشف الفساد والجريمة فبالتأكيد استخدامهم للدارك ويب سيفيد في تتبع وإسقاط الفاسدين من أجل مجتمع أفضل وهذا سيعطي للمواد الصحفية المقدمة قيمة أعلى وستكون أكثر عمقا وتأثيراً (٣٠) .

ونوه د.**مصطفى أبو جمرة** " أنه من المتوقع استخدام الشبكات المظلمة فى اختراق حسابات **منصة نتفلكس ، وشاهد** ، بالاضافة إلى شراء أسماء المشاهير عبر اليوتيوب وقنواتهم وكلمات مرورهم" (٣١) ، وذكر خبراء أخرون أن من المتوقع استخدامها فى التقليل من قيمة المؤسسات الإعلانية: من خلال تقويض الثقة في علامة تجارية بعينها، أو تضر بسمعة شركة أو خدمة منافسة، أو تسمح بتحقيق شركة منافسة لمكاسب على حساب شركة أخرى، ونوه الخبراء إلى أن شبكات الدارك تستخدم فى نقل مواد إعلامية لا يرغب المشاهد فى رؤيتها مثل المواد الإباحية وذلك من خلال ما يسمى (بالروابط المشبوهة) فإذا نقر المستخدم على أي روابط يتم نقله مباشرة إلى مادة لا يرغب في رؤيتها، والخطورة فى فئة الأطفال والمراهقين مما يترك أثارًا سلبية نتيجة ما يشاهدونه من مواد غير أخلاقية ".

ثالثًا:- الأساليب التى من الممكن اتباعها على المستوى الإعلامي والتشريعى والتقني لمواجهة مخاطر الدارك الويب من وجهة نظر الخبراء.

أولًا: فيما يتعلق بالمجال التقني : خلصت نتائج التحليل الكيفي إلى تباين أراء الخبراء فيما يتعلق بأساليب مواجهة مخاطر الدارك ويب ما بين اللجوء إلى الوسائل التقنية والتوعية الرقمية والغلق الكامل لتلك الشبكات وتفعيل الجانب القانونى، فى حين رأى الفريق الأخر صعوبة مواجهة مخاطر الدراك ويب وملاحقة التطور السريع والمتزايد لها يوماً بعد يوم ، فقد نصح كل من **أحمد على ، عادل أبو المجد** ، " بضرورة الوصول إلى برامج تكنولوجيه تسمح بتتبع المستخدمين غير القانونين للشبكات المظلمة خاصة لمن يملكون قدر محدود من التعامل التكنولوجى وذلك بإمكانية التعاقد مع الخدمات الرقمية أو الجنائية، بدءاً من حملات البريد المزعج (spam) إلى هجمات التعطيل المنتشر للخدمة (DDoS) ويمكن للمبتدئين حتى شراء الكتب الإلكترونية التي تشرح كيفية مهاجمة المواقع، وسرقة الهويات ، وأكدوا على " ضرورة تفعيل جميع الوسائل التقنية ممثلة فى التطبيقات الحاسوبية لحماية أمن المعلومات من اختراقها من قبل الهاكرز عبر الشبكات المظلمة للحماية من جرائم الاحتيال وسرقة الأموال والبطاقات الائتمانية ، لا سيما البنوك وشركات الصرافة من خلال استخدام أحدث برامج الحماية لأجهزة الكمبيوتر، وإبلاغ السلطات الأمنية الرسمية ممثلة فى إدارة مكافحة الجرائم الإلكترونية، في حالات سرقة البيانات الشخصية أو الهويات أو المعلومات ويعد هذا هو الحل الأمثل للوقايه من مخاطر الإختراق" (٣٢) ، وأضاف كل من **وليد حجاج ، أحمد بهاء "** أن التوعية هى الأسلوب الأمثل لمواجهة مخاطر شبكات الدارك ، يتمثل فى استحداث أليات أكثر تطورا عن

المستخدمة حالياً لتحديد هوية المستخدم، وزيادة الإنفاق فى مجال الأمن المعلوماتى، حيث عملية التتبع التقنى لإيقاف شبكة الدارك تتطلب أموالاً طائلة ، وموارد ضخمة (٣٣) ، وتوصل كل من **طارق عباس، مصطفى عمران** " أنه يمكن تتبع مجرمى الشبكات المظلمة والوصول إليهم من خلال تحديد عناوينهم على الإنترنت(IP Address) ، ومن ثم التعرّف على هوياتهم الحقيقية وإلقاء القبض عليهم ، كما أقترح البعض أنه يمكن أيضاً من خلال الأجهزة الأمنية في الدول المختلفة مراقبة الإنترنت المظلم، وسرعة القبض على الشبكات التى تقوم بأنشطة إجرامية ، فيما اعترض البعض الأخر على هذا الأسلوب(٣٤)، فقد رأى كل من **عمرو صبحى ، وليد حجاج** " أن هذا الأسلوب يعد حل مؤقت فقط مع الجرائم الفردية أما الجرائم التى تتم من قبل الجماعات الإرهابية أو مافيا شبكات الدارك فالخطورة تكمن فى صعوبة الكشف عن مرتكبى الجرائم أو العائدات التى يحصل عليها مرتكبيها نظرًا لأن الجانب التقنى الذى تتميز به شبكات الدارك ويشجع المستخدمين من الإنخراط فى الأنشطة الإجرامية هو صعوبة الكشف عن هوية المستخدم. حيث أن مستخدمي الشبكة لديهم تطبيقات تُخفي هوياتهم وتُبقيهم مجهولين" (٣٥) وهذا ما أكدته نتائج الدراسات السابقة.

وعلى الجانب الأخر رأى البعض صعوبة الوصول إلى أساليب محددة يمكن توظيفها لمواجهة مخاطر الدارك ويب فقد أشار كل من **عربى السيد، أحمد إدريس** " أن هذا العالم الخفى يستحيل اختراقه تكنولوجياً مما يصعب تعقبهم من قبل الشرطة والسلطات، كما يصعب وجود برامج تقنيه لمواجهة مخاطر الويب المظلم ولكن يمكن التوعية إعلامياً والتنبية على المستخدمين بتطبيق القوانين على الخارج عن القانون وأنه سيعرض نفسه للمسألة القانونية" (٣٦) .

وخلصت إجابات جميع الخبراء بالاتفاق على أن هناك " فجوة رقمية " بين الدول فى تتبع الجرائم الإلكترونية التى تتم بواسطة الشبكات المظلمة. فإذا ظهر موقع إرهابي اليوم ، فسرعان ما يغير نمطه الإلكتروني، ثم يختفي ليظهر مرة أخرى بشكل وعنوان إلكتروني جديدين بعد فترة قصيرة، وأكدوا أن من **الصعب في ظل التكنولوجيا الحديثة وضع آلية مراقبة دقيقة لمتصفحي الإنترنت المظلم، وأنه** يجب وضع خطة من قبل وزارة الاتصالات لحجب المواقع الإلكترونية والأنظمة التي تعرض المستخدمين لمخاطر عديدة يصعب القضاء عليها بعد حدوثها.

على المستوى التشريعى:-

تباينت الأراء فيما يتعلق بالأساليب القانونية التى من الممكن استخدامها للحد من الجرائم السيبرانية عبر شبكات الدارك وتتبع منفذيها ، فالبعض رأى صعوبة فى الوصول إلى نص قانونى للحد من انتشار تلك الجرائم لأنها تتم على المستوى الدولى بصورة أكبر، والبعض الأخر أشار إلى جهود العديد من الدول فى تطبيق القوانين على مستخدمي الشبكات المظلمة ونجاح شرطة مكافحة جرائم الإنترنت على أرض الواقع فى القبض وملاحقة شبكات الإتجار بالبشر عبر الشبكات المظلمة، وأنه تم فى بعض الدول تعديل بعض أحكام قانون جرائم الإنترنت مثل جرائم الاحتيال المالى للتمكن من التصدى لتلك الجرائم من المستوى المحلى.

كما أكد **هشام صبرى ، عادل عبد المنعم** على " ضرورة إصدار مجموعة من القوانين للتقليل من الجرائم الإلكترونية خاصة القوانين والتشريعات الداعمة لمواجهة أية تهديدات لمجال الأمن السيبرانى". (٣٧)، وأضاف **أحمد سعيد** قائلاً " أنه بجانب تلك القوانين يجب **القيام بالتوعية القانونية** عبر وسائل الإعلام الرقمي والتقليدي بالعقوبات القانونية التى تقع على المستخدمين لتل الشبكات بشكل غير شرعى بمخاطرها وتعليم المستخدمين كيفية حماية أنفسهم من الإنسياق وراء استخدام شبكات الدارك". (٣٨)، يرى **اللواء محمود الرشيدي** أن أساليب المواجهة تكمن فى " أن بعض المؤسسات يجب عليها أن تقوم بجهود كبيرة لمكافحة هذه النوعية من المواقع عن طريق التتبع والمراقبة، من خلال مباحث الإنترنت، بالتعاون مع وزارة الاتصالات وأجهزتها الفنية، والمجلس القومي للأمن السيبراني، وذلك لحماية الفضاء الإلكتروني المصري من أي هجوم إلكتروني خارجي، مشيراً إلي أن الهجمات الإلكترونية متبادلة بين دول العالم ولن تتوقف، ولكن نعمل على كبح جماحها، والتقليل منها" (٣٩) .

وأضاف **اللواء يحيى كدوانى** قائلًا " أن الجرائم التي تمارس على «الويب المظلم» من جانب عصابات المافيا تحتاج في مكافحتها ومجابهتها إلي تعاون دولي، ونظرة جديدة، لأنها جرائم عابرة للحدود، ولأن المنظم والمسيطر علي هذه المنظومة يوجد خارج الدولة، وما أكثر القوانين التي تجرّم وتكافح الجرائم السيبرانية، كما طالب بضرورة تشديد الرقابة المستمرة والفاعلة، وتكاتف الجهود وتضافرها لحفظ الأمن والاستقرار(٤٠). **فيما أسند البعض أن العقبة تتمثل فى التطور التكنولوجى السريع** حيث رأى الكثير من الخبراء " صعوبة إيجاد قانون للحد من الجرائم السيبرانية والقبض على مرتكبيها فقد أشار الخبرا إلى إزدياد الفجوة بين التطور التكنولوجي المتلاحق والشروع فى قوانين للحد من انتشار الشبكات مما يزيد من صعوبة ملاحقة مرتكبة الأعمال غير القانونية. (٤١) ، وأكد كل **من أحمد السخاوى، عادل العمدة** على " ضرورة التوصل الى اتفاقية دولية بها نصوص قانونية للتصدى لظاهرة الجرائم الإلكترونية لا سيما العمليات الإرهابية لأنها تستهدف الدول كافة وليس دولة بعينها، مما يساعد على السرعة فى تطبيق القانون على منفذيها والدليل أن العلمليات الارهابية التى وقعت فى باريس، حيث أشارت التحقيقات إلى أن السرعة والتعقيد التى تتم بها الجرائم السيبرانية عبر الشبكات المظلمة تمثل عائق وتحدى أمام ملاحقة مرتكبيها، واتخاذ الإجراءات القانونية قبل البدء فى تنفيذها" كما أشاروا إلى " ضرورة أن يكون هناك أساليب جديدة للتحقيق فى الجرائم الإلكترونية تتناسب مع الطبيعة التقنية التى تتم بها تلك الجرائم وعلى رأسها اتباع مرتكبيها وسائل وتطبيقات لحماية أنفسهم من الكشف عن هويتهم" (٤٢). ونوه كل من **محمد عبد المقصود ، بهاء الدين حسن** " أن مجرمو الإنترنت يتقدمون على السلطات الأمنية، حيث تتسم شبكات الدارك بثغرات أمنية تسمى بثغرات **ساعة الصفر** والتي لا يوجد لها حلول قانونية حازمة لها حتى الآن (٤٣).

ثالثًا من الناحية الإعلامية:-

إتفقت أراء الخبراء فى مجال الإعلام الرقمى مع أراء الخبراء فى المجال التقني فقد أكدوا على ضورة التوعية الرقمية لمستخدمي شبكات الدارك ، وضرورة كشف مخاطر هذا العالم الخفي عبر الحملات الإعلامية التوعوية فى مختلف وسائل الإعلام الرقمية والتقليدية، وفى

نفس السياق أكد البعض الأخر من خبراء الإعلام الرقمي على " أن التوعية الإعلامية بخطورة الشبكات المظلمة يجب أن تبدأ من المدارس والجامعات لأن لا يوجد فئة عمرية محددة لمستخدمى الويب العميق والويب المظلم والويب السطحي بل هو عالم يستخدمه مختلف الأعمار لا سيما أن هناك ضحايا من **الأطفال والمراهقين** (٤٤)، وأشار كل من **مصطفى أبو جمرة ،علاء الغطريفى "** أن الدور الإعلامى يتمثل فى ضرورة التوعية المستمرة، بعدم استخدام أي موقع مجهول المصدر أو الهوية ، وعدم استخدام أى تقنيات جديدة لأنها تستهدف ابتزاز الأطفال والشباب والفتيات للإنخراط فى الأنشطة الإجرامية كما يجب ان يكون هناك توعية رقمية وقانونية فى الوقت ذاته" (٤٥).

ونصح كل من **أحمد عصمت، أسامه الديب ، خالد البرماوى "** يجب على المستخدمين لا سيما الصحفيين توخي الحذر عند استخدام الإنترنت المظلم، وأن يقوم بإخفاء المعلومات بطرق ذكية، وقد اقترح مؤلف كتاب «Deep Web for Journalists» (آلان بيرس) أنه يمكن إخفاء المحادثات داخل الملفات الرقمية المرتبطة بالصور الفوتوغرافية، ويستطيع الصحفي أيضًا إخفاء اللقطات المصورة داخل تسجيل مقطع موسيقي على جهاز الايبود أو الهاتف الذكي، إضافة إلى ذلك، فإنه من المفيد للصحفي أن يستخدم كلمة سر معقدة ويصعب اكتشافها لكي يحمي المعلومات والملفات السرية التي توجد لديه من خطر الوقوع في قبضة الشخص الخطأ" (٤٦)، وأضافت **رضوى عبد اللطيف** أن من أهم أساليب المواجهة " التدريب على كيفية الاستخدام الأمن للدارك ويب ويشمل ذلك تدريبات على الأمن الرقمي والتحقق من المحتوى ومعرفة الجرائم الإلكترونية وأساليب تجنيد الجماعات الإرهابية وغيرها من الموضوعات التي تدخل في دائرة اهتمام أي مستخدم

لا سيما الصحفيين من أجل تقديم محتوى هادف يكشف الفساد ويساهم في توعية الجمهور" (٤٧) ، **وذكر فريق أخر من الخبراء "** أن مصر تفتقر أساليب مواجهة مخاطر شبكات الدارك فحملات التوعية المتمثلة فى الإعلانت التليفزيونية والرقمية وإصدار منشورات وصفحات للتوعية الرقمية مع الأسف لا توجد فى مصر بشكل كبير**"** (٤٨).

مناقشة نتائج الدراسة والتوصيات:

أولًا : مناقشة أبرز النتائج التى توصلت إليها الدراسة

خلصت النتائج الكمية للدراسة

- خلصت النتائج الكمية للدراسة إلى ارتفاع تعرض الخبراء فى المجالات الثلاثة للشبكات المظلمة وقد تركز وقت التعرض لها (عند الحاجة للبحث عن موضوع محدد فى مجال التخصص) وجاء التعرض نشط والذى ظهر من خلال أنماط التعرض للشبكات المظلمة وذلك من خلال وأكدت تلك النتيجة ارتفاع درجة اهتمام الخبراء بالدخول الى الشبكات المظلمة والتى ظهرت بدرجة كبيرة بنسبة ٤٠%، وتمثل تعرض الخبراء للشبكات المظلمة بشكل نشط والذى ظهر بنسبة كبيرة من خلال الانضمام للمجموعات المستخدمة للشبكة للبحث فى موضوع التخصص) والذى يمثل درجة عالية من درجات التعرض النشط وذلك بنسبة ٤٣,٣%.

- كشفت نتائج اختبارات فروض الدراسة عن وجود علاقة ارتباطية دالة احصائيًا بين حجم تعرض ودرجة الخبراء فى المجالات الثلاثة بالشبكات المظلمة وبين تشكيل الاتجاهات نحوها ، كما أشارت نتائج الفرض الثالث بوجود فروق دالة احصائيًا بين تخصصات الخبراء فى المجالات الثلاثة وبين درجة اهتمامهم بالتعرض للشبكات المظلمة وجاءت الفروق لصالح الخبراء فى المجال التشريعى والإعلام الرقمى من حيث ارتفاع درجة اهتمامهم بالتعرض للشبكات المظلمة.

- وفقًا للنتائج التي تم جمعها من خلال المقابلات المتعمقة التي أجرتها الباحثة مع الخبراء في المجالات الثلاثة (التقني والتشريعي والإعلامي)، فإن هناك استجابة إيجابية لدى الخبراء تجاه الشبكات المظلمة وتأثيرها على مجالاتهم، وقد لوحظ أن الخبراء الذين يعملون في مجال التشريع والإعلام الرقمى أكثر اهتمامًا بالشبكات المظلمة من الخبراء الذين يعملون في المجال التقنى ، وهذا يشير إلى أن الشبكات المظلمة تصبح أكثر أهمية في الأوساط الإعلامية والتشريعية ، بينما اختلف القليل منهم لا سيما خبراء المجال التشريعى فى الأساليب التى يمكن من خلالها مواجهة أخطار الدارك ويب والمجال التقنى فى الأثار المستقبلية للشبكات المظلمة على مصر، وفيما يلي عرض لأهم النتائج التي اتفق واختلف عليها خبراء التكنولوجيا والتشريع والإعلام الرقمي:

- **فيما يتعلق بالأثار المستقبلية للشبكات المظلمة** اتفق الخبراء في المجالات الثلاثة عينة الدراسة على أن من أهم الأثار المستقبلية للشبكات المظلمة هو انتشار الجرائم الإلكترونية أو ما يسمى بـ "الجرائم المظلمة"، وظهور أنماط جديدة منها في المستقبل القريب، وحذر الخبراء أيضًا من صعوبة الوصول إلى قوائم بالجرائم الإلكترونية قبل أن يتم تنفيذها على أرض الواقع، مما يتطلب جهود دولية لرصد وتتبع مستخدمي شبكات الدارك في جميع الأنشطة غير القانونية. واتفق الخبراء على أن ظاهرة الجرائم الإلكترونية هي ظاهرة عالمية وليست محلية، وتستوجب تعاون دولي لإصدار وتفعيل قوانين صارمة لمستخدمي شبكات الدارك في الاستخدام غير المشروع.

- أشارت نتائج الدراسة إلى تخوف الخبراء في ظل غياب التوعية الإعلامية والتطورات التكنولوجية المتسارعة وعدم إصدار قوانين صارمة في مصر للقبض على مرتكبي جرائم شبكات الدارك. ويتطلب ذلك تعاونا دولياً قوياً وتوعية إعلامية شاملة لرفع الوعي بأهمية الأمن السيبراني والحد من الجرائم الإلكترونية في جميع أنحاء العالم، ويجب على الحكومات والمؤسسات التعاون في تطوير تقنيات جديدة لمكافحة الجرائم الإلكترونية وتعزيز القدرة القانونية للسلطات القضائية للتعامل مع هذه الجرائم،وتؤكد الدراسة على أهمية تبني سياسات وإجراءات صارمة للتحقق من هوية المستخدمين والحد من الاستخدام غير القانوني للشبكات المظلمة

- **فيما يتعلق بالإستخدامات المستقبلية اتفق غالبية الخبراء فى المجال التقني أن الأستخدامات السلبية المستقبلية للشبكات المظلمة** تشير النتائج إلى أنه من المتوقع أن يزداد عدد مستخدمي الشبكات المظلمة في المستقبل القريب نظرًا للمميزات التي تتمتع بها، وعلى رأسها إخفاء هوية المستخدم. ولكن هناك رأي واحد فقط يشكك في التخوفات من الاستخدامات

المستقبلية للشبكات المظلمة، وذلك لقلة استخدامها بشكل كبير في مصر، حيث لا تتعدى نسبة استخدام المصريين لهذه النوعية من الشبكات سوى ٤%.

- وفقًا لإجابات الخبراء في المجال التشريعي، تشير النتائج إلى أن أبرز الاستخدامات غير القانونية للشبكات المظلمة في المستقبل هي: الاتجار بالمخدرات والأسلحة وترويج البرمجيات الخبيثة، مثل برامج الفيروسات، وتجارة الأعضاء البشرية، وأدوات الجرائم الإلكترونية، والاستغلال الجنسي للأطفال، وشراء العقاقير غير المشروعة والأسلحة والسلع المقلدة وبطاقات الائتمان المسروقة والبيانات المخترقة، والعملات الرقمية وجوازات السفر. ويؤكد ذلك على التنوع في الاستخدامات غير المشروعة للشبكات المظلمة في المستقبل. ويجب على الحكومات والجهات المعنية اتخاذ إجراءات صارمة لمكافحة هذه الجرائم وتعزيز الوعي العام بأهمية الأمن السيبراني.

- تباينت آراء الخبراء في مجال الإعلام الرقمي بشأن استخدامات الشبكات المظلمة، حيث يرى بعضهم أنها توفر منبرًا مجانيًا لنشطاء الرأي والمعارضة كبديل عن منصات التواصل الاجتماعي، دون الكشف عن هويتهم وتعقبهم من قبل حكوماتهم. ويرون آخرون خطورة الاستخدام الإعلامي السلبي للشبكات المظلمة، حيث يتمثل ذلك في اختراق حسابات المنصات الرقمية مثل منصة "نتفليكس وشاهد"، بالإضافة إلى استخدامها في نقل مواد إعلامية لا يرغب المشاهد في رؤيتها، مثل المواد الإباحية، وزيادة المنشورات الإعلانية التي تحث على التطرف والانضمام للجماعات الإرهابية. ويجب على الحكومات والمؤسسات المعنية تحديد الخطورات المحتملة للاستخدامات غير القانونية للشبكات المظلمة واتخاذ إجراءات صارمة لمواجهتها وتعزيز الوعي العام بأهمية الأمن السيبراني.

- **أسفرت نتائج محور أساليب مواجهة مخاطر الشبكات المظلمة** إلى اتفاق واختلاف الخبراء عينة الدراسة فى المجالات الثلاثة ، فقد رأى بعض الخبراء فى المجال التقنى والقانونى بأن هناك صعوبة في تتبع مجرمي شبكات الدارك نتيجة الفجوة الرقمية، حيث يستحيل اختراقها تكنولوجيا، مما يصعب تعقبهم من قبل السلطات القانونية وتطبيق القانون عليهم. بينما يرى فريق آخر أن هناك بعض الدول نجحت من الناحية القانونية والتكنولوجية في استصدار قوانين لمتابعة مجرمي الشبكات المظلمة وتطبيق القانون عليهم.

التوصيات:

- إجراء مجموعة من الدراسات البينية المستقبلية لمراقبة ورصد الأثار الاجتماعية والسياسية والنفسية والاقتصادية التي يتركها استخدام الشبكات المظلمة، سواء على المجتمع بشكل عام أو على المستخدمين بشكل خاص.
- توجيه الاهتمام نحو إنشاء مراكز بحثية تكنولوجية تمكن الباحثين من إجراء الدراسات الإعلامية التي تتطلب مهارات تقنية متقدمة، مما يتيح ذلك للباحثين تطبيق الأبحاث العلمية التي لا يمكن إجراؤها في بيئة بحثية تقليدية غير متوافقة مع مجال الإعلام الرقمي، ويجب أن يكون لدى هذه المراكز التكنولوجية القدرة على التعامل مع البرامج المحددة المطلوبة للوصول إلى الشبكات المظلمة، سواء كان المستخدم شخصًا عاديًا أو باحثًا أكاديميًا.
- إعادة النظر في القوانين والتشريعات المنظمة لاستخدام التكنولوجيا، بهدف إصدار قانون يمكن للدولة تنفيذه لمواجهة التطور السريع في تكنولوجيا الإعلام الرقمي، تمامًا كما فعلت بعض الدول.
- إنشاء وحدات تكنولوجية مشابهة لتلك التي أنشأتها فرنسا ونيوزيلندا والولايات المتحدة والإمارات والمملكة العربية السعودية، والتي تهتم برصد استخدامات التقنيات الجديدة في مجال التواصل الرقمي، ويهدف ذلك إلى رصد الجماعات التي تستخدم تلك التقنيات في أنشطة غير قانونية.
- تصميم حملات إعلامية شاملة ومكثفة عبر جميع وسائل الإعلام التقليدية والرقمية، بهدف زيادة الوعي التكنولوجي والقانوني لدى المستخدمين حول خطورة الشبكة المظلمة.

مراجع الدراسة:

1- Jagdish Sheth , "Prediction of Attitudes – A Comparative Study of the Rosenberg, Fishbein and Sheth Models**", journal of Advances in Consumer Research**, Vol.2, pp. 389-404, 1989. Available at**:** https://www.jagsheth.com.

2- judith G Smetana& Nancy Adler, "Fishbein's Value x Expectancy Model: An Examination of Some Assumptions", **journal of Personality and Social Psychology Bulletin**", Vol.6, No.1, Pp.89-96, 1998. Available at: https://www.researchgate.net

3- M. Fishbein and I. Ajzen, "**Belief, Attitude, Intention, and Behavior, An Introduction to Theory and Research**, (Reading, MA: Addison-Wesley, 2002), pp.13-188. Available at: https://www.researchgate.net.

4- James R Bettman, Noel Capon, and Richard J Lutz, "Cognitive Algebra in Multi-Attribute Attitude Models," **Journal of Marketing Research",** vol.12, No.2, p. 151, 2011. Available at: https://people.duke.edu

5- Oli T. Ahtola, "The Vector Model of Preferences: An Alternative to the Fishbein Model", **Journal of Marketing Research, vol**. 34, No.8, pp.52-59, 2009. https://www.sciencedirect.com

6- Sumeet Raghunath & Yache Vishal Shivra **,"**Invisible Web"**, International Journal of Trend in Scientific Research and Development,** Vol.2,No.4,pp. 56-64, **2020.** Available at**:** www.ijtsrd.com

7- Nuruddin Bin Razali, "The Dark Web A Nest for Cyber Criminals", **Computing Department Faculty Of Communication, Visual Arts And Computing**, UNISEL, (Bestari Jaya, Selangor, Malaysia),pp.32-45, 2018. Available at: https://www.sciencedirect.com

8- Mohd Faizan and Raees Ahmad Khan, Exploring and analyzing the dark Web: A new alchemy, **journal of First Monday**, Vol. 24, No., pp. 56-69, 2019. Available at: https://www.researchgate.net.

9- Shillito, Matthew Robert, "untangling the 'Dark Web': an emerging Technological challenge for the criminal law", **journal of Information & Communications Technology Law**, Vol. 28, Issue. 2, pp. 186-207, 2019 Available at: https://www.ebsco.com.

١٠- رامى متولى القاضى، مكافحة الإجرام المنظم عبر شبكة الإنترنت المظلمة : دراسة تحليلية فى التشريع المصرى، **بحث منشور فى: المجلة الجنائية القومية**، المجلد الرابع والستون، العدد الثالث، نوفمبر ٢٠٢١. ، ص ص ٤٤-١٠٥. متاح على موقع:

https://ncj.journals.ekb.eg

11- Natalia Grivas, "Dark Web and ISIS**", Journal of Quantitative Criminology**, Vol.23, issu.3, pp. 113-121, 2017. Available at: https://www.academia.edu.

12- Goldman, Z. K., Maruyama, E., Rosenberg, E., Saravalle, E., & Solomon-Strauss, J., "Terrorist use of virtual currencies, containing the Potential Threat", **Washington DC Center for a New American Security**, p.27, 2017. Available at: https://www.academia.edu.

١٣- محمد على محمود كرباس، جرائم غسل الأموال فى ضوء الفقه والقضاء- دراسة مقارنة، **رسالة ماجستير**، (جامعة أم درمان الإسلامية، السودان) ٢٠١٦، ص ٥٢.

١٤- انظر: **الموقع الإلكترونى لمركز المعلومات ودعم اتخاذ القرار بمجلس الوزراء المصرى** على الرابط، التالى:

https://www.idsc.gov.eg.

15- Julia Ebner and Cécile Guerin**, "**From Satirical Memes to Massacring Muslims: How the Dark Web Turns White Supremacists Into Terrorists"**,** March 19, 2019. Available at: https://www.isdglobal.org.

16-Saini, Jaspal Kaur and Bansal, Divya, "A Comparative Study and Automated Detection of Illegal Weapon Procurement over Dark Web", **Journal of Cybernetics and Systems**, vol.50, issu.5, pp.405-416,2019Available at: https://www.tandfonline.com.

17- Gabriel Weimann, "Terrorist Migration to the Dark Web, Source", **Journal of Perspectives on Terrorism**, Vol. 10, No.3, pp, 40-44, 2016. Available at: https://web.s.ebscohost.com.

18- Emily Chiang, Dark web: Study reveals how new offenders get involved in online pedophiles communities. Available at: https://theconversation.com.

19- Navi Mumbai, & Maharashtr, "Invisible Web", **International Journal of Trend in Scientific Research and Development"**, Vol.2, Issue. 4, May-Jun 2018, Available at: www.ijtsrd.com

20- Scott W. Duxbury & Dana L. Haynie, "The Network Structure of Opioid Distribution on a Dark net Crypto market", **Journal of Quantitative Criminology**,vol.34,issu.1, pp,921-941,2018 Available at : https://link.springer.com

21- Carly Chatfield, "Legitimate Uses for the Dark Web", **Security Journal**, vol. 25, issue. 1, pp, 57–75, 2022. Available at: https://www.makeuseof.com.

22- Mihnea Mirea ,Victoria Wang & Jeyong Jung, "The not so dark side of the dark net: a qualitative study", Published on, **Institute of Criminal Justice Studies (ICJS), University of Portsmouth, Portsmouth, UK**,2019. Available at: https://www.port.ac.uk.

23- Moore, D., and T. Rid, "Cryptopolitik and the Dark net", **Global Politics and Strategy**, Vol.58, issu.1, pp, 7–38, 2016. Available at: https://www.tandfonline.com.

24- Arbër S. Beshiri , Arsim Susuri, "Dark Web and Its Impact in Online Anonymity and Privacy: A Critical Analysis and Review", **Journal of Computer and Communications**, Vol.7, Issue.30, pp, 30-437, 2019. Available at: http://www.scirp.org/journal/jcc

25- Cybercrime and Dark Web Research, **Dark Web Monitoring: The Good, the Bad, and the Ugly**. Available at: https://www.digitalshadows.com

٢٦- رحاب أحمد فايز، أدبيات الويب المظلم بمرصد بيانات شبكة العلوم WOS دراسة تحليلية ببليومترية ، **بحث منشور فى :المجلة العربية للأرشيف والتوثيق والمعلومات** ، السنة الثالثة والعشرون ، العدد ٤٦، ديسمبر ٢٠١٩.

هوامش المقابلات

(*)- قامت الباحثة بإجراء المقابلات الفردية المتعمقة فى الفترة من ا سبيتمبر ٢٠٢٢ إلى نهاية مارس ٢٠٢٣، مع كل من: خالد البرماوى ، مدرب الإعلام الرقمى بشركة DIGI ME ، أحمد عصمت ، الرئيس التنفيذى لمنتدى الأسكندرية للإعلام، أسامه الديب، مدير تحرير الملتيميديا لمؤسسة أونا للصحافة والإعلام، طارق عطية ، الرئيس التنفيذى ل البرنامج المصرى لتطوير الإعلام، د. رضوى عبد اللطيف ،مساعد رئيس تحرير الأهرام ، وخبير صناعة الإعلام الرقمى، علاء الغطريفي، رئيس التحرير التنفيذي لمجموعة أونا للإعلام، د. مصطفى أبو جمرة ، الرئيس التنفيذى لشركة media sci ، أحمد عبد البديع مسؤول الاتصال الاعلامى بمجموعة المستقبل القابضة للإعلام والاتصالات ، د. أشرف جلال استاذ الإذاعة والتليفزيون – كلية الإعلام – جامعة القاهرة، د. فتحى شمس الدين، استاذ الإذاعة والتليفزيون المساعد- كلية الأداب جامعة بنها، اللواء محمد حجازى ، الرئيس السابق للجنة التشريعات فى وزارة الاتصالات وتكنولوجيا المعلومات، د. الدكتور بهاء الدين حسن ، خبير امني المعلومات والرئيس التنفيذى لشركة isec ، د. عادل عبد المنعم خبير الأمن السيبرانى والأدلة الرقمية بالمركز العربي للأمن السيبراني بالاتحاد الدولي للاتصالات، أحمد سعيد ، استاذ القانون الدولى بالجامعة البريطانية، هشام صبرى، النائب الاسبق لمعهد تدريب الضباط بأكاديمية الشرطة،

أحمد السخاوى ، مدير الأمن السيبرانى فى شركة اوميجا جيت للحلول المتكاملة، - اللواء محمود الرشيدي مساعد وزير الداخلية الاسبق وخبير الانترنت وأمن المعلومات، اللواء يحيي كدواني، عضو لجنة الدفاع والأمن القومي بمجلس النواب، اللواء عادل العمدة المستشار بأكاديمية ناصر العسكرية العليا، اللواء محمد عبد المقصود رئيس محور دعم القرار بمركز المعلومات، مهندس وليد حجاج ، عضو لجنة الثقافة الرقمية والبنية المعلوماتية بالمجلس الأعلى للثقافة، مهندس طارق عباس، مدير هندسة النظم .بشركة بالو التو نتوركس، د. توفيق اسماعيل ، خبير تكنولوجيا المعلومات ، عضو جمعية خبراء العلوم والتكنولوجيا، عمرو صبحي عبد العاطي ، خبير أمن المعلومات والتحول الرقمى ، د. عربى السيد كشك، العميد السابق لكلية الحاسبات والمعلومات جامعة المنوفية ، عادل ابو المجد سويسى، العميد السابق لكلية الحاسبات والمعلومات جامعة اسيوط،، أحمد على ، مهندس برمجيات بشركة فيس بوك، مصطفى عمران ، الرئيس التنفيذى لهيئة تنمية صناعة التكنولوجيا، مهندس أحمد إدريس، خبير تكنولوجيا المعلومات ، د. أحمد بهاء، الأستاذ بكلية الحاسبات والمعلومات بجامعة حلوان.

١- عمرو صبحي عبد العاطي ، خبير أمن المعلومات والتحول الرقمى.

٢- عادل ابو المجد سويسى، العميد السابق لكلية الحاسبات والمعلومات جامعة أسيوط.

٣- مصطفى عمران ، الرئيس التنفيذى لهيئة تنمية صناعة التكنولوجيا.

٤- د. عربى السيد كشك، العميد السابق لكلية الحاسبات والمعلومات جامعة المنوفية.

٥- مهندس أحمد إدريس، خبير تكنولوجيا المعلومات، بوزارة الاتصالات.

٦- د. توفيق اسماعيل ، خبير تكنولوجيا المعلومات ، عضو جمعية خبراء العلوم والتكنولوجيا.

٧- مهندس طارق عباس، مدير هندسة النظم بشركة بالو التو نتوركس.

٨- وليد حجاج ، مهندس عضو لجنة الثقافة الرقمية والبنية المعلوماتية بالمجلس الأعلى للثقافة.

٩- أحمد على ، مهندس برمجيات بشركة فيس بوك.

١٠-، د. أحمد بهاء، الأستاذ بكلية الحاسبات والمعلومات بجامعة حلوان.

١١-د. عادل عبد المنعم خبير الأمن السيبرانى والأدلة الرقمية بالمركز العربي للأمن السيبراني بالاتحاد الدولي للاتصالات، هشام صبرى، النائب الاسبق لمعهد تدريب الضباط بأكاديمية الشرطة، د. الدكتور بهاء الدين حسن ، خبير أمن المعلومات والرئيس التنفيذى لشركة isec .

١٢- اللواء محمد حجازى ، الرئيس السابق للجنة التشريعات فى وزارة الاتصالات وتكنولوجيا المعلومات.

١٣-، د.أحمد سعيد ، استاذ القانون الدولى بالجامعة البريطانية.

١٤- اللواء محمود الرشيدي مساعد وزير الداخلية الاسبق وخبير الانترنت وأمن المعلومات.

١٥- أحمد السخاوى ، مدير الأمن السيبرانى فى شركة اوميجا جيت للحلول المتكاملة.

١٦- اللواء يحيي كدواني، عضو لجنة الدفاع والأمن القومي بمجلس النواب، اللواء عادل العمدة المستشار بأكاديمية ناصر العسكرية العليا، اللواء محمد عبد المقصود رئيس محور دعم القرار بمركز المعلومات.

١٧- د. عادل عبد المنعم ، مرجع سابق- هشام صبرى، مرجع سابق- وليد حجاج، مرجع سابق- أحمد السخاوى، مرجع سابق- اللواء محمود الرشيدي، مرجع سابق.

١٨-، د. رضوى عبد اللطيف ،مساعد رئيس تحرير الأهرام ، وخبير صناعة الإعلام الرقمى- ، د. أشرف جلال استاذ الإذاعة والتليفزيون – كلية الإعلام – جامعة القاهرة، د. فتحى شمس الدين، استاذ الإذاعة والتليفزيون المساعد- كلية الأداب جامعة بنها- أحمد عصمت ، الرئيس التنفيذى لمنتدى الأسكندرية للإعلام.

١٩- علاء الغطريفي، رئيس التحرير التنفيذي لمجموعة أونا للإعلام- أحمد عبد البديع مسؤول الاتصال الاعلامى بمجموعة المستقبل القابضة للإعلام والاتصالات.

٢٠- أحمد إدريس، مهندس وخبير تكنولوجيا المعلومات بوزارة الاتصالات- د. عربى السيد كشك، العميد السابق لكلية الحاسبات والمعلومات جامعة المنوفية- د. أحمد بهاء، الأستاذ بكلية الحاسبات والمعلومات بجامعة حلوان.

٢١- وليد حجاج، مرجع سابق- عادل السويسى، مرجع سابق.

٢٢- طارق عباس، مرجع سابق- مصطفى أو جمرة ، مرجع سابق- أحمد إدريس، مرجع سابق.

٢٣- مصطفى عمران ، مرجع سابق- أحمد على، مرجع سابق-عمرو صبحى، مرجع سابق.

٢٤-توفيق اسماعيل، مرجع سابق.

٢٥- عادل العمدة ، مرجع سابق- محمود الرشيدى، مرجع سابق

٢٦-هشام صبرى ، مرجع سابق- محمود حجازى، مرجع سابق.

٢٧- عادل عبد المنعم ، مرجع سابق- أحمد السخاوى، مرجع سابق- بهاء الدين حسن، مرجع سابق.

٢٨- د.أشرف جلال، مرجع سابق- فتحى شمس الدين ، مرجع سابق، - أحمد عبد البديع ، مرجع سابق.

٢٩- علاء الغطريفي، مرجع سابق- أسامه الديب، مرجع سابق- أحمد عصمت، مرجع سابق.

٣٠- د. رضوى عبد اللطيف، مرجع سابق-خالد البرماوى ، مرجع سابق -أحمد عصمت، مرجع سابق.

٣١- د. مصطفى أبو جمرة، مرجع سابق.

٣٢- أحمد على ، مرجع سابق- عادل أبو المجد، مرجع سابق.

٣٣- وليد حجاج ، مرجع سابق- أحمد بهاء، مرجع سابق.

٣٤- طارق عباس، مرجع سابق- مصطفى عمران، مرجع سابق.

٣٥- عمرو صبحى، مرجع سابق- وليد حجاج ، مرجع سابق.

٣٦- عربى السيد ، مرجع سابق- أحمد إدريس، مرجع سابق.

٣٧- هشام صبرى ، مرجع سابق- عادل عبد المنعم ، مرجع سابق.

٣٨- د.أحمد سعيد ، مرجع سابق.

٣٩- محمود الرشيدى ، مرجع سابق.

٤٠- يحيى الكدوانى ، مرجع سابق.

٤١- محمد عبد المقصود ، مرجع سابق- بهاء الدين حسن، مرجع سابق

٤٢- أحمد السخاوى، مرجع سابق -عادل العمدة، مرجع سابق.

٤٣- محمد عبد المقصود ، مرجع سابق- بهاء الدين حسن، مرجع سابق.

٤٤- أشرف جلال، مرجع سابق - فتحى شمس الدين، مرجع سابق.

٤٥- مصطفى أبو جميرة ، مرجع سابق - علاء الغطريف، مرجع سابق.

٤٦- أحمد عصمت، مرجع سابق - أسامه الديب ، مرجع سابق - خالد البرماوى، مرجع سابق.

٤٧- رضوى عبد اللطيف، مرجع سابق.

٤٨- أحمد عبد البديع ، مرجع سابق - أشرف جلال ، مرجع سابق - طارق عطية، مرجع سابق .