Journal of Al-Farabi for Humanity Sciences Volume (9), Issue (1) January (2026)

ISSN: 2957-3874 (Print)
Journal of Al-Farabi for Humanity Sciences (JFHS)
https://iasj.rdd.edu.iq/journals/journal/view/95
مجلة الفارابي للعلوم الإنسانية تصدرها جامعة الفارابي

الأرهاب الالكتروني في العصر الرقمي: التحديات والمخاطر

هـــدى عبــد الحسيــن فيــاض
جامعة النهرين/كلية العلوم السياسية

Cyberterrorism in the Digital Age: Challenges and Risks

huda.abdeh@nahrainuniv.edu.iq

الخلاصة:

يمثل الإرهاب الإلكتروني أحد أخطر التهديدات المعاصرة للأمن القومي واستقرار الدول، لما يتسم به من طابع عابر للحدود، وتطور تقني متسارع، وتعدد في الأدوات والأساليب. وقد أظهر التحليل أن مواجهة هذه الظاهرة لا يمكن أن تقتصر على المعالجات الأمنية التقليدية، بل تتطلب مقاربة شاملة ومتكاملة تقوم على تعزيز البنية التحتية الرقمية، وتحديث الأطر القانونية والتشريعية، وبناء القدرات البشرية، إلى جانب توسيع التعاون الدولي وتكثيف الجهود التقنية والاستخباراتية. وعليه، فإن اعتماد استراتيجيات وطنية ودولية منسقة في مجال الأمن السيبراني يُعد شرطًا أساسيًا للحد من مخاطر الإرهاب الإلكتروني، وضمان أمن الفضاء الرقمي وحماية مصالح الدول والمجتمعات في العصر الرقمي.

الكلمات المفتاحية: الارهاب الالكتروني، الامن السيبراني، مكافحة الارهاب، التحديات, المخاطر.

Abstract:

Cyberterrorism represents one of the most serious contemporary threats to national security and state stability, due to its transnational nature, rapid technological evolution, and the diversity of its tools and methods. The analysis has shown that confronting this phenomenon cannot be limited to traditional security measures; rather, it requires a comprehensive and integrated approach based on strengthening digital infrastructure, updating legal and legislative frameworks, building human capacities, and expanding international cooperation alongside intensified technical and intelligence efforts. Accordingly, the adoption of coordinated national and international cybersecurity strategies constitutes a fundamental requirement for mitigating the risks of cyberterrorism and ensuring the security of cyberspace while safeguarding the interests of states and societies in the digital age.Keywords: Cyber terrorism, Cybersecurity, Counter-terrorism, Security challenges.

المقدمة

يشكل الإرهاب الإلكتروني أحد أبرز التهديدات الحديثة التي تواجه الدول والمجتمعات في العصر الرقمي، حيث أتاح التطور التكنولوجي والتحول إلى الاعتماد الكلي على الفضاء الإلكتروني إمكانية تنفيذ هجمات دقيقة وواسعة النطاق، تصل إلى حد تهديد الأمن الوطني واستقرار البنى التحتية الحيوية. فقد أصبح الفضاء الرقمي منصة مفتوحة للجماعات الإرهابية لتنفيذ عملياتها، سواء عبر اختراق الأنظمة الحكومية والعسكرية، أو تعطيل الخدمات الحيوية، أو نشر الفيروسات والبرمجيات الخبيثة، أو ممارسة الابتزاز الإلكتروني، أو التجسس الرقمي، وصولًا إلى تجنيد الأفراد ونشر الدعاية المتطرفة, ويتسم الإرهاب الإلكتروني بتعقيده وامتداده على مستويات متعددة، فهو ليس مجرد تهديد تقني، بل يشمل أبعادًا قانونية، وأمنية، واجتماعية، واقتصادية، وسياسية، ما يجعل مواجهته تحديًا معقدًا يتطلب مقاربة شاملة ومتكاملة. وقد أدى الاعتماد المتزايد على الشبكات الرقمية والتكنولوجيا الحديثة إلى اتساع دائرة المخاطر، بحيث يمكن للهجمات الإلكترونية أن تؤثر على استقرار المؤسسات، وثقة المواطنين، وفاعلية القرارات الحكومية, ويهدف هذا البحث إلى تحليل الظاهرة بدقة، من خلال استعراض أشكال الإرهاب الإلكتروني، والتحديات المصاحبة له، والمخاطر الناتجة عنه، مع تقديم رؤية شاملة حول الأساليب الممكنة للتصدي لهذه الظاهرة المعقدة. كما يسعى البحث إلى تسليط الضوء على أهمية تطوير الإجراءات التقنية والقانونية والأمنية، وتعزيز التعاون الدولي والوعي المجتمعي، باعتبارها أدوات رئيسية للحد من تأثيرات الإرهاب الإلكتروني وضمان الأمن الرقمي في العصر الحديث.

هدف البحث:

يهدف البحث الى عرض وتبيان ماهية الارهاب من خلال طرح مفهومه برؤية اكاديمية والوقوف على اهم التحديات والمخاطر التي يفرضها الارهاب الالكتروني ووضع استراتيجية فاعلة في مواجهة الارهاب الالكتروني.

فرضية البحث:

نفترض أن التطور المتسارع في تكنولوجيا المعلومات والاتصالات، إلى جانب ضعف الأطر القانونية والسياسية المنظمة للفضاء السيبراني، قد أسهم في تصاعد وتيرة الإرهاب الإلكتروني، وتحول هذا النوع من التهديد إلى أداة استراتيجية بيد الفاعلين من غير الدول، بما يؤدي إلى تقويض السيادة الرقمية، وزعزعة الاستقرار السياسي والاجتماعي والاقتصادي للدول.

اشكالية البحث:

تكمن اشكالية البحث في مجموعة من التساؤلات من ابرز هذه التساؤلات ما مدى الخطر الناجم عن الارهاب الالكتروني والابعاد السياسية والاقتصادية والاجتماعية ؟ ومدى سرعة التصدي للخطر الناجم عنه ؟ وهل يمكن وضع الية للتصدي والرد عن مثل هذه المخاطر الالكترونية؟

اهمية البحث:

تنبع أهمية هذا البحث من تناوله لظاهرة الإرهاب الإلكتروني بوصفها أحد أخطر التهديدات المستجدة التي تواجه الأمن القومي واستقرار الدول في العصر الرقمي، لاسيما في ظل الاعتماد المتزايد على التكنولوجيا والفضاء السيبراني في مختلف القطاعات الحيوية. وتكمن أهمية البحث في سعيه إلى توضيح الأبعاد المتعددة للإرهاب الإلكتروني، والكشف عن مخاطره التقنية والاقتصادية والاجتماعية والسياسية، فضلًا عن تحليل التحديات التي تواجه الدول في مكافحته.

المحور الاول: مفهوم الارهاب الالكتروني

يُعدّ الإرهاب من أخطر الظواهر التي تواجه المجتمعات والدول في العصر الحديث، إذ يقوم على استخدام العنف أو التهديد به بهدف بثّ الرعب والخوف بين الناس، والتأثير على استقرار الأمن والنظام العام لتحقيق أهداف سياسية أو أيديولوجية أو عقائدية, على الرغم من تعدد التعريفات واختلاف وجهات النظر حوله، يبقى الإرهاب سلوكًا منظمًا يستهدف المدنيين والمنشآت الحيوية لإحداث أكبر قدر من التأثير النفسي والمادي، مما يجعله تهديدًا مباشرًا للسلم والأمن سواء على المستوى المحلي أو الدولي[١], وذكر مصطلح الارهاب في القران على انه اثارة الرعب في قوله تعالى "إِيَّيَ فَٱرۡهَبُونِ"[٢], وقوله تعالى "وَٱسۡتَرۡهَبُوهُمۡ وَجَآءُو بِسِحۡرٍ عَظِيمٖ" [٣], فكلمة الارهاب في القران الكريم وردت بدلالات الرعب في قلوب الناس. اما من الناحية اللغوية لم تذكر المعاجم العربية القديمة كلمة الارهاب ولكنها عرفت الفعل رهبَ يرهبُ رهباً وهو يعني الاخافة وقد تداركت المعاجم ذلك الحديث فقد جاء في المعجم الوجيز ان الارهابيين هو وصف يطلق على الذين يسلكون سبل العنف والارهاب لتحقيق اهدافهم السياسية[٤].

اما من الناحية الاصطلاحية فتعرفه الاتفاقية العربية لمكافحة الارهاب انه كل فعل من افعال العنف او التهديد اياً كانت بواعثه او اغراضه يقع تنفيذا لمشروع اجرامي فردي او جماعي ويهدف الى القاء العنف او التهديد او الرعب بين الناس او ترويعهم بإيذائهم او تعريض حياتهم او حريتهم او امنهم للخطر او الحاق الضرر بالبيئة او بأحد المرافق او الاملاك العامة او الخاصة او احتلالها او الاستيلاء عليها[٥], كما نجد ان كل الدول لم تتفق على وضع تعريف محدد للارهاب الا انه في الوقت نفسه نجد ان كل دولة او منظمة اقليمية اعطت تعريفا للارهاب انطلاقا من وضعها ومصالحها, وتعرف الموسوعة السياسية الارهاب هو استخدام العنف غير القانوني او التهديد به بأشكاله المختلفة كالاغتيال و التشويه والتعذيب والتخريب والنفس بغية تحقيق هدف سياسي معين وبشكل عام هو استخدام الاكراه للإخضاع طرف مناوئ لمشيئة الجهة الارهابية [٦], وكذلك يعرف المعجم السياسي الارهاب بأنه (محاولة نشر الذعر والفزع لأغراض سياسية وهو وسيلة تستخدمها حكومة استبدادية او دكتاتورية لأجبار الشعب على الاستسلام لها) [٧].وقد عرف قانون مكافحة الارهاب العراقي ذي الرقم (١٣) لسنة ٢٠٠٥ وبمقتضى احكام المادة الاولى المقصود بالارهاب (هو كل فعل اجرامي يقوم به فرد او جماعة منظمة استهدفا فردا او مجموعة افراد او جماعات او مؤسسات رسمية او غير رسمية اوقع الضرر بالممتلكات العامة او الخاصة بغية الاخلال بالوضع الامني او الاستقرار والوحدة الوطنية او ادخال الرعب والخوف والفزع بين الناس او اثارة الفوضى تحقيقا لغايات ارهابية).[٨] وعرف قانون مكافحة الارهاب الامريكي لسنة ١٩٥٨ في المادة الاولى منه الارهاب بأنه الاستخدام غير المشروع للقوة والعنف في حق الافراد او الممتلكات بهدف ترويع الحكومة والمدنيين او قسم منهم في اطار السعي الى تحقيق اهداف سياسية او اجتماعية[٩], ولا يختلف مفهوم الارهاب الالكتروني عن مفهوم الارهاب التقليدي فقط يختلف من حيث الادارة المستخدمة في تنفيذ المشروع فالإرهاب الالكتروني يعتمد على استخدام المكانيات العلمية والتقنية واستغلال وسائل الاتصال والشبكات المعلوماتية من اجل تخويف

وترويع الاخرين والحاق الضرر بهم وتهديدهم[١٠].ويتكوّن مصطلح الإرهاب الإلكتروني (Cyberterrorism) من كلمتين: Cyber وتعني الإنترنت أو الفضاء السيبراني، وTerrorism وتعني الإرهاب, وقد برز هذا المصطلح وانتشر استعماله مع الثورة التقنية والتطور الهائل في الحضارة الرقمية خلال عصر المعلومات، خاصة بعد إساءة استخدام الفضاء الإلكتروني بطرق تطورت تدريجيًا من جرائم إلكترونية عادية إلى أعمال إرهابية كاملة تُنفَّذ عبر الوسائط الرقمية, وعلى الرغم من كثرة تداول المصطلح في وسائل الإعلام العالمية خلال السنوات الأخيرة، لا يزال الباحثون يختلفون في وضع تعريف جامع ودقيق للإرهاب الإلكتروني، سواء من حيث طبيعته أو تاريخ ظهوره ونشأته، وذلك بسبب تنوع الأساليب الإرهابية وتباين وجهات النظر اللغوية والقانونية المتعلقة به[١١].ويُعرَّف الإرهاب الإلكتروني بأنه كل فعل عدواني أو تخويفي أو تهديدي، ماديًا كان أو معنويًا، يُنفَّذ عبر الوسائل والتقنيات الإلكترونية، سواء صدر عن دول أو جماعات أو أفراد، مستهدفًا الفضاء الإلكتروني باعتباره بيئة ووسيطًا لتنفيذ أنشطة إرهابية أو أعمال حرب, ويتجلى هذا النوع من الإرهاب في الهجمات المباشرة على البنية التحتية المعلوماتية، أو في إحداث تأثيرات نفسية ومعنوية عبر نشر الكراهية الدينية والتحريض الفكري، كما قد يظهر بصور رقمية تعتمد على استخدام أسلحة إلكترونية حديثة مخصّصة للمعارك الإلكترونية، وقد يقتصر أثره على العالم الرقمي أو يمتد ليصيب أهدافًا مادية وحيوية مرتبطة بالبنى التحتية للدول[١٢].

المحور الثاني: اشكال الارهاب الالكتروني

تعددت أشكال الإرهاب الإلكتروني، ومن أبرزها:

١-اختراق الأنظمة الحكومية والعسكرية: يُعدّ اختراق الأنظمة الحكومية والعسكرية أحد أخطر أشكال الإرهاب الإلكتروني، لما يشكّله من تهديد مباشر للبُنى الاستراتيجية والأمن الوطني للدول, إذ تستهدف هذه الهجمات الأنظمة الحساسة بهدف الوصول غير المشروع إلى البيانات أو تعطيل الخدمات الحيوية وتُظهر الدراسات أن الجماعات الإرهابية والجهات المعادية باتت تستخدم أدوات متقدمة لاختراق بُنى الدولة الرقمية، ما يزيد من مستوى المخاطر وتركّز الهجمات السيبرانية الموجهة نحو الأنظمة العسكرية على إضعاف قدرات القيادة والسيطرة، والتشويش على شبكات الاتصالات، وجمع معلومات استخباراتية سرّية قد تغيّر ميزان القوة في النزاعات المسلحة, وفي العديد من الحالات، تعمل الهجمات الإلكترونية كمرحلة تمهيدية للعمليات العسكرية التقليدية، بهدف إرباك الدولة المستهدفة وتعطيل جاهزيتها الدفاعية[١٣]كما تُعدّ الهجمات المتقدمة المستمرة (APT) إحدى أخطر الوسائل المستخدمة، إذ يستطيع المخترقون التغلغل داخل الشبكات الحكومية والبقاء فيها لفترات طويلة دون اكتشافهم، ما يؤدي إلى استنزاف معلوماتي وتقني خطير وللتعامل مع هذه المخاطر، عمدت العديد من الدول إلى تطوير استراتيجيات وطنية تعتمد على تعزيز الدفاعات الرقمية، وتطوير أنظمة إنذار مبكر، وتوسيع التعاون بين المؤسسات الأمنية والاستخبارية[١٤].

٢- الهجمات على البُنى التحتية الحيوية : تُعدّ الهجمات الإلكترونية على البُنى التحتية الحيوية من أخطر أشكال الإرهاب الإلكتروني التي تستهدف الدول، نظرًا لما تمثّله هذه البُنى من عمود فقري للحياة اليومية والأمن الوطني, وتشمل هذه البُنى قطاعات الكهرباء والمياه والاتصالات والمواصلات والطاقة والمستشفيات والمطارات وغيرها من المنشآت الحساسة التي يؤدي تعطيلها إلى شلل واسع في الدولة وتكتسب هذه الهجمات خطورتها من قدرتها على التأثير المباشر في حياة المواطنين، وإحداث اضطرابات اقتصادية وأمنية كبيرة قد تمتدّ آثارها لأسابيع أو أشهر[١٥], وتسعى الجهات الإرهابية والخصوم الدولية من خلال استهداف هذه القطاعات إلى تحقيق مكاسب استراتيجية مثل إرباك الحكومة، إضعاف الثقة بالمؤسسات، أو خلق حالة من الصدمة الاجتماعية. كما تُظهر الحوادث العالمية أن الهجمات على شبكات الكهرباء ومحطات معالجة المياه والمستشفيات باتت أكثر تعقيدًا، مع اعتماد المهاجمين على برمجيات خبيثة متطورة قادرة على تعطيل الأنظمة الصناعية (SCADA) والتحكم بها عن بُعد وتُعدّ الحادثة الشهيرة لهجوم "ستوكسنت" أحد أبرز الأمثلة على قدرة الهجمات السيبرانية على التغلغل داخل الأنظمة الصناعية الحساسة[١٦].

وتتزايد خطورة هذه الهجمات مع ارتفاع درجة الاعتماد على الأنظمة الرقمية والمنصّات الذكية لإدارة البُنى التحتية، مما يخلق مساحات واسعة للثغرات الأمنية في حال عدم تحديث الأنظمة بشكل دوري, وتؤكد الدراسات أن تعزيز أمن البُنى التحتية الحيوية يتطلب تطوير سياسات وطنية شاملة للأمن السيبراني، وبناء قدرات استجابة سريعة، وتكاملًا أكبر بين المؤسسات الأمنية والحكومية والخاصة لحماية القطاعات الحيوية من الانهيار المحتمل في حال حدوث هجمات واسعة النطاق[١٧].

٣- نشر الفيروسات والبرمجيات الخبيثة : يُعدّ نشر الفيروسات والبرمجيات الخبيثة أحد أكثر الأساليب شيوعًا وخطورة في مجال الإرهاب الإلكتروني، نظرًا لقدرة هذه الأدوات على الانتشار السريع وإحداث أضرار واسعة في الأنظمة الرقمية, وتعمل البرمجيات الخبيثة على اختراق الأجهزة والشبكات بهدف التجسس أو التخريب أو سرقة البيانات، وقد تُستخدم أحيانًا لابتزاز المؤسسات الحكومية والخاصة عبر تقنيات الفدية الرقمية ويتميّز هذا النوع من الهجمات بسهولة تنفيذه مقارنة بالأساليب الأكثر تعقيدًا، ما يجعله خيارًا مفضلًا لدى الجماعات الإرهابية والجهات

الإجرامية الإلكترونية[١٨].وتتنوّع البرمجيات الخبيثة بين فيروسات مدمّرة، وأحصنة طروادة، وبرمجيات فدية (Ransomware)، قادرة على التوسع الذاتي داخل الشبكات دون تدخل بشري, وقد أدت بعض الهجمات العالمية إلى خسائر اقتصادية كبيرة، مثل هجوم "WannaCry" الذي أصاب مئات الآلاف من الأنظمة حول العالم، بما في ذلك مؤسسات حكومية ومستشفيات وشركات نقل[3]. وتُظهر تقارير الأمن السيبراني أن مثل هذه الهجمات تسهم في تعطيل الخدمات الأساسية وإلحاق أضرار بالبُنى التحتية الرقمية، إضافة إلى تأثيراتها النفسية على المستخدمين والحكومات[١٩]. كما تعتمد الجماعات المتطرفة على نشر البرمجيات الخبيثة لأغراض التجسس، والتجنيد، وتنفيذ عمليات تخريبية موجهة تستهدف الأنظمة الحكومية أو العسكرية، مستفيدة من ثغرات أمنية في البرمجيات القديمة أو من خلال الهندسة الاجتماعية, وتؤكد الدراسات أن التصدي لهذه الهجمات يتطلب تطوير قدرات متخصصة في الكشف المبكر، واستخدام أنظمة متقدمة للحماية، وتعزيز وعي المستخدمين حول مخاطر الروابط المجهولة والملفات المرفقة المشبوهة[٢٠].

٤- الابتزاز الإلكتروني : يُعدّ الابتزاز الإلكتروني من أخطر أشكال الجرائم السيبرانية المرتبطة بالإرهاب الإلكتروني، نظرًا لقدرته على استهداف الأفراد والمؤسسات على حدّ سواء، وإحداث تأثيرات مالية ونفسية واسعة, ويعتمد هذا النوع من الهجمات على تهديد الضحية بنشر معلومات حساسة، أو تعطيل الأنظمة الإلكترونية، أو تدمير البيانات، ما لم يتم دفع مبالغ مالية أو تنفيذ مطالب معينة[1], وتتنوع أساليب الابتزاز بين اختراق الحسابات الشخصية، وسرقة الصور والملفات، واحتجاز البيانات عبر برمجيات الفدية التي تُعدّ اليوم أحد أكثر أشكال الابتزاز انتشارً[٢١].

وتعتمد الجماعات الإجرامية والإرهابية على الابتزاز الإلكتروني كوسيلة للحصول على تمويل سريع، إذ تكشف تقارير أمنية دولية أن بعض التنظيمات تستثمر بشكل مباشر في تطوير ونشر برمجيات الفدية أو التعاون مع مجموعات قرصنة متخصصة لتحقيق مكاسب مالية وقد استهدفت هذه الهجمات مستشفيات ومؤسسات حكومية وشركات مالية، وتسببت بخسائر تجاوزت مليارات الدولارات حول العالم، خاصة عند شلّ الأنظمة الحيوية لفترات طويلة, كما يحمل الابتزاز الإلكتروني أبعادًا اجتماعية ونفسية خطيرة، لاسيما حين يُستخدم لاستهداف الفئات الضعيفة أو ابتزاز موظفين داخل مؤسسات حكومية بهدف التجسس أو الحصول على معلومات سرّية. وتؤكد الدراسات أن الوعي الرقمي، وتدابير الحماية المتقدمة، والتدريب المؤسسي المستمر، تمثل عناصر أساسية للحد من مخاطر هذا النوع من الهجمات، إضافة إلى أهمية سنّ قوانين صارمة تُجرّم الابتزاز الإلكتروني وتُشدد العقوبات على مرتكبيه[٢٢].

٥- التجسس الإلكتروني : يعدّ التجسس الإلكتروني أحد أكثر الأساليب تطورًا وخطورة في مجال الإرهاب السيبراني، لما يتضمنه من محاولات للوصول غير المشروع إلى المعلومات الحساسة أو السرّية داخل المؤسسات الحكومية والعسكرية والاقتصادية. وتستهدف هذه الهجمات جمع بيانات استراتيجية يمكن استغلالها لإضعاف قدرات الدولة أو التأثير على قراراتها السياسية والأمنية[1]. ويعتمد التجسس الإلكتروني على أدوات متقدمة تشمل برمجيات التجسس، وتقنيات اختراق الأجهزة المحمولة، والاستفادة من الثغرات الأمنية في الأنظمة الرقمية, ويتميّز هذا النوع من الهجمات بطابعه السري وبقائه لفترات طويلة دون اكتشافه، إذ يعمل المهاجم عادة على التغلغل في الشبكة المستهدفة والحفاظ على وجوده داخلها بهدف مراقبة البيانات وسرقتها بشكل مستمر[3]. وتُظهر الدراسات أن العديد من الهجمات العالمية التي استهدفت وزارات الدفاع والطاقة والخارجية كانت ذات طابع تجسسي، وأن الجهة المنفذة غالبًا ما تكون مدعومة من جهات دولية أو تنظيمات متقدمة تمتلك قدرات تقنية عالية[٢٣].

كما تعتمد الجماعات الإرهابية على التجسس الإلكتروني لتعزيز عملياتها، سواء عبر مراقبة الاتصالات الحكومية، أو الحصول على معلومات أمنية، أو استهداف شخصيات سياسية وعسكرية. وتشير البحوث الحديثة إلى أن التجسس السيبراني أصبح جزءًا أساسيًا من الحروب الحديثة، حيث يُستخدم في جمع المعلومات الاستراتيجية، وتحديد الأهداف، وتهيئة المجال لعمليات لاحقة[5]. وتوصي التقارير الأمنية بتعزيز أنظمة الكشف المبكر، وتحديث البرمجيات بشكل دوري، وتقوية بنية التشفير كخط دفاع أول ضد الهجمات التجسسية[٢٤].

٦- الهجمات السيبرانية: هي عمليات عدوانية تُنفَّذ عبر الفضاء الإلكتروني من خلال جماعات إرهابية مدفوعة بدوافع سياسية، أيديولوجية، أو دينية، وتهدف إلى التأثير على الدول من خلال نشر الفوضى, يتم ذلك عبر استهداف البنية التحتية، مثل محطات توليد الطاقة، المياه، أو الاتصالات، وتعطيل الخدمات الحكومية الحيوية، أو التأثير على الحكومات والمؤسسات الأمنية عن طريق اختراق البيانات الحساسة, كما تشمل الهجمات السيبرانية الترويج للأيديولوجيات الإرهابية من خلال نشر أفكار متطرفة، تجنيد الأفراد، أو إلحاق أضرار اقتصادية عبر استهداف الأسواق المالية، سرقة الأموال، أو التجسس وسرقة المعلومات لاستخدامها في عمليات إرهابية مستقبلية, ومن الأمثلة على هذه الهجمات، الهجمات السيبرانية التي نفذها تنظيم داعش، حيث حاول اختراق أنظمة حكومية لنشر دعايته المتطرفة عبر الإنترنت[٢٥].

٧- الدعاية المتطرفة والتجنيد الالكتروني: هو عملية استقطاب الأفراد وتجنيدهم في الجماعات الإرهابية أو المنظمات السياسية والعسكرية، ويتم ذلك عبر وسال التواصل الاجتماعي، مثل الألعاب الإلكترونية والمنتديات المختلفة، أو البريد الإلكتروني. يتم التأثير على الأفراد وإقناعهم بالانضمام إلى تلك الجهات من خلال الدعاية، التلاعب النفسي، تقديم مبالغ مالية مغرية، أو إقناعهم بأفكار وأيديولوجيات معينة. ويهدف التجنيد الإلكتروني إلى إيجاد مقاتلين جدد للجماعات الإرهابية، نشر أفكارهم المتطرفة، أو تنفيذ هجمات سيبرانية عبر مجنّديهم عن بُعد, ومن الأمثلة على التجنيد الإلكتروني ما قامت به جماعات داعش الإرهابية، حيث حاولت تجنيد الأفراد عبر تويتر، فيسبوك، أو تطبيقات المراسلة الأخرى[٢٦].أصبح الفضاء الإلكتروني منصة مركزية تستخدمها الجماعات المتطرفة لنشر خطاب الكراهية وترويج أيديولوجياتها العنيفة، مستفيدة من الانفتاح الرقمي وغياب الرقابة الفورية على المحتوى. إذ تعتمد هذه الجماعات على مواقع التواصل الاجتماعي، ومنتديات النقاش، وتطبيقات التراسل المشفر في بث رسائل موجّهة تستهدف فئات معينة من الشباب، مركّزة على استغلال الأزمات المجتمعية والسياسية بهدف خلق بيئة نفسية قابلة للتأثر بالدعاية المتطرفة, ولا يقتصر النشاط على نشر الخطاب التحريضي فحسب، بل يمتد ليشمل عمليات التجنيد المنهجي عبر مراحل تبدأ بجذب الأفراد من خلال المحتوى المتطرف، ثم الانتقال إلى تواصل مباشر سري يُدار غالبًا عبر منصات مؤمّنة وتطبيقات مشفّرة. وقد أثبتت الدراسات أن الجماعات الإرهابية باتت تعتمد بشكل متزايد على تقنيات متقدمة مثل الفيديوهات المعدّة مسبقًا، والرسوميات الموجهة، واستغلال الوسائط الرقمية لزيادة تأثير دعايتها وتوسيع قاعدة مستهدفيها[٢٧], كما تُظهر التجارب العربية أن الدعاية الرقمية تُعدّ اليوم أحد أخطر أشكال الإرهاب الإلكتروني، لأنها تسهّل انتشار الأفكار العنيفة على نطاق واسع، وتخلق شبكات افتراضية من المؤيدين، وتتيح للتنظيمات إمكانية استقطاب عناصر جديدة دون الحاجة إلى وجود ميداني مباشر[3]. ومن هنا، تؤكد الدراسات أهمية تطوير استراتيجيات وطنية لمواجهة هذا النوع من الإرهاب، تشمل مراقبة المحتوى الرقمي، وبناء برامج توعية تستهدف الفئات الأكثر عرضة للتطرف، وتعزيز التعاون بين الجهات الحكومية وشركات التكنولوجيا لمنع انتشار المحتوى المتطرف [٢٨].

المحور الثالث: التحديات المتعددة الابعاد للإرهاب الالكتروني

يشكّل الإرهاب الإلكتروني تحديًا متناميًا للدول والمؤسسات على مستوى العالم، نظرًا لتعدد أساليبه وارتفاع درجة تعقيد الهجمات الرقمية. ومن أبرز هذه التحديات حماية البنى التحتية الحيوية، بما في ذلك الكهرباء والمياه والاتصالات، والتي يمكن أن يؤدي تعطيلها إلى أضرار اقتصادية واجتماعية جسيمة[1],كما يفرض الإرهاب الإلكتروني تحديات أمنية وسياسية، إذ يستخدم كأداة للتأثير على القرارات الحكومية، وزعزعة الاستقرار الداخلي، وتوجيه الرأي العام, ويواجه القطاع الأمني تحديات تقنية وفنية متعلقة بالكشف المبكر عن الهجمات السيبرانية، ومواكبة أدوات الاختراق المتطورة، مثل البرمجيات الخبيثة، والهجمات المستمرة المتقدمة (APT)، وهجمات حجب الخدمة (DDoS).[3] كما يمثل البعد القانوني والتشريعي تحديًا إضافيًا، إذ تختلف القوانين الوطنية بشأن الجرائم الإلكترونية، ويستغل الإرهابيون هذه الفجوات القانونية لتعطيل الإجراءات الأمنية[٢٩], إضافة إلى ذلك، يشكل البعد البشري والاجتماعي تحديًا، حيث يصعب أحيانًا توعية المستخدمين وتدريبهم على الوقاية من الهجمات، خاصة في المؤسسات الكبيرة التي تضم آلاف الموظفين، مما يزيد من احتمالات التسريب أو الانتهاك[5]. ومن هنا تبرز الحاجة إلى استراتيجيات شاملة تشمل تطوير البنية التحتية الأمنية الرقمية، وتحسين قدرات المراقبة والاستجابة، وتعزيز التعاون الدولي لمكافحة الإرهاب الإلكتروني بشكل فعال. [٣٠].

تزداد خطورة الإرهاب الإلكتروني يومًا بعد يوم على الأفراد والشركات والدول التي تعتمد بشكل كبير على الفضاء الإلكتروني، وهو المجال الذي يُستغل لشن هجمات ذات طابع إرهابي. ويمكن تقسيم التحديات التي يفرضها إلى ثلاث مجموعات رئيسية:

- **التحديات التقنية:** يطرح الإرهاب الإلكتروني العديد من التحديات التقنية التي تتطلب استجابة متطورة وفعالة، وتنبع هذه التحديات من الطبيعة الديناميكية للإنترنت، حيث إن الأجهزة والبرامج تتطور باستمرار، مما يزيد من صعوبة مواجهة التهديدات الإلكترونية. وفيما يلي أبرز هذه التحديات: [٣١].تطور أساليب الهجوم: أصبحت الهجمات الإلكترونية أكثر تعقيدًا نتيجة لاستخدام تقنيات متطورة مثل الذكاء الاصطناعي. كما أن تعدد الوسائِل الهجومية، مثل البرمجيات الخبيثة، وهجمات الحرمان من الخدمة (DDoS)، والتصيد الاحتيالي (Phishing)، زاد من صعوبة التصدي لها إخفاء الهوية: يستخدم الإرهابيون تقنيات متقدمة مثل الشبكات الافتراضية الخاصة (VPNs) وبروتوكولات التوجيه المشفر لإخفاء هوياتهم. بالإضافة إلى ذلك، أدى انتشار العملات الرقمية إلى زيادة صعوبة تتبع مصادر تمويل الأنشطة الإرهابية.استغلال الثغرات الأمنية: يعتمد الإرهابيون على استغلال الثغرات الأمنية غير المكتشفة أو التي لم يتم تصحيحها بعد لشن هجماتهم. كما أن ضعف أنظمة الحماية أو عدم تحديثها بانتظام يجعلها عرضة للاختراق.

١-**التحديات القانونية:** عتبر الجانب القانوني من أبرز التحديات التي تواجه مكافحة الإرهاب الإلكتروني، إذ إن الجرائم الرقمية غالبًا ما تتجاوز الحدود الوطنية، مما يعقد مهمة تطبيق القوانين المحلية والدولية, وتعاني العديد من الدول من ثغرات تشريعية نتيجة قدم القوانين أو عدم مواكبتها للتطورات التقنية، ما يتيح للمجرمين استغلال هذه الفجوات في تنفيذ هجماتهم, كما يشكّل تفاوت القوانين الدولية تحديًا آخر، إذ تختلف العقوبات ودرجة تجريم الجرائم الإلكترونية بين دولة وأخرى، مما يعيق التعاون القضائي وتبادل المعلومات بين الدول, ومن التحديات الأخرى صعوبة تحديد الجهة المنفذة للجرائم الرقمية، خاصة عند استخدام تقنيات إخفاء الهوية أو الشبكات المجهولة، ما يجعل تتبع المهاجمين وإحالتهم للعدالة أمراً معقدا[٣٢].ولهذا، توصي الدراسات بضرورة وضع إطار تشريعي موحد على المستوى الإقليمي والدولي، يشمل تعريفات دقيقة للجرائم الإلكترونية، وآليات تعاون قضائي فعّالة، وتعزيز قدرات الدول على التحقيق الرقمي والتحليل الجنائي للبيانات، بما يضمن حماية الأمن الوطني دون المساس بحقوق الأفراد[٣٣].

- **التحديات الأمنية:** إضافةً إلى التحديات التقنية والقانونية، فإن الإرهاب الإلكتروني يفرض تحديات أمنية كبيرة على الدولة، وذلك بسبب طبيعته المتطورة وقدرته على التسبب في أضرار جسيمة.تشكّل التحديات الأمنية أحد أبرز العقبات التي تواجه الدول والمؤسسات في مكافحة الإرهاب الإلكتروني، نظرًا لتطور أساليب الهجوم وارتفاع درجة تعقيدها. وتشمل هذه التحديات صعوبة حماية الأنظمة الحيوية والمعلومات الحساسة، مثل البنى التحتية للطاقة والمواصلات والاتصالات، والتي قد تؤدي أي هجمة ضدها إلى أضرار جسيمة على المستوى الوطني, كما تتجلى التحديات الأمنية في صعوبة رصد الهجمات المبكرة وكشف مصدرها، إذ يستخدم المهاجمون تقنيات متطورة مثل إخفاء الهوية، واستخدام الشبكات المجهولة، واستغلال الثغرات الأمنية في الأنظمة القديمة والجديدة[2]. ويزيد من تعقيد الوضع تعدد الجهات المستهدفة، حيث تشمل الهجمات المؤسسات الحكومية، والمنظمات الخاصة، والبنية التحتية الاستراتيجية، ما يفرض على أجهزة الأمن تطوير استراتيجيات متكاملة للتصدي لهذه المخاطر[٣٤], وتتطلب مواجهة هذه التحديات الأمنية تعزيز قدرات الاستجابة الفورية للحوادث السيبرانية، وتطوير برامج التدريب المستمر للعاملين في المؤسسات الحكومية والخاصة، وبناء أنظمة مراقبة وتحليل متقدمة للكشف عن التهديدات المحتملة قبل وقوعها[4]. كما يشدد الباحثون على أهمية التعاون الدولي والإقليمي لتبادل المعلومات والخبرات، خصوصًا عند التعامل مع هجمات إرهابية تتجاوز الحدود الوطنية[٣٥].وفيما يلي أبرز التحديات الأمنية: [٣٦]تهديد البنية التحتية: تستهدف الهجمات الإرهابية الإلكترونية مصادر توليد الطاقة، أو محطات تصفية المياه، أو شبكات الاتصالات، أو أنظمة النقل. وتؤدي هذه الهجمات إلى تعطيل الخدمات الأساسية، مما قد يترتب عليه تأثيرات كارثية، إضافةً إلى التسبب في خسائر اقتصادية كبيرة.تهديد الأمن القومي: يمكن للإرهابيين سرقة البيانات الحساسة المتعلقة بالأمن القومي أو الاستخبارات، أو استخدام التجسس الإلكتروني لجمع المعلومات الاستخباراتية، مما يعرض الأمن القومي لخطر جسيم ويجعل الدولة مكشوفة أمام أعدائها.استغلال الثغرات الأمنية: يستغل الإرهابيون الثغرات الأمنية غير المكتشفة، إضافةً إلى ضعف الوعي الأمني لدى الأفراد أو المنظمات بشأن أفضل ممارسات الأمن السيبراني، لشن هجمات معقدة تعتمد على الذكاء الاصطناعي أو تنفيذ هجمات متعددة ومتزامنة بهدف تعطيل الاستجابة الأمنية. كما أن ضعف التنسيق بين الجهات الأمنية المختلفة لمواجهة هذه الهجمات يزيد من صعوبة الاستجابة السريعة والفعالة للحد من تأثيرها.

المحور الرابع: مخاطر الارهاب الالكتروني

يشكّل الإرهاب الإلكتروني تهديدًا متعدد الأبعاد للدول والمجتمعات، إذ يمتد تأثيره ليشمل الأمن الوطني، الاقتصاد، المجتمع، والبنية التحتية الرقمية ومن أبرز المخاطر الاقتصادية الخسائر الكبيرة التي قد تنتج عن تعطيل المؤسسات الحكومية والشركات الخاصة، واستهداف الأنظمة المصرفية، والهجمات على البنى التحتية الحيوية, كما يشكل الإرهاب الإلكتروني خطرًا على الأمن الاجتماعي والنفسي للأفراد، إذ يمكن للهجمات الإلكترونية مثل الابتزاز الرقمي، ونشر خطاب الكراهية والدعاية المتطرفة، أن تزرع الخوف والاضطراب في المجتمع ويترتب على ذلك تأثيرات سياسية وأمنية، حيث تستخدم الجماعات الإرهابية هذه الهجمات للتأثير على القرارات الحكومية، وزعزعة الثقة بالمؤسسات، وإحداث حالة من عدم الاستقرار.[٣٧] إضافة إلى ذلك، يمثل الإرهاب الإلكتروني تهديدًا للبنية التحتية الرقمية، إذ يمكن للفيروسات والبرمجيات الخبيثة، والهجمات المتقدمة المستمرة (APT)، أن تتسبب في اختراق الشبكات، وسرقة المعلومات، وتعطيل الخدمات الحيوية ولهذا فإن مواجهة هذه المخاطر يتطلب وضع استراتيجيات شاملة للأمن السيبراني، تشمل تعزيز الحماية التقنية، تدريب الكوادر، تطوير القوانين والتشريعات، والتعاون الدولي لمكافحة الجرائم الإلكترونية. [٣٨] يفرض الإرهاب الإلكتروني مخاطر متعددة على الاقتصاد والمجتمع والسياسة، ولذلك فهو يشكل تهديدًا للأمن القومي واستقرار الدولة. ومن بين هذه المخاطر نذكر:

- **المخاطر الاقتصادية:** يشكل الإرهاب الإلكتروني تهديدًا كبيرًا للاقتصاد، إذ إن الهجمات على محطات الطاقة، أو المؤسسات المالية، أو شبكات الاتصال، أو أنظمة النقل، يمكن أن تؤدي إلى خسائر اقتصادية فادحة ويعد تهديدًا خطيرًا للاقتصادات الحديثة، حيث قد يتسبب في عدة أزمات اقتصادية، منها: [٣٩].استهداف المؤسسات المالية: إن استهداف المؤسسات المالية يؤدي إلى مشاكل كبيرة في الاقتصادين المحلي والعالمي، إذ قد يتسبب في خسائر مالية ضخمة، وزعزعة الثقة بالمؤسسات المالية، وتعطيل الخدمات الأساسية. ومن الأمثلة على ذلك هجوم SWIFT على بنك بنغلاديش المركزي عام ٢٠١٦، حيث نجح المهاجمون في سرقة ٨١ مليون دولار قبل اكتشاف الاختراق، مما أدى إلى زعزعة الثقة في نظام SWIFT وكشف نقاط ضعف في الأمن السيبراني للبنوك كما يمكن أن تؤدي الهجمات الإلكترونية إلى تعطيل أنظمة الدفع والتحويلات المالية، مما يعرقل الأنشطة الاقتصادية.خسائر الشركات: تتسبب الهجمات الإلكترونية في خسائر كبيرة للشركات على مستويات متعددة، سواء كانت مالية أو تشغيلية أومتعلقة بالسمعة. وقد تكون هذه الخسائر مباشرة، مثل سرقة الأموال، كما حدث في هجوم Carbanak الذي استهدف البنوك وسرق مليار دولار أو غير مباشرة، مثل فقدان الفرص التجارية وضعف القدرة التنافسية، خاصة إذا أدت الهجمات إلى تسريب معلومات سرية. كذلك، قد تؤدي الهجمات إلى ارتفاع أقساط التأمين السيبراني نتيجة زيادة المخاطر، كما حدث في اختراق Equifax الذي تسبب في تسريب بيانات ١٤٣ مليون عميل، وبلغت تكاليف التعافي منه أكثر من ١.٤ مليار دولار[٤٠].تعطيل الأسواق: تؤدي الهجمات الإرهابية الإلكترونية على المؤسسات المالية والشركات، كما أشرنا سابقًا، إلى تعطيل الأسواق على المستويين المحلي والعالمي، لما لها من تأثير على البنية التحتية وفقدان الثقة بالنظام المالي أو بالمؤسسات المالية. فاستهداف أنظمة الدفع الإلكتروني والتحويلات المالية يؤدي إلى تأخير المعاملات وتعطيل تدفق الأموال، مما يخلق اضطرابات اقتصادية كبيرة.

١- **المخاطر الاجتماعية:** يؤدي الإرهاب الإلكتروني إلى مخاطر اجتماعية، نظرًا لتأثيره المباشر على المجتمع، وقد يشكل تهديدًا للسلم الاجتماعي بعدة طرق:

-نشر الذعر بين الناس: يتسبب الإرهاب الإلكتروني في نشر الذعر بأساليب متعددة، إذ يعتمد على الهجمات الرقمية التي تستهدف الأفراد[٤١]، والمؤسسات، والبنية التحتية للدول. فالهجمات على البنية التحتية والخدمات الأساسية، والمؤسسات المالية، إضافة إلى عمليات القرصنة وتسريب المعلومات، تؤدي إلى فقدان الثقة بالنظام المالي، وانتشار الذعر، وإثارة الفوضى والخوف بين المواطنين. كما أن السيطرة على وسائل الإعلام والمنصات الرقمية، واختراق الوسائل الإعلامية الرسمية، وبث الأخبار الزائفة عن هجمات إرهابية أو كوارث محتملة، بالإضافة إلى نشر مشاهد مرعبة أو تهديدات مباشرة عبر الإنترنت، يسهم في زيادة حالة الخوف والذعر بين الناس. كذلك، يؤدي استخدام مواقع التواصل الاجتماعي والمنصات الإلكترونية لنشر معلومات مضللة إلى ردود فعل غير محسوبة، مثل تدافع الناس أو شراء السلع بكميات مفرطة نتيجة الخوف من الأزمات المحتملة. من ناحية أخرى، فإن الهجمات على الأمن الشخصي للأفراد، مثل الاختراق الإلكتروني والتجسس، تُستخدم أحيانًا لابتزاز الشخصيات العامة أو المواطنين العاديين[٤٢]، مما يولد شعورًا بالخوف من المراقبة المستمرة. كما أن تهديد الأفراد بنشر معلومات خاصة أو استغلال بياناتهم لأغراض إرهابية يزيد من القلق ويعزز الشعور بعدم الأمان.تجنيد الشباب: أصبح تجنيد الإرهابيين عبر الإنترنت من أخطر الوسائل المتبعة لاستقطاب الأفراد والتأثير عليهم فكريًا ونفسيًا، إذ يعتمدون على استراتيجيات متطورة تستخدم التكنولوجيا ووسائل التواصل الاجتماعي للوصول إلى الفئات المستهدفة. يبحث الإرهابيون عن أفراد يواجهون أزمات هوية أو يبحثون عن معنى لحياتهم، وكذلك عن أولئك الذين يعانون من الفقر والبطالة، حيث يغروهم بمبالغ مالية لاستقطابهم. كما يستهدفون الأفراد ذوي النزعة الدينية القوية، الذين يمكن التلاعب بمعتقداتهم بسهولة. كما يستخدم الإرهابيون وسائل متعددة لتحقيق أهدافهم، من بينها منصات التواصل الاجتماعي، وغرف الدردشة، والمواقع المظلمة. ويتم جذب الأفراد من خلال نشر الدعاية والأيديولوجية المتطرفة، بالإضافة إلى التلاعب النفسي بالمستهدفين عبر التقرب العاطفي، وغسل الدماغ التدريجي، أو إثارة مشاعر الذنب والغضب، أو تقديم الإغراءات والوعود الكاذبة[٤٣].ترويج الفكر المتطرف: إنَّ الإنترنت بيئة خصبة لترويج الفكر المتطرف، إذ يعتمد الإرهابيون على وسائل متنوعة في الفضاء الإلكتروني نظرًا لقدرته على الوصول إلى جماهير واسعة. ومن الأساليب المتبعة في ذلك استغلال مواقع التواصل الاجتماعي والتجنيد عبر الألعاب الإلكترونية، حيث يستهدفون الفئات ضعيفة النفسية أو التي تعاني من العزلة. ويتم ذلك عن طريق التلاعب بالعاطفة أو إثارة الشكوك لاستقطاب الشباب.

٢-**المخاطر السياسية:** ان السياسة المحلية والعالمية ليست بمنئى عن خطر الارهاب الالكتروني اذ يشكل تهديدا للاستقرار السياسي للدول والمجتمعات حيث يستهدف البنى التحتي ويضعف الثقة في المؤسسات ويزيد من حجم الصراعات الداخلية والدولية، وفيما يلي ابرز المخاطر السياسية:

-**استهداف الحكومات وتقويض الأمن القومي:** كما أشرنا سابقًا، فإن الإرهاب الإلكتروني يمكن أن يستهدف البنى التحتية للدولة، مما يسبب شللاً في مؤسساتها ويظهر عجز الحكومة عن حماية مواطنيها. بالإضافة إلى ذلك، فإن عدم القدرة على الرد أو تحديد المصدر بدقة يُضعف من هيبة الدولة. علاوة على ذلك، تسهم حملات التضليل ونشر الأخبار الكاذبة، مثل (الشائعات حول انهيار النظام المصرفي)، في زيادة الاستقطاب السياسي وتعقيد عملية الحكم. كما يستغل الإرهاب الإلكتروني المنصات المشفّرة لنشر أيديولوجيات متطرفة وتجنيد أفراد لتنفيذ هجمات إرهابية ميدانية.**زعزعة الاستقرار:** إنَّ تسريب البيانات، واختراق مؤسسات حكومية، وكشف معلومات سرية يُلحق الضرر بسمعة الدولة ويُضعف ثقة المواطن بحكومته، وهي أمور من شأنها زعزعة الاستقرار الداخلي للدولة. كما أنَّ تزييف الانتخابات عبر اختراق أنظمة التصويت الإلكتروني أو نشر معلومات مضللة لتشويه العملية الديمقراطية، كما حدث في الانتخابات الأمريكية عام ٢٠١٦، كلها عوامل تُساهم في زعزعة الثقة بالمؤسسات الحكومية.**التأثير على العلاقات الدولية:** إنَّ هجمات الإرهاب الإلكتروني تزيد من التوتر بين الدول، إذ تتصاعد الاتهامات المتبادلة، مثل اتهام روسيا بالتدخل في الانتخابات الغربية أو اتهام الصين بأعمال تجسس إلكتروني، مما يُفاقم خطر المواجهة المباشرة أو العقوبات. كما أن الهجمات الإلكترونية تُسبب خسائر كبيرة للاقتصاد الدولي وقد تؤدي إلى انهيار العملات الرقمية.

المحور الخامس: استراتيجية الحد من الارهاب الالكتروني

يزداد خطر الإرهاب الإلكتروني بزيادة الحاجة إلى التكنولوجيا ودخولها في جميع مجالات الحياة، حتى أصبحت بعض الدول تعتمد اعتمادًا شبه كامل على التكنولوجيا في تقديم الخدمات للمواطنين وتشغيل البنية التحتية وعليه يجب مواجهة الإرهاب الإلكتروني والحد من تأثيراته على المجتمع الدولي.

ومن اجل الحد من ظاهرة الإرهاب الإلكتروني لابد من تضافر الجهود واتباع سياسات عدة ومن بين هذه الإجراءات نذكر:

١- **وضع وتعزيز الاطر القانونية والتشريعية:** ان الاتفاقيات الدولية مثل اتفاقية بودابست للجرائم الالكترونية عام (٢٠٠١) والتي توفر اطارا لتنسيق القوانين الوطنية وتعزيز التعاون في التحقيقات وتكمن اهمية هذه الاتفاقية بفعاليتها على اقرارها اجراءات عملية. اذ ان المنظمات الدولية كالامم المتحدة والانتربول والاتحاد الدولي للاتصالات طورت اتفاقيات دولية من شأنها مكافحة الجرائم الالكترونية اضافة الى ذلك تعزيز القوانين الوطنية لتجريم الارهاب الالكتروني وضمان توحيد التشريعات بين الدول.[٤٤]

٢- **تعزيز التعاون الامني والمعلوماتي:** ان التعاون الدولي في تبادل المعلومات الخاص بالجماعات الارهابية والتهديدات السيبرانية من شانه ان يحد من خطر هذه الجماعات كما له دور في كشفهم ومعرفتهم وتسهيل عملية القاء القبض عليهم في حال الامساك بيهم والتعرف عليهم كما ان انشاء مراكز مشتركة لمراقبة الانشطة الالكترونية المشبوهة يعمل كمنظومة انذار مبكر للهجمات الالكترونية ومن هذه المراكز مركز مكافحة الارهاب التابع للامم المتحدة (UNCCT).[٤٥].

٣- **التدريب وبناء القدرات:** على الدول ان تقوم بتدريب كوادر متخصصة وتنظيم ورش عمل لمساعدة الدول في رفع امكانيات كوادرها وتطوير انظمتها الامنية السيبرانية اضافة الى تقديم الدعم الفني للدول التي لا تمتلك القدرة ولا الامكانيات الكافية لمكافحة الجرائم الالكترونية.

٤- **تعزيز الامن السيبراني وحماية البنية التحتية:** على الحكومات ان تقوم بتطوير معايير امنية خاصة لحماية البنية التحتية الالكترونية الحساسة مثل شبكات الطاقة والاتصالات والخدمات المصرفية من الهجمات الارهابية الالكترونية ويتم هذا عن طريق دعم الابحاث في مجال الامن السيبراني وتشجيع الابتكارات في تقنيات الحماية، اذ تقوم بعض الشركات بتعيين هاكرية مهمتهم محاولة اختراق انظمتهم الامنية السيبرانية بهدف ايجاد الثغرات الامنية ومحاولة اصلاحها[٤٦].

٥- **مكافحة تمويل الارهاب الالكتروني:** يتم ذلك من خلال مراقبة تدفق الاموال التي تستخدم لتمويل الهجمات السيبرانية والتعاون مع المؤسسات المالية لمنع استغلال العملات الرقمية في تمويل الانشطة الارهابية، حيث اصدر البنك الدولي مذكرة مناقشة مركزة حول موضوع مكافحة غسيل الاموال و ومحاربة تمويل الارهاب.

٦- **التوعية ونشر ثقافة الامن السيبراني:** على الحكومات ان تقوم باطلاق حملات توعوية عالمية لتعزيز الوعي بمخاطر الارهاب الالكتروني ورق الحماية منه كما يجب ان تقوم باشراك القطاع الخاص والمجتمع المدني في جهود مكافحة الارهاب الالكتروني .

٧- **المراقبة والاستخبارات الإلكترونية:** يساهم الذكاء الاصطناعي وتحليل البيانات الضخمة في رصد الأنشطة المشبوهة على الإنترنت، ويتم ذلك من خلال تتبع الاتصالات المشفرة عبر منصات التواصل الاجتماعي والمراسلة، بالإضافة إلى تحليل أنماط الهجمات الإلكترونية السابقة للتنبؤ بالتهديدات المستقبلية[٤٧].

٨- **تعزيز الحماية السيبرانية:** يتم تعزيز الحماية السيبرانية من خلال تطوير أنظمة كشف التسلل (IDS) والجدران النارية (Firewalls) لمنع الاختراقات، إضافةً إلى استخدام التشفير المتقدم لحماية المعلومات الحساسة من الاختراق، وتنفيذ سياسات وصول صارمة لمنع تسرب البيانات إلى الجهات الإرهابية.

٩- **مكافحة الدعاية والتجنيد الإلكتروني:** تلعب التكنولوجيا والأمن السيبراني دورًا فعالًا في تتبع وإزالة المحتوى الإرهابي عبر منصات التواصل الاجتماعي، كما تساهم في استخدام تقنيات الذكاء الاصطناعي لكشف الحسابات الوهمية والمحتوى التحريضي. بالإضافة إلى ذلك، تسهم في تعزيز الوعي الرقمي لحماية الأفراد من الاستقطاب والتجنيد الإلكتروني.

١٠- **تعطيل الشبكات والبنية التحتية الإرهابية:** تساعد التكنولوجيا في شن هجمات سيبرانية مضادة على منصات تمويل الإرهاب ووسائل تواصله، كما أن تطوير تقنيات تتبع المعاملات المالية المشبوهة على الإنترنت المظلم (Dark Web) يسهم في كشف مصادر تمويل الإرهابيين. ويتم ذلك باستخدام برامج اختراق متطورة لتعطيل خوادم الإرهابيين وشبكاتهم.

١١- **التعاون الدولي والتشريعات:** يعد تبادل المعلومات بين الدول أمرًا ضروريًا لتعقب التهديدات الإلكترونية الإرهابية، كما أن تطوير قوانين صارمة تُجرِّم الهجمات السيبرانية والدعاية الإرهابية يساعد في الحد من هذه الهجمات، ويعزز الأمن السيبراني للبنى التحتية الوطنية الحيوية ضد الأعمال التخريبية. [٤٨].

١٢- **الاستعداد والتدريب السيبراني:** يجب على الحكومات تنظيم تدريبات محاكاة للهجمات الإلكترونية بهدف تحديد نقاط الضعف، كما ينبغي تدريب فرق الأمن السيبراني على أحدث تقنيات مكافحة الإرهاب الإلكتروني، وتعزيز ثقافة الأمن السيبراني لدى المؤسسات والأفراد.

الخاتمة:

في ختام هذا البحث، يتضح جليًا أن الإرهاب الإلكتروني يمثل تحديًا استراتيجيًا حقيقيًا يهدد الأمن الوطني والدولي على حد سواء، ويستغل التطور التقني والتحولات الرقمية لتوسيع دائرة تأثيره, لقد أظهر التحليل أن أشكال الإرهاب الإلكتروني متعددة، بدءًا من اختراق الأنظمة الحكومية والعسكرية، وصولاً إلى استهداف البنى التحتية الحيوية، ونشر الفيروسات والبرمجيات الخبيثة، والابتزاز الإلكتروني، والتجسس الرقمي، وصولاً إلى التجنيد والدعاية المتطرفة عبر الإنترنت، ما يجعل هذه الظاهرة ذات أبعاد شمولية معقدة تتطلب معالجة متكاملة, كما أظهرت الدراسة أن التحديات التي يفرضها الإرهاب الإلكتروني ليست مقتصرة على الجانب التقني فحسب، بل تمتد لتشمل الجوانب القانونية، والأمنية، والبشرية، والسياسية، والاقتصادية، مما يزيد من صعوبة التصدي لهذه الظاهرة بفاعلية, وتشير المخاطر المصاحبة للإرهاب الإلكتروني إلى إمكانية تعطيل البنى التحتية الحيوية، وتهديد الاستقرار الاجتماعي والسياسي، وزعزعة الثقة في المؤسسات الرسمية، وتأثير مباشر على الاقتصاد الوطني, من هذا المنطلق، فإن مواجهة الإرهاب الإلكتروني لم تعد خيارًا بل ضرورة استراتيجية ملحة، تستدعي تبني سياسات شاملة ومتعددة الأبعاد، تجمع بين التطوير التقني، وتعزيز الأمن السيبراني، والتشريعات القانونية الفعّالة، وبناء القدرات البشرية، والتعاون الدولي، مع تبني استراتيجيات استباقية تتيح التنبؤ بالتهديدات والحد من آثارها المحتملة, إن إدراك خطورة هذه الظاهرة والتعامل معها بجدية علمية واستراتيجية عملية هو السبيل لضمان حماية المجتمع والدولة في عصر يتسم بالاعتماد المتزايد

التوصيات:

١. تعزيز البنية التحتية الرقمية في المؤسسات الحكومية والخاصة لتكون قادرة على مواجهة الهجمات الإلكترونية المحتملة.
٢. سن وتحديث التشريعات والقوانين المتعلقة بالجريمة الإلكترونية، بما يواكب تطور أدوات وأساليب الإرهاب الرقمي.
٣. رفع الوعي المجتمعي من خلال حملات توعوية وتثقيفية حول مخاطر الإرهاب الإلكتروني وطرق الوقاية منه.
٤. تشجيع التعاون الدولي وتبادل المعلومات والخبرات بين الدول في مجال الأمن السيبراني.
٥. دعم البحث العلمي والتقني في مجال مكافحة الإرهاب الإلكتروني وتطوير أدوات رصد وتحليل الهجمات الإلكترونية
٦. إنشاء مراكز وطنية متخصصة للاستجابة للحوادث السيبرانية,, تتولى رصد التهديدات الإلكترونية، والتعامل السريع مع الهجمات، وتنسيق الجهود بين المؤسسات الحكومية والخاصة.
٧. تأهيل وتدريب الكوادر الأمنية والتقنية بشكل مستمرمن خلال برامج تدريبية متقدمة تواكب التطور السريع في أدوات الاختراق، والذكاء الاصطناعي، وتحليل البيانات الضخمة.

٨. تعزيز الشراكة بين القطاعين العام والخاص لا سيما مع شركات التكنولوجيا ومزودي خدمات الإنترنت، بهدف حماية البنية التحتية الرقمية وتبادل المعلومات حول التهديدات السيبرانية.

٩. تطوير آليات رقابة على المحتوى الرقمي دون المساس بالحريات بما يحقق التوازن بين متطلبات الأمن وحماية حقوق الإنسان، خاصة فيما يتعلق بمكافحة الدعاية المتطرفة والتجنيد الإلكتروني.

١٠-مكافحة تمويل الإرهاب الإلكتروني من خلال تشديد الرقابة على المعاملات المالية الرقمية والعملات المشفرة، وتعزيز التعاون مع المؤسسات المالية الدولية.

١١-اعتماد استراتيجيات وطنية شاملة للأمن السيبراني تدمج الجوانب التقنية والقانونية والأمنية والتوعوية ضمن إطار استراتيجي موحد طويل الامد.

المصادر:

١. رفد عيادة الهاشمي، الإرهاب الالكتروني القانوني، ط١، دار المجد للطباعة والنشر، عمان، ٢٠١٩، ص٢٠.

٢. الاية (٤٠) ,سور البقرة, القران الكريم.

٣. –الاية (١١٦) , سورة الاعراف , القران الكريم.

٤. –سلوى احمد ميدان, الارهاب والجهود الدولية لمكافحته, مجلة كلية القانون والعلوم السياسية,جامعة كركوك,عدد٥,٢٠١٦,ص٥٣–٥٤..

٥. –محمد عبد المحسن سعدون, مفهوم الارهاب وتجريمه في التشريعات الجنائية الوطنية الدولية, مركز دراسات الكوفة ,جامعة الكوفة ,عدد ٧,٢٠٠٨, ص١٣٩.

٦. – عبد الوهاب الكيالي, الموسوعة السياسية الجزء السابع, المؤسسة العربية للدراسات والنشر, بيروت, ١٩٩٤, ص١٥٣.

٧. – وضاح زيتون , المعجم السياسي , دار اسامة المشرق الثقافي, الاردن,٢٠٠٦, ص٢١ .

٨. –المادة الاولى, قانون مكافحة الارهاب العراقي رقم ١٣, ٢٠٠٥, .

٩. – المادة الاولى, قانون مكافحة الارهاب الامريكي, ١٩٥٨. ينظر ايضا عبد القادر نقوزي , المفهوم القانوني لجرائم الارهاب الداخلي والدولي,منشورات الحلبي الحقوقية, بيروت ,٢٠٠٨, ص٣٢.

١٠. – عبد الرحمن السند , الاحكام الفقهية للتعاملات الالكترونية, دار الرواق, الرياض,ص٩.

١١. – محمد عبدالله المنشاوي، جرائم الإنترنت من منظور شرعي وقانوني. مطبعة جامعة الملك فهد الرياض , ١٤٢٣,ص

١٢. – عادل عبد الصادق ,الإرهاب الإلكتروني نمط جديد وتحديات مختلفة، المركز العربي للأبحاث الفضاء الإلكتروني, القاهرة, ٢٠١٣,ص٦٢.

١٣. – محمد عبد الكريم رعد, الأمن السيبراني ومهددات الفضاء الرقمي, دار المسيرة، عمّان, ٢٠٢٠، ص ٥٥.

١٤. – **حيدر حسن رضا, الحرب السيبرانية في الاستراتيجيات العسكرية الحديثة ,المركز العربي، ٢٠١٩، بيروت ص ١١٢.**

١٥. – **Singer, P. W., and Allan Friedman. Cybersecurity and Cyberwar: What Everyone Needs to Know .New York: Oxford University Press, 2014, 65**

١٦. – أحمد حسن الطائي. الأمن السيبراني ومخاطر الهجمات على الأنظمة الصناعية, المركز العربي للأبحاث، بيروت ٢٠٢٠، ص ١٢٨.

١٧. –New Zetter, Kim. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon .York: Crown Publishers, 2014, 93

١٨. – ندى عبد الله جاسم, البرمجيات الخبيثة وتأثيرها على أمن المعلومات ,: مكتبة المعرفة، ٢٠٢١, بغداد، ص ٧٧.

١٩. – New Singer, P. W., and Allan Friedman. Cybersecurity and Cyberwar: What Everyone Needs to Know .York: Oxford University Press, 2014, 54

٢٠. – فراس محمود العلي, الهجمات الإلكترونية, المخاطر وأساليب المواجهة , ,دار الثقافة، ٢٠٢٠، عمان ,ص ٩١.

٢١. – أميرة خالد, الجريمة الإلكترونية وأساليب الابتزاز عبر الفضاء الرقمي, دار الفكر الجامعي، ٢٠٢٠، القاهرة ,ص ٦٤.

٢٢. – سيف الدين العاني, الابتزاز الرقمي: مخاطره وسبل مكافحته , دار الحكمة، ٢٠٢١, بغداد، ص ٨٨.

٢٣. – ، محمود كامل العطار, الحرب الإلكترونية, المفاهيم والتهديدات ,: مركز الدراسات الاستراتيجية، ٢٠٢٠ ,بيروت، ص ١١٩.

٢٤. – Clarke, Richard A., and Robert K. Knake. Cyber War: The Next Threat to National Security and What to Do About It (New York: Ecco, 2010), 172.

٢٥. – ابراهيم محمد بن حمودالزنداني وبكيل احمد الزنداني، الجرائم السيبرانية ودور السياسة الجنائية في مواجهتها والحد منها وأثرها على الأمن الدولي، دار الكتب اليمنية للطباعة والنشر، والتوزيع، صنعاء، ٢٠٢١، ص٢٤٤.

٢٦. – غادة ممدوح امين، استخدام الشبكات االاجتماعية في التجنيد الالكتروني الارهابي في ظل جائحة كورونا: تأثر الشخص الثالث مدخلا نظريا، المجلة العلمية لبحوث الاذاعة والتلفزيون، العدد الرابع والعشرون، الجزء الثاني، جامعة القاهرة، ٢٠٢٢، ص٢٩٠.

٢٧. – سارة لطيف كريم, الدعاية الرقمية والتنظيمات الإرهابية , مركز الدراسات الأمنية ، ٢٠٢١، بيروت, ص ١٠٣.

٢٨. – حسين عبد الهادي النجار, الحرب الإعلامية للجماعات المتطرفة في العصر الرقمي, دار الثقافة، ٢٠٢٠،عمّان, ص ١١٨.

٢٩. – أحمد حسن الطائي, الأمن السيبراني ومخاطر الهجمات على الأنظمة الصناعية, المركز العربي للأبحاث، ٢٠٢٠، بيروت, ص ١٢٨.

٣٠. – مريم خالد الجبوري, خطاب الكراهية في الفضاء الرقمي: المخاطر وأساليب المواجهة (بغداد: دار الأفق الجديد، ٢٠٢١)، ص ٦٢.

٣١. – سيف الدين العاني, الابتزاز الرقمي: مخاطره وسبل مكافحته,دار الحكمة، ٢٠٢١ ,بغداد, ص ٩٢.

٣٢. – محمد عبد الكريم رعد, الأمن السيبراني ومهددات الفضاء الرقمي, دار المسيرة، ٢٠٢٠,عمّان, ص ٦١.

٣٣. – سامر العابد, حماية البنى التحتية الحيوية في عصر التهديدات السيبرانية , دار الفكر الجامعي، ٢٠٢١، القاهرة,ص ٤١.

٣٤. – فارس العمارات ومحمد الحمامصة، الامن السيبراني (المفهوم وتحديات العصر)، دار الخليج للنشر والتوزيع، عمان،٢٠٢٢، ص٥٧.

٣٥. – Hugh Brooks،Ravi Gupta , ترجمة عاصم سيد عبد الفتاح، وسائل التواصل الاجتماعي وتأثيرها على المجتمع، ط١، المجموعة العربية للتدريب والنشر، القاهرة، ٢٠١٧، ص٤٩.

٣٦. – ايمن عبد الله فكري، الجرائم المعلوماتية دراسة مقارنة في التشريعات العربية والأجنبية، ط١، المنهل، دبي، ٢٠١٤، ص٣٣٣.

٣٧. – منال البلقاسي، تأمين التهديدات السيبرانية تحت المجهر، ط١، العبيكان للنشر، الرياض، ٢٠٢٤، ص٢٤٩.

38. - https://alwatannews.net/life-style/article/786975/ .

39. - Clarke, R. A., & Knake, R. K. (2010). *Cyber War: The Next Threat to National Security and What to Do About It*. HarperCollins.

هوامش البحث

[١] – رفد عيادة الهاشمي، الإرهاب الالكتروني القانوني، ط١، دار المجد للطباعة والنشر، عمان، ٢٠١٩، ص٢٠.

[٢] – الاية (٤٠) ,سور البقرة, القران الكريم.

[٣] –الاية (١١٦) , سورة الاعراف , القران الكريم.

[٤] –سلوى احمد ميدان, الارهاب والجهود الدولية لمكافحته, مجلة كلية القانون والعلوم السياسية,جامعة كركوك,عدد٥,٢٠١٦,ص٥٣–٥٤..

[٥] –محمد عبد المحسن سعدون, مفهوم الارهاب وتجريمه في التشريعات الجنائية الوطنية الدولية, مركز دراسات الكوفة , ٧,٢٠٠٨, ص١٣٩.

[٦] – عبد الوهاب الكيالي, الموسوعة السياسية الجزء السابع, المؤسسة العربية للدراسات والنشر, بيروت, ١٩٩٤, ص١٥٣.

[٧] – وضاح زيتون , المعجم السياسي , دار اسامة المشرق الثقافي, الاردن,٢٠٠٦, ص٢١ .

[٨] –المادة الاولى, قانون مكافحة الارهاب العراقي رقم ١٣, ٢٠٠٥, .

[٩] – المادة الاولى, قانون مكافحة الارهاب الامريكي, ١٩٥٨. ينظر ايضا عبد القادر نقوزي , ,٢٠٠٨, ص٣٢.

[١٠] – عبد الرحمن السند , الاحكام الفقهية للتعاملات الالكترونية, دار الرواق, الرياض,ص٩.

[١١] – محمد عبدالله المنشاوي، جرائم الإنترنت من منظور شرعي وقانوني. مطبعة جامعة الملك فهد الرياض , ١٤٢٣,ص

[١٢] – عادل عبد الصادق ,الإرهاب الإلكتروني نمط جديد وتحديات مختلفة، المركز العربي للأبحاث الفضاء الإلكتروني, القاهرة, ٢٠١٣,ص٦٢.

[١٣] – محمد عبد الكريم رعد, الأمن السيبراني ومهددات الفضاء الرقمي, دار المسيرة، عمّان, ٢٠٢٠، ص ٥٥.

[١٤] – حيدر حسن رضا, الحرب السيبرانية في الاستراتيجيات العسكرية الحديثة ,المركز العربي، ٢٠١٩، بيروت ص ١١٢.

[١٥] - Singer, P. W., and Allan Friedman. Cybersecurity and Cyberwar: What Everyone Needs to Know New York: Oxford University Press, 2014, 65.

[١٦] – أحمد حسن الطائي. الأمن السيبراني ومخاطر الهجمات على الأنظمة الصناعية, المركز العربي للأبحاث، بيروت ٢٠٢٠، ص ١٢٨.

[17] -Zetter, Kim. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon New York: Crown Publishers, 2014, 93.

[١٨] – ندى عبد الله جاسم, البرمجيات الخبيثة وتأثيرها على أمن المعلومات ,: مكتبة المعرفة، ٢٠٢١, بغداد، ص ٧٧.

[19] -Singer, P. W., and Allan Friedman. Cybersecurity and Cyberwar: What Everyone Needs to Know New York: Oxford University Press, 2014, 54.

[٢٠] – فراس محمود العلي, الهجمات الإلكترونية, المخاطر وأساليب المواجهة , ,دار الثقافة، ٢٠٢٠، عمان ,ص ٩١.

[٢١] – أميرة خالد, الجريمة الإلكترونية وأساليب الابتزاز عبر الفضاء الرقمي, دار الفكر الجامعي، ٢٠٢٠، القاهرة ,ص ٦٤.

[٢٢] – سيف الدين العاني, الابتزاز الرقمي: مخاطره وسبل مكافحته , دار الحكمة، ٢٠٢١, بغداد، ص ٨٨.

[٢٣] – ، محمود كامل العطار, الحرب الإلكترونية, المفاهيم والتهديدات ,: مركز الدراسات الاستراتيجية، ٢٠٢٠ ,بيروت، ص ١١٩.

[24] -Clarke, Richard A., and Robert K. Knake. Cyber War: The Next Threat to National Security and What to Do About It (New York: Ecco, 2010), 172.

[٢٥] – ابراهيم محمد بن حمودالزنداني وبكيل احمد الزنداني، الجرائم السيبرانية ودور السياسة الجنائية في مواجهتها والحد منها وأثرها على الأمن الدولي، دار الكتب اليمنية للطباعة والنشر، والتوزيع، صنعاء، ٢٠٢١، ص٢٤٤.

[٢٦] – غادة ممدوح امين، استخدام الشبكات االاجتماعية في التجنيد الالكتروني الارهابي في ظل جائحة كورونا: تأثر الشخص الثالث مدخلا نظريا، المجلة العلمية لبحوث الاذاعة والتلفزيون، العدد الرابع والعشرون، الجزء الثاني، جامعة القاهرة، ٢٠٢٢، ص٢٩٠.

[٢٧] – سارة لطيف كريم, الدعاية الرقمية والتنظيمات الإرهابية , مركز الدراسات الأمنية ، ٢٠٢١، بيروت, ص ١٠٣.

[٢٨] – حسين عبد الهادي النجار, الحرب الإعلامية للجماعات المتطرفة في العصر الرقمي, دار الثقافة، ٢٠٢٠،عمّان, ص ١١٨.

[٢٩] – أحمد حسن الطائي, الأمن السيبراني ومخاطر الهجمات على الأنظمة الصناعية, المركز العربي للأبحاث، ٢٠٢٠، بيروت, ص ١٢٨.

[٣٠] – مريم خالد الجبوري, خطاب الكراهية في الفضاء الرقمي: المخاطر وأساليب المواجهة , دار الأفق الجديد، بغداد٢٠٢١, ص ٦٢.

[٣١] – عادل عبد الصادق، مصدر سبق ذكره ، ص١٩٤. ينظر ايضا ، سيف الدين العاني, الابتزاز الرقمي: ٢٠٢١ ,بغداد, ص ٩٢.

[٣٢] – محمد عبد الكريم رعد, الأمن السيبراني ومهددات الفضاء الرقمي, دار المسيرة، ٢٠٢٠,عمّان, ص ٦١.

[٣٣] – أحمد حسن الطائي، مصدر سبق ذكره, ص ١٣٣.

[٣٤] – سامر العابد, حماية البنى التحتية الحيوية في عصر التهديدات السيبرانية , دار الفكر الجامعي، ٢٠٢١، القاهرة,ص ٤١.

[٣٥] – مريم خالد الجبوري، مصدر سبق ذكره، ص ٦٤.

[٣٦] – فارس العمارات ومحمد الحمامصة، الامن السيبراني (المفهوم وتحديات العصر)، دار الخليج للنشر والتوزيع، عمان،٢٠٢٢، ص٥٧.

[٣٧] – سيف الدين العاني، مصدر سبق ذكره، ص ٨٨.

[٣٨] – أحمد حسن الطائي، مصدر سبق ذكره، ص ١٢٨.

[٣٩] – مريم خالد الجبوري، ص ٦٢. ينظر ايضا ، سامر العابد ,مصدر سبق ذكره، ص ٤١.

[٤٠] – سعد عبد القادر ماهر, مصدر سبق ذكره.، الظل الرقمي ص٧٥،

[٤١] – https://www.aljazeera.net/blogs/2019/3/22/.

[٤٢] – رفد عيادة الهاشمي, مصدر سبق ذكره, ص٥٧.

[٤٣] – Hugh Brooks،Ravi Gupta , ترجمة عاصم سيد عبد الفتاح، وسائل التواصل الاجتماعي ، ط١، ، ٢٠١٧، ص٤٩.

[٤٤] – ايمن عبد الله فكري، الجرائم المعلوماتية دراسة مقارنة في التشريعات العربية والأجنبية، ط١، المنهل، دبي، ٢٠١٤، ص٣٣٣.

٤٥ – منال البلقاسي، تأمين التهديدات السيبرانية تحت المجهر، ط١، العبيكان للنشر، الرياض، ٢٠٢٤، ص٢٤٩.

[٤٦] – https://alwatannews.net/life-style/article/786975/ .

[47] - Clarke, R. A., & Knake, R. K. (2010). Cyber War: The Next Threat to National Security and What to Do About It. HarperCollins.

[٤٨] – أحمد حسن الطائي.,مصدر سبق ذكره,ص ١٢٨.