Journal of Al-Farabi for Humanity Sciences Volume (8), Issue (6) December (2025)

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

الإرهاب الالكتروني في العصر الرقمي التحديات والمخاطر

م.م هدى عبد الحسين فياض[1]

جامعة النهرين-كلية العلوم السياسية

Cyberterrorism in the Digital Age: Challenges and Risks

الخلاصة:

يتناول هذا البحث ظاهرة الإرهاب الإلكتروني بوصفها أحد أخطر التحديات الأمنية التي تواجه العالم في العصر الرقمي. ومع تزايد الاعتماد على التكنولوجيا وشبكات الإنترنت، ظهرت جماعات وأفراد يستخدمون الفضاء السيبراني لشن هجمات تهدف إلى بث الرعب، وتعطيل البنى التحتية، وسرقة المعلومات، ونشر الأيديولوجيات المتطرفة. يناقش البحث أبرز أشكال الإرهاب الإلكتروني، مثل الهجمات على الأنظمة الحكومية، والتجنيد عبر الإنترنت، واستخدام العملات الرقمية في تمويل العمليات الإرهابية. كما يستعرض التحديات التي تواجه الحكومات في مواجهة هذا النوع من الإرهاب، وعلى رأسها ضعف التشريعات، والتطور السريع للتقنيات، وصعوبة تعقب المهاجمين. ويختتم البحث بتوصيات لتعزيز التعاون الدولي، وتحديث الأطر القانونية، وتطوير القدرات التقنية لمكافحة هذه الظاهرة المتنامية

الكلمات المفتاحية: الارهاب الالكتروني، الامن السيبراني، مكافحة الارهاب، التحديات الامنية.

Abstract:

This research addresses the phenomenon of cyber terrorism as one of the most serious security challenges in the digital age. With the increasing reliance on technology and the internet, various groups and individuals have emerged who exploit cyberspace to launch attacks aimed at spreading fear, disrupting infrastructure, stealing information, and promoting extremist ideologies. The study discusses the main forms of cyber terrorism, such as attacks on government systems, online recruitment, and the use of digital currencies to fund terrorist operations. It also explores the challenges governments face in combating this type of terrorism, including weak legislation, rapid technological advancements, and the difficulty of tracking perpetrators. The research concludes with recommendations to enhance international cooperation, update legal frameworks, and develop technical capabilities to counter this growing threat.

Keywords: Cyber terrorism, Cybersecurity, Counter-terrorism, Security challenges.

المقدمة

يعد الإرهاب الإلكتروني أحد اهم التحديات الأمنية والسياسية في العصر الرقمي، إذ يُعدّ امتدادًا جديدًا للتهديدات التقليدية، لكنه يتميز بقدرة عالية على الانتشار العابر للحدود فقد أتاح التطور السريع في تكنولوجيا المعلومات والاتصالات بيئة خصبة للجهات المتطرفة والتنظيمات الإرهابية لتوظيف الفضاء السيبراني كمنصة للتجنيد، ونشر الأيديولوجيا، وتخطيط العمليات، بل وتنفيذها أحيانًا دون الحاجة إلى الوجود المادي في ساحة المواجهة لم يعد الإرهاب الإلكتروني مجرّد اختراق أو تشويش تقني، بل أصبح سلاحًا جيوسياسيًا يُوظّف في إطار استراتيجيات الحرب الهجينة، ويؤثر في استقرار الدول، وتماسك المجتمعات، وأمن الأفراد. لذا، تستوجب دراسة هذا النمط من الإرهاب فهماً معمقًا لأبعاده التكنولوجية والقانونية والأمنية اذ إن من أكثر التحديات خطورة التي تواجهها الدول في عصر التكنولوجيا هي الهجمات الإرهابية, وفي هذا البحث سنوضح مفهوم الإرهاب الإلكتروني، والتحديات التي يفرضها، والمخاطر المترتبة عليه، وطرق مواجهته.

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 وهي 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؟

المبحث الأول مفهوم الارهاب الالكتروني وماهيته

أولًا: تعريف الإرهاب الإلكتروني

إن مفهوم الإرهاب، بصورة عامة، هو القيام بأعمال من شأنها إثارة الرعب بين الناس، وقد تختلف أسباب الإرهاب باختلاف الجهات المنفذة له، أما الإرهاب الإلكتروني فهو فعل عدواني يصدر عن دولة أو جماعة تجاه أخرى، ويعتمد على التكنولوجيا والوسائل الرقمية، مثل الأنترنت، والحواسيب، والشبكات، للقيام بأعمال تهدف إلى إثارة الرعب وتهديد بالأمن والسلم، أو تحقيق أهداف سياسية اودينية أو اقتصادية او اجتماعية عبر وسائل غير قانونية[٢].يختلف الإرهاب الإلكتروني عن الجرائم الإلكترونية؛ لأنه يهدف إلى تحقيق أهداف إرهابية واضحة، وليس مجرد تحقيق مكاسب مادية أو فردية, فالجرائم الإلكترونية هي نشاط إجرامي يستهدف جهاز حاسوب واحدًا أو شخصًا أو مؤسسة بهدف الحصول على مكاسب مادية أو منفعة شخصية, ورغم التشابه بين الإرهاب الإلكتروني والجرائم الإلكترونية في كونهما يتمان عبر التكنولوجيا والإنترنت، إلا أن هناك اختلافات جوهرية بينهما من حيث الأهداف، والأساليب، والجهات الفاعلة، والتأثير.

١- **من حيث الهدف:** يهدف الإرهاب الإلكتروني إلى إثارة الفوضى والرعب وتهديد الأمن القومي، وغالبًا ما يكون مدفوعًا بدوافع سياسية أو أيديولوجية, أما الجرائم الإلكترونية، فتهدف إلى تحقيق مكاسب مالية أو إلحاق أضرار شخصية، مثل السرقة أو الابتزاز أو الاحتيال[٣].

٢- **من حيث الجهات الفاعلة:** غالبا ما يكون الإرهاب الإلكتروني صادر من جماعات إرهابية أو دول معادية، وقد يكون جزءًا من هجوم منظم, أما الجريمة الإلكترونية فعادة ما تُرتكب من قبل أفراد أو عصابات إجرامية تحقق مكاسب مالية.

٣- **من حيث الأسلوب:** تتميز الهجمات الإرهابية الإلكترونية بتأثيرات مدمرة، مثل استهداف محطات توليد الطاقة أو المياه، أو الهجوم على البنية التحتية الحيوية، أو نشر الفيروسات الإلكترونية لتعطيل الأنظمة الحكومية, أما الجرائم الإلكترونية التي تعتمد على سرقة المعلومات الشخصية أو الاحتيال المالي، أو القرصنة، دون أن تكون لها دوافع إرهابية[٤].

٤- **من حيث التأثير:** يكون تأثير الإرهاب الإلكتروني واسع النطاق، اذ يهدد الأمن القومي، ويؤثر على المن الدولة والمجتمع, أما الجريمة الإلكترونية فيقتصر تأثيرها على الأفراد أو الشركات بشكل مباشر، دون أن تمثل تهديدًا للأمن القومي.

ثانيا: اشكال الارهاب الالكتروني

تعددت أشكال الإرهاب الإلكتروني، ومن أبرزها:

١- **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[٥].

٢- **التجنيد الإلكتروني:** 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[٦].

٣- **نشر الأيديولوجيات المتطرفة:** يُعَدّ الإنترنت فضاءً مناسبًا للجماعات الإرهابية، إذ يصعب تتبع أماكن وجودهم، وهو من أخطر أشكال الإرهاب الإلكتروني. ومن الأساليب المتبعة في نشر هذه الأفكار:

- وسائِل التواصل الاجتماعي[٧]: تُعتبر منصات التواصل الاجتماعي والألعاب الإلكترونية أدوات مناسبة لنشر محتوى مرئي ونصي بهدف تجنيد أفراد جدد أو نشر الأفكار المتطرفة. كما تُوظَّف الأخبار العاجلة، المظالم الاجتماعية، والصراعات الجيوسياسية لتأطير خطاباتهم كحل للأزمات. بالإضافة لى ذلك، توفر هذه المنصات إمكانية التواصل المباشر مع المستخدمين، كما تتيح إعادة نشر المحتوى المتطرف عن طريق المؤيدين، مما يساعد على انتشاره بشكل أوسع.
- المواقع الإلكترونية والمدونات: تقوم الجماعات الإرهابية بإنشاء مواقع إلكترونية لنشر مقالات وتفسيرات دينية مشوهة تدعم أفكارهم المتطرفة. كما تدير مدونات سرية تُستخدم كمنصات لنشر الأفكار المنحرفة عبر مقالات ومواد تثقيفية تستهدف الشباب.
- منصات الفيديو والبث المباشر: أصبحت خاصية البث المباشر في مواقع التواصل الاجتماعي من الأدوات التي سهّلت للجماعات الإرهابية نشر أفكارهم والتواصل مع الأفراد بشكل مباشر وفوري. كما أصبح بإمكانهم بث العمليات الإرهابية مباشرة أو إنتاج مقاطع فيديو احترافية.
- استخدام الشبكات المظلمة (Dark Web): أصبحت الشبكات المظلمة بيئة آمنة ومناسبة للجماعات الإرهابية لنشر الكتب والمناهج المتطرفة، شراء الأسلحة، أو بيع الممنوعات بطريقة آمنة وبعيدة عن الرقابة الأمنية[٨].

ثالثا: الادوات الارهاب الالكتروني

يعتمد الإرهاب الإلكتروني على عدة أدوات وتقنيات لشنّ هجمات إرهابية تهدف إلى التخريب، التجسس، نشر الذعر، أو تعطيل البنية التحتية الحيوية. ومن أبرز هذه الأدوات:

١-**الشبكات المظلمة:** هي جزء من الإنترنت ولا يمكن الوصول إليها عبر المتصفحات العادية، بل تتطلب متصفحات خاصة مثل متصفح تور (Tor)، حيث تتميز هذه المتصفحات بقدرتها على إخفاء هوية المستخدم عبر حجب عناوين IP الخاصة بهم. ولهذا، تُعَدّ الشبكات المظلمة بيئة مناسبة للأنشطة غير القانونية ودعم الإرهاب[٩]. لذا، تستغلّ الجماعات المتطرفة هذه الشبكات من أجل التنظيم، التجنيد، التواصل، والتمويل.

٢-**البرمجيات الخبيثة:** تستخدم الجماعات الإرهابية مجموعة من البرمجيات التي تستهدف البنية التحتية التكنولوجية بهدف تعطيلها. ومن أمثلة هذه البرمجيات: الفيروسات الإلكترونية بأنواعها، برامج الفدية، والتشفير[١٠]. ومن أشهر البرمجيات المستخدمة في هذا المجال: فيروس الدودة، أحصنة طروادة، وبرامج الفدية.

٣-**الهجمات السيبرانية:** هناك عدة أنواع من هذه الهجمات، وتختلف حسب الهدف منها:

- هجمات حجب الخدمة (DDoS): تهدف إلى إغراق الخوادم بحركة مرور زائدة لتعطيلها[١١].
- الهجمات التي تستهدف سرقة المعلومات الحساسة: مثل التصيّد الاحتيالي وسرقة البيانات.
- الهجمات التي تستهدف مزودي الخدمة: لاختراق أنظمة أكبر والتحكم بها.

٤-**الاختراق والتجسس:** يُعَدّ الاختراق والتجسس نشاطين مرتبطين بالإنترنت، لكنهما يختلفان في الأهداف والأساليب:الاختراق: هو عملية الوصول إلى أجهزة الكمبيوتر أو البيانات باستخدام تقنيات متقدمة لاستغلال الثغرات الأمنية[١٢]، وقد يكون لأغراض إيجابية (مثل الاختراق الأخلاقي لحماية الأنظمة) أو سلبية (مثل الاختراق لأغراض تخريبية أو تجسسية)اما التجسس: هو عملية جمع معلومات سرية أو حساسة دون إذن، سواء كانت عسكرية، أمنية، سياسية، أو اقتصادية[١٣]. يتم التجسس إما عن طريق الاختراق الإلكتروني أو بوسائل تقليدية أخرى. وبناءً على ذلك، يمكن القول إن الفرق بين الاختراق والتجسس يكمن في أن الاختراق يركز على الوصول إلى الأنظمة، وقد يكون لأغراض إيجابية أو سلبية، ويعتمد على التقنيات الإلكترونية. أما التجسس، فيركز على جمع المعلومات، وغالبًا ما يكون لأغراض سرية أو عدائية، ويمكن أن يكون إلكترونيًا أو تقليديًا. ومع ذلك، فإن الاختراق يمكن استخدامه كأداة للتجسس، لكن التجسس يشمل نطاقًا أوسع وقد يتم بوسائل غير إلكترونية. وفي كلتا الحالتين، يشكل كل من الاختراق والتجسس تهديدًا كبيرًا للأفراد، الشركات، والدول إذا استُخدما لأغراض ضارة.

المبحث الثاني التحديات والمخاطر التي يفرضها الارهاب الالكتروني

أولا: تحديات الأرهاب الاكتروني 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:

١- 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:

– 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[١٤].

– 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[١٥].

– 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[١٦].

٢- **التحديات القانونية**[١٧]: تواجه جهود مكافحة الإرهاب الإلكتروني العديد من العقبات القانونية التي تعيق التعاون الدولي والمحلي، حيث تنبع هذه التحديات من الطبيعة العابرة للحدود للإنترنت، إضافةً إلى التعقيدات القانونية والسياسية واختلاف الأنظمة التشريعية بين الدول. ومن أبرز هذه التحديات:

– عدم وجود إطار قانوني موحد: تختلف القوانين المتعلقة بالجرائمالإلكترونية من دولة إلى أخرى، مما يصعّب تنسيق الجهود الدولية لمكافحة الإرهاب الإلكتروني.

– التحديات المتعلقة بالسيادة الرقمية: بعض الدول تفرض قوانين صارمة بشأن البيانات والسيادة السيبرانية، مما قد يعيق تبادل المعلومات بين الحكومات بشأن التهديدات الإرهابية.

– التوازن بين الأمن والخصوصية: تثير القوانين المتعلقة بمكافحة الإرهاب الإلكتروني جدلًا حول التوازن بين تعزيز الأمن القومي وحماية خصوصية الأفراد، حيث يمكن أن تؤدي بعض الإجراءات الأمنية إلى انتهاك الحريات الشخصية.

٣- **التحديات الأمنية**[١٨]: إضافةً إلى التحديات التقنية والقانونية، فإن الإرهاب الإلكتروني يفرض تحديات أمنية كبيرة على الدولة، وذلك بسبب طبيعته المتطورة وقدرته على التسبب في أضرار جسيمة. وفيما يلي أبرز التحديات الأمنية:

– 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.

ثانيا: مخاطر الارهاب الاكترني:

يفرض الإرهاب الإلكتروني مخاطر متعددة على الاقتصاد والمجتمع والسياسة، ولذلك فهو يشكل تهديدًا للأمن القومي واستقرار الدولة. ومن بين هذه المخاطر نذكر:

١- **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[١٩]. ويعد تهديدًا خطيرًا للاقتصادات الحديثة، حيث قد يتسبب في عدة أزمات اقتصادية، منها:

– 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[٢٠]. 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 أو متعلقة بالسمعة. وقد تكون هذه الخسائر مباشرة، مثل سرقة الأموال، كما حدث في هجوم Carbanak الذي استهدف البنوك وسرق مليار دولار[٢١]، 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[٢٢].

– 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.

٢– **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[٢٣]، 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[٢٤]، 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[٢٥].

– 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.

٣– **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.

المبحث الثالث استراتيجية مكافحة الإرهاب 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:

اولا: دور المنظمات الدولية والتعاون بين الدول

ان دور المنظمات الدولية والتعاون الدولي ذو اهمية كبيرة في مواجهة الارهاب الالكتروني كون ان هذه التهديدات ذات طابع عابر للحدود ولهذا اصبح لزاما على الدول التعاون لايقاف خطر مثل هكذا تهديدات، ويمكن تلخيص دور المنظمات الدولية والتعاون الدولي في النقاط التالية:

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[٢٦]. 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.

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[٢٧]. 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).

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[٢٨].

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 .

وعليه فان التعاون الدولي الفعال بين الحكومات والمنظمات الدولية والشركات التقنية الكبرى ضروري للحد من مخاطر المتزايدة للارهاب الالكتروني وضمان استقرار الفضاء الرقمي العالمي

ثانيا: التكنولوجيا والامن السيبراني

بما أن الإرهاب الإلكتروني يعتمد على الإنترنت والأجهزة الإلكترونية لتنفيذ هجماته الإرهابية، فإن مواجهة هذه الهجمات تتطلب إجراءات إلكترونية أيضًا، خصوصًا في ظل تطور الذكاء الاصطناعي. فالتكنولوجيا والأمن السيبراني يلعبان دورًا حاسمًا في مواجهة الإرهاب الإلكتروني. فيما يلي بعض الأدوار الرئيسية: [٢٩].

١- 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.

٢- 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.

٣- 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.

٤- 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.

٥- 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.

٦- 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.

بناءً عليه، فإن التكنولوجيا والأمن السيبراني يشكلان خط الدفاع الأول ضد الإرهاب الإلكتروني من خلال المراقبة والحماية ومكافحة الدعاية وكذلك تعطيل الشبكات الإرهابية، وتعزيز التعاون الدولي ومع ذلك فإن التحدي يكمن في مواكبة تطور التقنيات التي يستخدمها الإرهابيون، مما يتطلب جهودًا مستمرة واستراتيجيات مبتكرة.

الخاتمة:

في خضم التطور التكنولوجي المتسارع الذي يشهده العالم اليوم، أصبح الإرهاب الإلكتروني واحدًا من أخطر التحديات التي تهدد أمن الأفراد والمجتمعات والدول. لقد بيّن هذا البحث كيف استطاع الإرهاب أن ينتقل من ميادين القتال التقليدية إلى الفضاء الرقمي، مستغلًا منصات الإنترنت وشبكات الاتصال الحديثة لشن هجمات معقدة ومتنوعة تستهدف البنى التحتية، والمعلومات، وحتى العقول. ومما لا شك فيه أن خطورة هذا النوع من الإرهاب تكمن في صعوبة تعقبه، وسرعة انتشاره، وتأثيره الواسع النطاق.ومن هنا، فإن مكافحة الإرهاب الإلكتروني لا تتطلب فقط تطورًا تقنيًا وأمنيًا، بل تحتاج أيضًا إلى وعي مجتمعي وتشريعات قانونية صارمة وتعاون دولي فعال. إن التصدي لهذا الخطر هو مسؤولية جماعية، تتطلب جهودًا متكاملة للحفاظ على أمن الفضاء الرقمي وضمان استخدامه في ما يخدم الإنسانية ويعزز السلام والاستقرار.

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

المصادر:

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

٢- ابراهيم محمد بن حمودالزنداني & بكيل احمد الزنداني، الجرائم السيبرانية ودور السياسة الجنائية في مواجهتها والحد منها وأثرها على الأمن الدولي، ط١، دار الكتب اليمنية للطباعة والنشر، والتوزيع، صنعاء، ٢٠٢١، ص٢٤٤.

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

٤ – ايهاب خليفة، الحرب السيبرانية الاستعداد لقيادة المعارك العسكرية في الميدان الخامس، ط١، العربي للنشر والتوزيع، ٢٠٢١، ص١٧٠.

٥ – بسيوني محمد الخولي، رؤية الإسلام للتأثير المبتكر للذكاء الاصطناعي (المُحْدَث) (الجزء الثاني) في أهم قطاعات الاقتصادات المتقدمة الصناعة . الزراعة . الغذاء . الدواء . الدفاع، الجزء الثاني، مثابة الابداع للطباعة والنشر،

٥ – رفد عيادة الهاشمي: الارهاب الالكتروني القانوني، ط١، دار امجد للطباعة والنشر، عمان، ٢٠١٩، ص٥٧.

٨ – عادل عبد الصادق، الارهاب الالكتروني القوة في العلاقات الالكترونية: نمط جديد وتحديات مختلفة، ط١، مركز الدراسات السياسية والاستراتيجية بالاهرام، القاهرة، ٢٠٠٩، ص١٩٤.

٩ – عبد العزيز اغراز، الشبكة المظلمة والارهاب، مقال منشور على الموقع الاكتروني،
https://www.imctc.org/ar/eLibrary/Articles/Pages/article20062022.aspx

١٠ – 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.

١١ – غادة نصار، الإرهاب والجريمة الالكترونية، ط١، دار النهل، دبي، ص٩١.

١٢ – فارس العمارات & محمد الحمامصة، الامن السيبراني (المفهوم وتحديات العصر)، ط١، دار الخليج للنشر والتوزيع،٢٠٢٢، ص٥٧.

١٣ – فاضل عباس صباح، تهديدات الارهاب السيبراني في عصر الذكاء الاصطناعي، جامعة كربلاء، ٢٠٢٤، مقال منشور.

١٤ – فراس عقيل الدويري، البيانات الضخمة ودورها في الحد من الجرائم الإلكترونية في ظل إستراتيجية الأمن السيبراني، ط١، دار الخليج للنشر والتوزيع، عمان، ص١٠٩.

١٥ – محمد كمال، الارهاب السيبراني..عندما يستخدم الارهابي الكيبورد بدلا من القنبلة، ط١، دار كليم للطباعة والنشر، ، ٢٠٢٢، ص١٥.

١٦ – محمد&علي حجازي، سيكولوجيا الارهاب، ط١، دار غيداء للنشر والتوزيع، عمان، ٢٠١٩، ص١٣٥.

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

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

1 - Riza Montasari, Cyberspace, Cyberterrorism and the International Security in the Fourth Industrial Revolution Threats, Assessment and Responses, 1st edition, Springer International Publishing, UK, p172.

٢ - John Knittel & Michael Soto, The Rosen Publishing group Inc, 1st edition, NY, 2000, p6-11.

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

٤ - Eamon Doyle, The Dark Web, Greenhaven Publishing LLc, 1st edition, NY, 2020, p109.

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

٦ - https://arabic.rt.com/news/774152

٧ - https://root-x.dev/blog/article/hide_hackers.

٨ - https://www.aljazeera.net/blogs/2019/3/22/.

٩ - Paulo Shakarian and others, Introduction to Cyber-Warfare A Multidisciplinary Approach, 1st edition, Elsevier Science, Amsterdam, 2013, p115.

هوامش البحث

[١] – جامعة النهرين–كلية العلوم السياسية–huda.abdeh@nahrainuniv.edu.iq

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

[٣] – محمد كمال، الارهاب السيبراني..عندما يستخدم الارهابي الكيبورد بدلا من القنبلة، ط١، دار كليم للطباعة والنشر،الرياض، ٢٠٢٢، ص١٥.

[٤] – فراس عقيل الدويري، البيانات الضخمة ودورها في الحد من الجرائم الإلكترونية في ظل إستراتيجية الأمن السيبراني، ط١، دار الخليج للنشر والتوزيع، عمان، ص١٠٩.

[٥] – ابراهيم محمد بن حمودالزنداني & بكيل احمد الزنداني، الجرائم السيبرانية ودور السياسة الجنائية في مواجهتها والحد منها وأثرها على الأمن الدولي، ط١، دار الكتب اليمنية للطباعة والنشر، والتوزيع، صنعاء، ٢٠٢١، ص٢٤٤.

[٦] – 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.

[٧] – غادة نصار، الإرهاب والجريمة الالكترونية، ط١، دار النهل، دبي، ص٩١.

[٨] – عبد العزيز اغراز، الشبكة المظلمة والارهاب، مقال منشور على الموقع الاكتروني،

[٩] - Eamon Doyle, The Dark Web, Greenhaven Publishing LLc, 1st edition, NY, 2020, p109.

[١٠] – محمد&علي حجازي، سيكولوجيا الارهاب، ط١، دار غيداء للنشر والتوزيع، عمان، ٢٠١٩، ص١٣٥.

[١١] – ايهاب خليفة، الحرب السيبرانية الاستعداد لقيادة المعارك العسكرية في الميدان الخامس، ط١، العربي للنشر والتوزيع، ، ٢٠٢١، ص١٧٠.

[١٢] – John Knittel & Michael Soto, The Rosen Publishing group Inc, 1st edition, NY, 2000, p6-11.

[١٣] - Paulo Shakarian and others, Introduction to Cyber-Warfare A Multidisciplinary Approach, 1st edition, Elsevier Science, Amsterdam, 2013, p115.

[١٤] – عادل عبد الصادق، الارهاب الالكتروني القوة في العلاقات الالكترونية: نمط جديد وتحديات مختلفة، ط١، مركز الدراسات السياسية والاستراتيجية بالاهرام، القاهرة، ٢٠٠٩، ص١٩٤.

[١٥] - https://root-x.dev/blog/article/hide_hackers.

[١٦] – بسيوني محمد الخولي، رؤية الإسلام للتأثير المبتكر للذكاء الاصطناعي (المُحْدَث) (الجزء الثاني) في أهم قطاعات الاقتصادات المتقدمة الصناعة . الزراعة . الغذاء . الدواء . الدفاع، الجزء الثاني، مثابة الابداع للطباعة والنشر،

[١٧] – Riza Montasari, Cyberspace, Cyberterrorism and the International Security in the Fourth Industrial Revolution Threats, Assessment and Responses, 1st edition, Springer International Publishing, UK, p172.

[١٨] – فارس العمارات & محمد الحمامصة، الامن السيبراني (المفهوم وتحديات العصر)، ط١، دار الخليج للنشر والتوزيع، عمان،٢٠٢٢، ص٥٧.

[١٩] – فاضل عباس صباح، تهديدات الارهاب السيبراني في عصر الذكاء الاصطناعي، جامعة كربلاء، ٢٠٢٤، مقال منشور.

[٢٠] – سعد عبد القادر ماهر، الظل الرقمي، دون نشر، ص١٣٣.

[٢١] – https://arabic.rt.com/news/774152

[٢٢] – سعد عبد القادر ماهر، الظل الرقمي، دون نشر، ص٧٥، مصدر سبق ذكره.

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

[٢٤] – رفد عيادة الهاشمي: الارهاب الالكتروني القانوني، ط١، دار امجد للطباعة والنشر، عمان، ٢٠١٩، ص٥٧.

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

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

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

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