Dirasat: Human and Social Sciences, Volume 53, No. 1, 2026, 7474

Deanship of Scientific Research

The Role of Governments in Countering Cyberterrorism is a "Model" for the Government of Iraq

Mukhalad Maher Dawood *

Department of Comparative Religions, College of Islamic Sciences, University of Baghdad, Baghdad, Iraq

Received: 12/4/2024
Revised: 19/7/2024
Accepted: 18/9/2024
Published online: 1/8/2025

* *Corresponding author:*
mukhaled.m@cois.uobaghdad.edu.iq

Citation: Dawood, M. M. (2025). The Role of Governments in Countering Cyberterrorism is a "Model" for the Government of Iraq . *Dirasat: Human and Social Sciences*, *53*(1), 7474. https://doi.org/10.35516/Hum.2025.7474

Abstract

Objectives: This study aims to provide a description of the role of governments in countering electronic terrorism operations across various fields, particularly in light of the current changes we are witnessing, including the growing phenomenon of the information revolution. This revolution has contributed to the emergence of various websites that play a key role in influencing individuals on a broad scale, creating a need to activate the role of information security to participate in informational or digital awareness processes.

Methods: The study adopted the descriptive analytical approach, one of the most important and widely used methods in scientific research. It is capable of accurately analyzing the problem or phenomenon under study and identifying the causes behind its occurrence.

Results: The study found that the significant technological transformations experienced worldwide have led to radical changes in the lives of peoples and societies, resulting in major effects and repercussions. Information and knowledge have become critical indicators and sources of power and security. However, the use of this technology and the internet has not been limited to positive outcomes; it has also led to serious negative consequences that have affected societies and states, including Iraq.

Conclusions: The introduction of the concept of cyberterrorism in writings on cybersecurity since the end of the twentieth century represents an important and early attempt to express the urgent need to expand the concept of international terrorism.

Keywords: Terrorism, cyberterrorism, cybersecurity, information revolution, information security.

دور الحكومات في مواجهة الإرهاب الإلكتروني حكومة العراق "أنموذجًا"

مخلد ماهر داود السعدي*

قسم الأديان المقارنة، كلية العلوم الإسلامية، جامعة بغداد، بغداد، العراق

ملخّص

الأهداف: تهدف هذه الدراسة إلى تقديم توصيف لدور الحكومات في مواجهة العمليات التي يلعبها الإرهاب الإلكتروني في مختلف الميادين، خاصة في ظل المتغيرات الراهنة التي نشهدها، وتنامي ظاهرة الثورة المعلوماتية، التي ساهمت في ظهور المواقع الإلكترونية المختلفة، التي أصبحت تلعب دورًا رئيسًا في التأثير في الأفراد ككل، ومنه خلق ضرورة لتفعيل لدور الأمن المعلوماتي، وذلك للمشاركة في عمليات التوعية المعلوماتية أو الرقمية.

المنهجية: اعتمدت الدراسة المنهج التحليلي الوصفي يعد هذا المنهج أحد اهم المناهج العلمية وأكثرها استخدامًا في البحث العلمي، فهو القادر على تحليل مشكلة أو ظاهرة البحث العلمي على نحو دقيق، وتعرُّف أسباب حدوثها.

النتائج: توصلت الدراسة إلى أن التحولات التكنولوجية الكبيرة التي عرفها العالم إلى إحداث تغيرات جذرية في حياة الشعوب والمجتمعات وخلفت آثارًا وانعكاسات كبرى. أصبحت المعلومات والمعرفة مظهرًا ومؤشرًا ومصدرًا هامًا للقوة والأمن، فاستخدام هذه التكنولوجيا وشبكة الشبكات العنكبوتية لم يقتصر فقط على جانب إيجابي بل له مظاهر خطيرة سلبية أثرت في المجتمعات والدول، ومن بينها العراق.

الخلاصة: إن دخول مفهوم الإرهاب الإلكتروني ضمن الكتابات التي سادت حول الأمن السيبراني Cyber Security منذ نهاية القرن العشرين، من المحاولات الأولية والمهمة للتعبير عن الحاجة الملحة في توسيع مفهوم الإرهاب الدولي.

الكلمات الدالة: الإرهاب، الإرهاب الإلكتروني، السيبرانية، الثورة المعلوماتية، الأمن المعلوماتي..

المقدمة

لقد أصبح موضوع الإرهاب الإلكتروني يمثل التحدي الأكبر بين كل التحديات الأمنية التي تتعرض لها كثير من دول العالم، حيث يمر العالم في المرحلة الراهنة بتطور الأساليب المستخدمة من قبل الإرهاب ومريدي، فقد بات الإرهاب ظاهرة متنامية محليًا ودوليًا، وبدا كأسلوب للتعبير عن اتجاه مرفوض من السلطة القائمة كونه الأكثر عنفًا نشأ وتطور وأخذ يمارس نشاطه في العادة بعيدًا عن القنوات الشرعية المعترف بها، ولأن القائمين بالأعمال الإرهابية يخشون أساسًا من التعرُّف إليهملذلك أصبح عملهم يأخذ طابع السرية الشديدة ويقومون بتوجيه الضربات إلى مواقع غير متوقعة، ولأنهم لا يستطيعوا غالبًا مواجهة السلطات القائمة بسبب ما تملكه من قدرات عسكرية وأمنية منتظمة، فإن المدنيين الذين لا حول لهم هم الجهة المستهدفة من الإرهابيين الذين يسعون لإشاعة الذعر وزعزعة الاستقرار في المجتمع وهز السلطة القائمة في الدولة.

وتؤكد الوقائع أن الإرهاب الإلكتروني أصبح ظاهــرة تغـزو كل يوم أراضٍ جديدة في خريطة العالم سواءً في المشـرق أو المغرب، التي انضمـت إلى قائمـة الـدول التقليدية التي تعاني مـن هذا النوع من الإرهاب، فبعد أن شهد العالم تطورًا كبيرًا في الجريمة الإرهابية في أعقاب التغافل الدولي عن هذه الظاهرة الخطيرة جراء انشغال الدول العظمى بقياس القدرات العسكرية للواحدة منها تجاه الأخرى، وذلك في مراحل متعددة من التاريخ سواء قبل اندلاع الحربين العالميتين أو بعدهما، إذ اعتادت كل واحدة من تلك الدول على وضع تقديرات شكلية أو موضوعية لمقارنة القدرة لكي تأخذ بالحسبان النزعات لدى الطرف الآخر، وأولت حكومات تلك الدول اهتمامًا بالغًا للتكنولوجيا العسكرية الجديدة بالاعتماد على هيئات الأركان العامة لكافة الجيوش التي تستخدم المذهب (التاريخي) والمذهب (النظري) من أجل قياس القدرة لدى كل طرف.

ولا يخفى أن ما نتج عن ثورات الاتصال التكنولوجية الهائلة، أخذ يعرف بالفضاء الإلكتروني، وهو المجال الذي يشهد حاليًا دورًا كبيرًا في استراتيجيات الدول التي تمتلك أدوات التقدم التكنولوجي، وذلك على المستوى السياسي والاقتصادي والاجتماعي، والأمني والثقافي.

وفي الوقت الذي انتشر فيه استخدام وسائل التكنولوجيا والاتصال في جميع أنحاء العالم، ظهرت مجموعة من الاستخدامات السلبية لتلك الوسائل المستحدثة، حيث أصبح بإمكان الجماعات الإرهابية التنسيق فيما بينها، والتجهيز والتعبئة للقيام بالهجمات الإرهابية من خلال الفضاء الإلكتروني الذي بات مفتوحًا للاختراق من قبل الحاصلين على القدرات التكنولوجية وهنا انتشر مفهوم الإرهاب الإلكتروني على نحو لم يسبق له مثيل.

وفي العراق ظهرت تحديات فعلية خطيرة بعد عام 2003، صارت فيها الظروف البيئية الداخلية حاضنة لعناصر إرهابية بعضها محلي وآخر خارجي جاء نتيجة الحرب على البلاد، وحينذاك برزت مفاهيم متعددة كتلك التي تتعلق بالإرهاب التكفيري واجياله المتوالية التي أرادت أن تختطف الأمن والاستقرار منه. كما ظهر مفهوم الإرهاب الإلكتروني كعنصر بارز في نشاطات التنظيمات الإرهابية الوافدة وعلى رأسها ما يعرف بتنظيم الدولة الإسلامية (داعش).

مشكلة الدراسة وأسئلتها

يتطلب حصول دولة ما على التقنية التكنولوجية المتقدمة في مجال الأمن الإلكتروني، وجود فريقًا متخصصًا لاستغلالها، تلك التقنية التي تشكل وبقدر كبير جدًا مفاتيح الحل والنجاح في أثناء التصدي لعمليات الاختراق والقرصنة الإلكترونية التي ينفذها عدد من الفاعلين سواء من الدول أو غير الدول كالمنظمات الإرهابية وبعض العناصر التي تمارس عمليات الإرهاب الإلكتروني لدوافع شتى. وعليه فإن الأجهزة الأمنية المختصة في أغلب دول العالم ومن بينها العراق، باتت تواجه مشكلات عديدة في عمليات مكافحة الهجمات التي يؤديها أولئك الفاعلين.

لذا فإن هذه الدراسة معنية بالإجابة عن الأسئلة الواردة فيها، وهي تسعى إلى التغلب على الإشكاليات التي تعترض إتمام العملية البحثية في هذا الموضوع المهم، وعليه فإن مشكلة الدراسة تكمن في مدى قدرتها على الإجابة عن التساؤل الرئيس الذي مفاده: كيف أسهمت أساليب الجريمة الإلكترونية في انتقال الإرهاب التقليدي إلى الإرهاب الالكتروني؟

ومن أجل وضع الحلول اللازمة للتغلب على إشكالية هذه الورقة البحثية جرى الشروع بالبناء المفاهيمي لأهم المتغيرات، عبر السعي للإجابة عن التساؤلات الفرعية الآتية:

- ما مراحل تطور الإرهاب الالكتروني؟
- ما أبرز أساليب الجرائم الالكترونية في الإرهاب الالكتروني؟
- ما دور الجرائم الإلكترونية في انتقال الإرهاب العادي إلى الإرهاب الرقمي؟
- ما أهم السبل المتبعة من قبل الحكومة العراقية لمكافحة الإرهاب الالكتروني؟
- ما أهم وسائل خلق حالة من الوعي الأمني المعلوماتي القادرة على مكافحة الإرهاب الالكتروني؟
- ما الاجراءات المتخذة من قبل الحكومة العراقية في حماية بيانات المجتمع المعلوماتي العراقي؟

أهمية الدراسة

1. **الأهمية العملية (التطبيقية)**: لا تعد أهمية الدراسة آنية فحسب، بقدر ما أنها تبحث في ظاهرة تمثل حالة قائمة ومستمرة، تتمثل في استمرارية الهجمات الإرهابية داخل العديد من دول العالم وبضمنها العراق الذي يعاني شعبه كثيرًا من أساليب الإرهاب الشرسة، لذا فإن الأهمية العملية لهذه الدراسة تقوم على إبراز سبل مكافحة الإرهاب الإلكتروني عبر التعاون بين جميع الدول للمحافظة على قدرات الدول والحفاظ على مواردها.
2. **الأهمية العلمية (النظرية)**: تكمن الأهمية العلمية للدراسة بكونها تسهم في تعميق الفهم لدى الباحثين في دراسات الإرهاب الدولي والجماعات البشرية المتباينة التي تتعرض لظاهرة الإرهاب ضمن الدولة الواحدة من خلال الوسائل الإلكترونية، حيث تقدم الدراسة خيارات عدة مبنية على أسس ذات فائدة للمهتمين والمتابعين للشأن المحلي العراقي الإقليمي ضمن منطقة الشرق الأوسط التي تشهد دولها هجمات مستمرة واختراقات سيبرانية مستمرة
3. **الأهمية المستقبلية**: لقد أصبح الإرهاب الإلكتروني ظاهرة تشهدها معظم دول العالم والعراق خاصة خلال الفترة الزمنية التي تغطيها هذه الدراسة، خاصة بعد أن تعرض الشعب العراقي لأزمات إنسانية كانت ناجمة عن عمليات غزو فكري شديد من قبل جماعات مسلحة استطاعت تحقيق وجود لها على الأرض بعد أن نجحت في غزو عقول كثير من المتطرفين عبر أيديولوجيات لا جرت للإنسانية بصلة الأمر الذي يحتم اللجوء لسبل علمية وتكنولوجية فضلًا عن القوانين الدولية التي تراعي الجوانب الإنسانية من أجل حظر هذه الأفكار الإرهابية والتخريبية والقضاء على التعقيد الذي فرضته على شعب العراق وشعوب المنطقة وما أوجدته من تحديات.

منهجية الدراسة

لغرض انجاز موضوع هذه الدراسة، جرى الاعتماد على المناهج التالية:

1. **المنهج التاريخي** في بيان تطور الجرائم الإلكترونية التي أفضت إلى ظاهرة الإرهاب الإلكتروني.
2. **المنهج التحليلي الوصفي** يعد هذا المنهج أحد اهم المناهج العلمية وأكثرها استخدامًا في البحث العلمي، فهو القادر على تحليل مشكلة أو ظاهرة البحث العلمي على نحو دقيق، وتعرُّف أسباب حدوثها، مما يساعد على الوصول الى استنتاجات ونتائج وحلول دقيقة لها، حيث تعد الأبحاث والدراسات الاجتماعية، من أكثر الدراسات العلمية التي تستخدم هذا المنهج.

الدراسات السابقة

- **دراسة مسلم (2021): الجرائم السيبرانية وأثرها في الأمن السيبراني (نبراس ابراهيم مسلم, 2021):** تهدف الدراسة إلى التعريف بالجرائم الإلكترونية، وبيان دور الاتفاقيات العالمية في مكافحة الجرائم السيبرانية وآثارها، وذلك من خلال الوقوف عند التحديات التي يمثلها الأمن السيبراني، وما هي العلاقة بين الأمن القومي والأمن السيبراني.

وتوصلت الدراسة إلى عدد من الاستنتاجات التي كان من أبرزها: عدم الاتفاق الفقهي على تعريف محدد للجرائم السيبرانية، وأن السنوات القليلة الماضية شهدت العديد من الجرائم السيبرانية التي كان من نتائجها الإضرار الجسيم بالدول، فضلًا عما تسببت به من أضرار بالمنشآت الحيوية للدول المستهدفة بتلك الجرائم.

- **دراسة علي (2017): إشكاليات تداخل الصراعات السيبرانية والتقليدية (خالد حنفي علي، 2017):** تهدف الدراسة إلى تعرُّف العلاقات الارتباطية بين طبيعة الصراعات وأشكالها، في ضوء ما تشهده الدول والمجتمعات من تطورات مادية وغير مادية، وتعارض تلك العلاقات مع مضمون الفكرة الصراعية، بعد أن عرف العالم في القرنين العشرين والحادي والعشرين، أنماطًا من الصراعات تعددت قضاياها داخليًا وخارجيًا.

وتناولت الدراسة موضوعها من خلال التطرق إلى تشابك المجالين الإلكتروني والواقعي بعد أن تبلورت ظاهرة الصراع السيبراني التي أثارت تحديًا أمام العلماء والباحثين من أجل فهم طبيعتها. كما عرجت الدراسة على العديد من المشاكل التي تتعلق بالحاجة لفهم الصراع السيبراني، والمتعلقة بطبيعة الأطراف المتنازعة حكومية كانت أم غير حكومية، مدنية أم عسكرية.

- **دراسة عبد الصبور (2017) الصراع السيبراني.. طبيعة المفهوم وملامح الفاعلين (سماح عبدالصبور، 2017):** تهدف مناقشة ظاهرة الصراعات السيبرانية بوصفها ساحة للصراع العالمي، إلى معرفة ماهية هذه الصراعات، وعوامل نشأتها، وحدود الاختلاف عن نظيراتها التقليدية، إلى جانب الاتجاهات المفسرة لظاهرة الصراعات السيبرانية ومساراتها المستقبلية في تشكيل التفاعلات العالمية، التي سبق أن واجهت مفاهيم تقليدية، مثل: الصراع والأمن والقوة والسيادة، لحين بروز مداخل ورؤى نظرية أكثر قدرة على تفسير طبيعة التغيرات التي ألحقتها التكنولوجية الحديثة بهذه المفاهيم؛ لذا فإن هذه الدراسة توصلت إلى خمسة سيناريوهات لمستقبل الصراع في الفضاء السيبراني في ظل التطورات والتغيرات المستمرة في هذا المجال، وقد استندت هذه الدراسة إلى ما وضعه جاسون هايلي لهذه السيناريوهات الخمسة، التي تتعلق بالاتي: استمرار الوضع الراهن، ووضع الأمان الجزئي، ووضع الأمان الواسع، ووضع البلقنة الإلكترونية، ووضع الخطر.

- **دراسة حسين (2017): فرص وقيود الأطراف المتنازعة على المجال العام السيبر اني (ابتسام علي حسين،2017):** تهدف إلى مناقشة ملامح ظاهرة المجال العام الإلكتروني، ومدى اختلاف توظيفها في الصراعات السياسية بين الأنظمة الحاكمة، والجماعات السياسية، بخلاف ما تطرحه من فرص وتحديات لهؤلاء الفاعلين. وتناولت الدراسة المجال العام بين التقليدي والسيبراني، كما تطرقت إلى الأنظمة السياسية وتقييد المجال العام، وتوصلت إلى نتائج عديدة تتعلق بالآتي:
  - أسهم الفضاء الإلكتروني في تعزيز فاعلية المجال العام، وزاد الصراع حوله بين الحكومات والجماعات المختلفة.
  - عدم قدرة الحكومات على منع المحتوى المتطرف قبل ظهوره في المجال العام السيبراني.
  - لا يمكن لأي دولة أن تنأى بنفسها عن الإرهاب الذي صار معولماً.

- **حرب الفضاء الالكتروني (التهديد التالي للأمن القومي وكيفية التعامل معه(ريتشارد كلارك, روبرت ديك ,2010).**

Cyber War: The Next Threat to National Security and What to Do About It. 2012

خلصت الدراسة الى:

- إنّ حرب الفضاء الالكتروني ليست نوعًا جديدًا نظيفًا من الحروب، التي لا ضحايا فيها، ومن ثم ينبغي ان نتبناها، وليست نوعًا من الاسلحة السرية التي يجب أن نبقيها خافية عن العيان وعن عامة الشعب؛ وذلك لأن الشعب من السكان المدنيين بالولايات المتحدة و الشركات العامة التي تدير نظمنا الوطنية الرئيسية هو من سيعاني في حال وقوع أي حرب الكترونية.
- ظاهرة حرب الفضاء الالكتروني برمتها تحيط بها السرية الحكومية الى حد يجعل الحرب الباردة تبدو و كأنها عصر من عصور الانفتاح و الشفافية. ولعل أكبر أسرار عالم حرب الفضاء الإلكتروني يتلخص في أن الولايات المتحدة بينما تعد العدة لها هجوميا، فإنها تواصل سياساتها التي تجعل من المستحيل الدفاع عنها دفاعًا فعالًا ضد أي هجوم الكتروني.
- كانت حرب الفضاء الالكتروني مزية لأمريكا على ما يبدو، فإنها في حقيقة الأمر تعرضها لخطر أكبر مما تتعرض له أي دولة أخرى. فهذا النوع الجديد من الحروب ليس لعبة أو شطحة من شطحات الخيال، وهي أبعد ما يكون عن كونها بديلًا للحرب التقليدية؛ حيث إنها قد تزيد من احتمالية القتال التقليدي بالمتفجرات والمقذوفات. لذلك علينا أن نشرع في سلسلة من المهام المعقدة، تتلخص في أن نفهم ماهية حرب الفضاء الالكتروني، ونتعلم كيف تدور ولماذا تدور، ونحلل أخطارها و نعد العدة لها ونفكر في كيفية السيطرة عليها.

- **الأمن السيبر اني و الحرب السيبر انية (P.W Singer and Allan Friedman, 2014)**

ماذا يجب علينا ان نعرف؟

Cybersecurity and Cyberwar what everyone needs to know by P.W Singer and Allan Friedman

تهدف هذه الدراسة إلى: معرفة العلاقة الثنائية بين الأمن السيبراني وأفعال الحرب السيبرانية مع بيان الفجوة المعرفية في الأمن السيبراني، وتسليط الضوء على الأخطار التي تمثلها، والمقارنة في الانفصال المعرفي (الرقمي) بين قادة من الشباب اليوم (مواطنون رقميون) نشأوا في عالم مرتبط رقميا مع الآخر وقيادات فاعلة يطلق عليها (المهاجرين الرقميين).

حاول الكاتبان معالجة القضايا الجوهرية التي يجب أن يعرفها الجميع حول الأمن السيبراني والحرب السيبرانية و تقوم منهجية الكتاب على طريقة الأسئلة و الأجوبة، وأدرج الكاتبان منهجية الأسئلة لثلاث فئات: وهي الأسئلة حول الخطوط الأساسية وديناميكيات الفضاء السيبراني والأمن السيبراني (أسئلة) من قبيل كيف يعمل كل هذا؟ لكونها الجزء (المحرك) الذي يضع لبنات البناء الأساسية لعالم الانترنت؟ و الفئة الثانية تساؤلات حول التداعيات الأكثر اتساعًا للأمن السيبراني خلف الفضاء السيبراني؟، ثم الفئة الثالثة حول الاستجابات المحتملة ماذا يمكننا أن نفعل؟.

- **الحروب المستقبلية في القرن الحادي و العشرين(مركز الإمارات للدراسات والبحوث الاستراتيجية, 2014) The Future of Warfare in the Twenty First Century**: يناقش هذا الكتاب الصادر عام 2014، لمجموعة كتاب صادر عن مركز الإمارات للدراسات و البحوث الاستراتجية، التحولات والتغيرات الجذرية في مفاهيم الحرب و نظرياتها , ومن ثم ما لحقت هذه التغيرات بالعقائد القتالية للجيوش. وظهرت مفاهيم ونظريات عسكرية جديدة ولدت من رحم التهديدات الأمنية غير التقليدية التي برزت على الساحة العالمية خلال العقدين الأخيرين، وباتت مصطلحات مثل (الحرب اللامتماثلة) و (الحرب السيبرانية) و (الحرب عن بعد) واقعًا متحققًا في العديد من الصراعات العسكرية في العالم.

وتناول هذا الكتاب الطبيعة المتغيرة للحرب والتهديدات الجديدة للأمن القومي؛ مثل: الإرهاب، حروب التمرد، والحرب السيبرانية. ثم يتناول موضوع الابتكار في الصناعة الدفاعية، و الدور المستقبلي للتكنلوجيا في الاستخدام العسكري، ويناقش الكتاب الجوانب السياسية والمدنية المؤثرة في الحروب المستقبلية، والعلاقات بين المؤسستين العسكرية والمدنية، ولاسيما العلاقة المتشابكة بين شركات تصنيع الأسلحة و المؤسسة العسكرية، والأبعاد الاستراتيجية لتلك العلاقة.

التعقيب على الدراسات السابقة

تعدّ الدراسات السابقة التي جرى استعراضها مجموعة تسلط الضوء على الأبعاد المتعددة للظواهر المرتبطة بالأمن السيبراني والإرهاب الإلكتروني. في بعض الدراسات لم نلحظ وجود اهتمام فعال بالمنهجية المتعمدة لاسيما تلك التي تناولت هذا الموضوع المهم من خلال عرضها للمعطيات بأسلوب إعلامي أكثر مما هو علمي يخضع للأساليب المتبعة في البحوث والدراسات الأكاديمية. لوحظ وجود قصور في عدد من الدراسات السابقة في ملاحقة التشريعات التي تصدرها الدول منفردة أو مجتمعة ضمن بعض التشكيلات الدولية أو الإقليمية في المجتمع الدولي.

هناك اختلاف في جوانب معينة مع الدراسات الحالية, وتتوافق في جوانب من ناحية ثانية، ان هذا الاختلاف لا يستبعد ان الباحثين قد انتفعوا بالفائدة من الدراسات السابقة من الناحية المنهجية التي جرى اتباعها, بالإضافة الى ذلك إفادة الباحثين من الدراسات السابقة في تحسين ادوات الدراسة, ودلالة على هذا ان الدراسة تعد استمرارًا للدراسات السابقة, من ناحية اهمية ارشاد مراكز التخطيط الاستراتيجي لتقديم مقترحات تستند إلى الأدلة والتوجهات المعاصرة في أمن المعلومات, يؤدي ذلك إلى تعزيز استعداد الحكومات، مثل الحكومة العراقية، لتطوير سياسات فعالة لمكافحة التهديدات السيبرانية.

الى جانب ذلك تطوير اسس ومعايير النواتج البحثية الاكاديمية وتحسينها, وفي ظل الاوضاع الامنية التي مر بها العراق لا بد من تقديم بحوث ودراسات في موضوع الدراسة واعطاء دور للكوادر التدريسية لتقديم انتاجات بحثية خلال حصول حدث امني معين يخص موضوع الدراسة.

المبحث الأول

الإطار المفاهيمي

أصبح الحديث عن ظاهرة الإرهاب يمثل ولوج في عالم الإنسانية بالكامل، فالإنسان بفطرته لا يتخلى عن قيمه الإنسانية إلا حين تهب عليه أحداث طارئة، هي إفراز لفقدان مناهج الحياة السياسية والاقتصادية والاجتماعية والنفسية، لمسارها الطبيعي المتولد نتيجة مسارها غير السوي في معالم الحياة، وما له من دور أيضًا في حدوث صراع في كيان الإنسان على ذاته، فيتحول من إنسان سوي إلى مخلوق عدواني يفوق البهائم في طمعها و وحشيتها، وبهذا تتقين أن الإنسان لا يثور على واقعه سعيًا إلى تغييره إلا بعد أن يعاني صراعًا في عالمه الداخلي المصاغ من واقعه المضطرب. وهذا يعني أن الإرهاب هو انعكاس لواقع يشكو الانفصام بين قيم الخير والشر، وبين الاستواء والانحراف في الذات الفردية والجماعية.

وقد بات لزامًا علينا تحديد المفاهيم المرتبطة بمفردة الإرهاب عبر توضيح معنى الإرهاب بعد أن غاب الاتفاق الواضح المحدد بين المتخصصين حول مفهومه، فالذي تراه طائفة عملًا إرهابيًا، تعده أخرى عملًا مشروعًا بطوليًا، مثلما يتداخل هذا المفهوم مع مفاهيم أخرى شبيهة له في العمل، مما أدى إلى اختلاط مفهوم الإرهاب مع تلك المفاهيم والعمليات التي تجيزها بعض المنظمات والحركات الدينية إسلامية كانت أو غير إسلامية التي تنادي باستخدام العنف بما فيها الإرهاب الموجه إلى أهداف معينة وإن لم يؤد إلى تحقيق الأهداف المنشودة أمرًا مقبولًا.

الإرهاب لغويًا: مأخوذ من رهب بالكسر، يرهب، رهبة أو رهبًا: وهو بمعنى خاف مع تحرز واضطراب **(محمد بن يعقوب الفيروز اباداي,1987)**، والإرهاب بكسر الهمزة: بمعنى الإزعاج والإخافة، ولها معنى آخر وهو قدع الإبل عن الحوض وذيادها **(اسماعيل بن حماد الجوهري,1979)**.

الإرهاب إصطلاحًا: هو " بث الرعب الذي يثير الخوف والفعل أي الطريقة التي تحاول بها جماعة منظمة أو حزب أن يحقق أهدافه عن طريق العنف، وتوجه الأعمال الإرهابية ضد الأشخاص سواء كانوا أفراد أو ممثلين للسلطة ممن يعارضون أهداف هذه الجماعة، مثل ما يعد هدم العقارات وإتلاف المحاصيل في بعض الأحوال كأشكال للنشاط الإرهابي **(احمد زكي بدوي, 1993)**. وهناك من قال إن الإرهاب هو: "محاولة نشر الذعر والفزع لأغراض سياسية، أو وسيلة تستخدمها حكومة استبدادية لإرغام الشعب على الخضوع والاستسلام لها **(احمد عطية, 1975)**.

مفهوم الإرهاب

ظهرت محاولات تعريف هذا المفهوم عن طريق ترتيب عناصره حسب أهميتها ومنها العنف، واستخدام القوة، والعنصر السياسي، والخوف، والفزع، والرهبة، والتهديد باستخدام القوة، أو التلويح بها، وإحداث نفسي ورد فعل أوسع لا ينحصر في الضحايا، واختيار الضحية من أجل ضمان تأثير أكبر لتحقيق الهدف، والتخطيط والنظام، وأسلوب القتال، والاستراتيجية والتكتيك، وخرق القوانين النافذة وتجاهل المبادىء الإنسانية، ونشر الشعور بالإذعان باستخدام القهر، والتركيز على الدعاية الإعلامية، والعشوائية وبدون تمييز وغيرها من الألفاظ الأخرى **(خالد عبيدات, 2006)**.

وعرفه قانون مكافحة الإرهاب العراقي بأنه: " كل فعل إجرامي يقوم به فرد، أو جماعة منظمة استهدف فردًا أو جماعات، أو مؤسسات رسمية، أو غير رسمية أوقع الضرر بالممتلكات العامة، أو الخاصة بغية الإخلال بالوضع الأمني، أو الاستقرار والوحدة الوطنية، أو إدخال الرعب لغايات إرهابية" **(وثيقة قانون مكافحة الارهاب العراقي رقم 13, 2005)**.

الإرهاب الدولي: ذكرت لجنة الإرهاب الدولي التابعة للأمم المتحدة عام 1980 بأن الإرهاب الدولي هو " عملٌ من أعمال العنف الخطيرة أو التهديد بالعمل

به، يصدر من فرد أو جماعة سواء كان يعمل بمفرده أو بالاشتراك مع أفراد آخرين ويوجه ضد الأشخاص، أو المنظمات، أو المواقع السكنية، أو الحكومية، أو الدبلوماسية، أو وسائل النقل والمواصلات، أو ضد أفراد الجمهور العام من دون تمييز للون، أو الجنس، أو الجنسية، بقصد تهديد هؤلاء، أو التسبب في إصابتهم، أو موتهم، أو التسبب في إلحاق الخسارة، أو الضرر، أو الأذى بهذه الأمكنة، أو الممتلكات، أو تدمير وسائل النقل والمواصلات، بهدف إفساد علاقات الود والصداقة بين الدول، أو بين مواطني الدول المختلفة، أو ابتزاز تنازلات معينة من الدول في أية صورة كانت **(مختار شعيب, 2004)**.

الإرهاب الإلكتروني: يعرف هذا المفهوم قانونيًا بأنه: كل استخدام للقوة، أو العنف، أو التهديد، أو الترويع الذي يلجأ إليه الجاني تنفيذًا لمشروع إجرامي، فردي، أو جماعي بهدف الإخلال بالنظام العام، أو تعريض سلامة المجتمع وأمنه للخطر إذا كان من شأن ذلك إيذاء الأشخاص، أو إلقاء الرعب بينهم، أو تعريض حياتهم، أو حرياتهم، أو أمنهم للخطر، إن إلحاق الضرر بالبيئة، أو بالاتصالات، أو بالمواصلات، أو بالأموال، أو المباني، أو بالأملاك العامة، أو الخاصة، أو احتلالها أو الاستيلاء عليها أو منع أو عرقلة، ممارسة السلطات العامة أو دور العبادة أو معاهد العلم، لأعمالها أو تعطيل تطبيق الدستور أو القوانين أو اللوائح **(احمد فتحي سرور, 2008)**.

مفهوم السيبرانية

اشتق مصطلح "سيبيرية" أو "سايبورغ" من Cybernetic Organism، وتعني حرفيًا الكائن المهجن بين الآلة والأعضاء الحية، وهي مفردة بدأ استخدامها عام 1960 من قبل مانفريد كلاينس وناثان كلاين في مقال لهما قصدا بها عملية المزج بين الاليكترونيات والأنسان **(ايهاب شوقي, 2015)**.

وشهد مصطلح السيبرانية استخدامًا متسارعًا أواخر القرن العشرين وأوائل القرن الحادي والعشرين، بعد أن اهتمت الدول بالتطورات التكنولوجية، وبات مصطلح الأمن السيبراني من أكثر المصطلحات استخدامًا، ويدل على: مجموع الوسائل التقنية والإدارية التي يجري استخدامها لمنع الاستخدام غير مصرح به وسوء الاستغلال واستعادة المعلومات الالكترونية ونظم الاتصالات والمعلومات التي تحتويها بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتأمين حماية وسرية وخصوصية البيانات الشخصية ولحماية المواطنين من المخاطر في الفضاء السيبراني**(ليال البيطار, 2014)**.

الأمن السيبراني: هو مجموع الوسائل التقنية والتنظيمية والإدارية التي يجري توظيفها لمنع الاستخدام غير المصرح، وسوء الاستغلال، واستعادة المعلومات السيبرانية، ونظم الاتصالات والمعلومات التي تحتويها، وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات، وتعزيز حماية وسرية وخصوصية البيانات الشخصية، واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني، ومن ثم فإن الأمن السيبراني يشكل مجموع الأطر القانونية والتنظيمية، والهياكل التنظيمية، وإجراءات سير العمل، بالإضافة إلى الوسائل التقنية والتكنولوجية، التي تمثل الجهود المشتركة للقطاعين الخاص والعام، المحلية والدولية، التي تهدف إلى حماية الفضاء السيبراني الوطني، مع التركيز على ضمان توافر أنظمة المعلومات، وحماية خصوصية وسرية المعلومات الشخصية، واتخاذ جميع الإجراءات الضرورية لحماية المواطنين من الفضاء السيبراني **(الدويك, عبدالغفار عفيفي, 2018)**.

المبحث الثاني

انتقال الجرائم الإلكترونية إلى الإرهاب الرقمي

تنوعت نشاطات الفاعلين في مجال الإرهاب الإلكتروني وسلوكاتهم وتباينت حتى أخذت شكل المستويات الهرمية من حيث تأثيراتها، ووفق الآتي **(Paul Roseenzweig,2013)**:

- **<u>الجرائم الإلكترونية</u>**: تحدث في قاعدة الهرم التي تكون مهيئة للحالات الأكثر حدوثًا، والأقل ضررًا، وهي الجرائم الإلكترونية، التي تنطوي على الاحتيال، وسرقة الأموال والهويات، وهي أحيانًا تكون كارثية، ولكن تهديدها ليس ساحقًا، ولا تمثل تهديدًا وجوديًا.
- **<u>التجسس السيبراني</u>**: يكون في وسط الهرم، وهو أكثر تطورًا، حيث يشمل هجمات إلكترونية من فاعلين من الدول، وغير الدول لسرقة الأسرار القومية، أو حقوق الملكية الفكرية، وهذا النمط هو الأكثر انتشارًا على الساحة الدولية، وله آثار سلبية على الأمن القومي للدول.
- **<u>الحروب السيبرانية</u>**: تظهر في قمة الهرم هذ النوع من الحروب بين الدول ذات القدرات الحاسوبية المتطورة التي تتصارع فيما بينها، ورغم أن هذه الحروب لا تظهر على نحو مستقل عن الحروب التقليدية، إلا أنها إذا حدثت على نحو منفصل فقد تكون آثارها التدميرية أعلى بكثير من الحروب التقليدية.

ووفقًا لذلك فإن الإرهاب الإلكتروني قد اتسع بصورة كبيرة تبعًا لتوسع مفهوم القوة الذي أصبح يضم أسلحة متنوعة عسكرية وغير عسكرية، خاصة بعد دخول المجال السيبراني ضمن مدلولات الإرهاب التي يجري فيها استخدام مختلف الأسلحة لإجبار الخصم على الخضوع لإرادة خصمه، وإذا ما جرى استخدام هذه الأسلحة بنجاح، فإنها من الممكن أن تهزم جيوشًا متعددة لا جيش واحد، وهناك مجالات رئيسية يسعى المهاجمون إلى استهدافها من خلال الإرهاب الإلكتروني، **هي(Brandon Valeriano, Ryan c. Maness,2014)**:

أولا: **تخريب ومهاجمة مواقع الانترنت Website Defacements or Vandalism**: وهو أبسط أشكال مجال الإرهاب الإلكتروني، ويتم ذلك عبر

مهاجمة مواقع الخصوم بهدف تدميرها، أو تشويهها، عبر نشر النصوص والصور المسيئة، وذلك لتوصيل رسالة إلى الهدف بأنه يفتقر لقدرة السيطرة على عمليات الفضاء الإلكتروني الخاصة به. وبرغم أن هذا النوع من المجالات الإرهابية قد لا يؤثر في الحكومات، إلا إن استهدافه يترك آثار قد تكون مضاعفة في المجتمعات.

ثانيا: **الحرمان من الخدمة Denial of Service Method :** وهو المجال الأكثر تطورًا، حيث يجري استهداف أجهزة التوجيه التي تغلق المواقع الإلكترونية، وتوقف الخدمات، مثل توقف الخدمات الحكومية المقدمة عبر المواقع الرسمية للدولة.

ثالثا: **الاقتحام الفيروسي Intrusions:** وهو المجال الأكثر حدة على المدى الطويل في الهجمات الإلكترونية، خاصة أنه كامنًا لفترة طويلة، ويظهر دون سابق إنذار. ويحتاج هذا المجال لأسلحة سيبرانية تضم برامج خبيثة يصعب الكشف عنها، وتقوم بسرقة المعلومات، وتكون لها آثار كبيرة على المصالح الحيوية للدولة، وقد لا يحتاج هذا المجال إلى قراصنة، وإنما برامج تقوم عليها دول.

رابعا: **عمليات التسلل Infiltrations:** ويقوم المهاجم في هذه العمليات بمحو جميع البيانات داخل نظام دولة أخرى أو شبكتها الإلكترونية، كما قد يتكرر الهجوم بقصد إفساد، أو تعديل الملفات، أو التقاط المعلومات المتدفقة عبر الويب. وتحتاج هذه النوعية من العمليات إلى أسلحة إلكترونية متطورة للغاية، وأكثر استهدافًا للعدو، نظرًا إلى فداحة تأثيراتها، خاصة إذا كانت تستهدف البنى التحتية للدول.

وعليه فإن تلك المجالات المستهدفة من قبل الفاعلين في الإرهاب الإلكتروني باتت تؤثر في قدرات الدول التي تدخل في صراعات وحروب مع الدول الأخرى، ورغم كل ذلك فأن هذه الصراعات والحروب كانت في السابق تحمل سمات تقليدية وأنها قد سيطرت على مجريات الأحداث لفترات طويلة من الزمن في الحروب اندلعت بين الدول، إلا أن النوع الجديد من الحروب التي تعرف بالسيبرانية قد اندلعت بعد اتساع نشاطات الفاعلين من الدول والفاعلين من غير الدول وامتدادها إلى ساحات مفتوحة، وذلك نتيجة سهولة دخول ساحة الفضاء الإلكتروني (السيبراني)، وعدم اقتصار امتلاك الأسلحة السيبرانية على دول أو جهات بعينها، وقد أثبتت الوقائع الفعلية للهجمات السيبرانية بما لا يدع مجالًا للشك مشاركة الفاعلين من غير الدول على نحو كبير ومتصاعد في شن الحروب السيبرانية، الأمر الذي يجعلها حربًا في غاية التعقيد، حيث تفرض العديد من الإشكاليات المتعلقة بحالة في غاية التعقيد، حيث تفرض العديد من الإشكاليات المتعلقة بحالة عدم اليقين حول منفذ الهجوم السيبراني، وما إذا كانت إحدى الدول هي التي نفذته أو الفاعلون من غير الدول لغرض معين، أو يجري استخدامهم للقيام بالهجوم لصالح جهة أخرى، ثم في حالة معرفة هؤلاء الفاعلين تظل الدولة أو الجهة المستهدفة مكتوفة الأيدي نتيجة لعدم تمكنها من تخطي سيادة الدولة الأخرى التي يوجد بها هؤلاء الفاعلون **(catherine A. Theohary, john w.Rollins,2013)**

المبحث الثالث

الإرهاب الإلكتروني في العراق والسبل المتبعة من قبل الحكومة لمكافحته

بات التعاون الجدي من قبل أغلب دول العالم يعد ضرورة لازمة لمواجهة نشاطات الفاعلين في مجال الإرهاب الإلكتروني، وذلك لصد الهجمات الإلكترونية التي ازدادت على نحو متسارع خلال الألفية الثالثة، وبالفعل عمدت كثير من الدول إلى عقد الاتفاقيات الجماعية والثنائية لتسهيل مهمة التصدي للهجمات السيبرانية ومكافحة الإرهاب الإلكتروني)**محمد الأمين البشرى, 2000).**

وفي العراق وما أن حدث التغيير عام 2003 حتى تعرض المجتمع العراقي إلى حالة من الاضطراب والاختلال الوظيفي في البناء الاجتماعي فضلًا عن السياسي والاقتصادي إذ حدث خلل في البنية الاجتماعية، وأسهمت حالات الفقر والعنف والتحول الديمقراطي في تعزيز هذا الاضطراب إذ تحول المجتمع العراقي من حالة الاستبداد والقهر والقيود في الحريات إلى حالة الانفتاح الشامل، مما جعل المجتمع العراقي يواجه ثقافات وسلوكات مختلفة، أثرت على نحو كبير في طبيعة النسق الاجتماعي مما سبب إرباكًا في المجتمع، وأشاع حالة من الاغتراب والتناحر الطائفي في جسده ومن ثم شيوع الثقافات والانتماءات الفرعية والقبلية **(عدنان ياسين مصطفى واخرون, 2015).**

ومنذ عام 2006 لاحظت الأجهزة الأمنية ازدياد النشاطات إلكترونية غير المشروعة في العراق بسبب الانتشار السريع للخدمات والعمليات عبر شبكة المعلومات العنكبوتية، فارتفعت معها نسبة جرائم الانترنت والنشاطات المضرة بالنظام والمجتمع العراقي، بل إن نسبة القرصنة السيبرانية في العراق باتت هي الأعلى في منطقة الشرق الأوسط، وتنوعت حالات الجرائم في العراق التي تحول أغلبها إلى الجرائم الرقمية، ومنها: عمليات الغش عبر الانترنت، وغسيل الأموال، وتزايد مواقع القرصنة، والتجارة الإلكترونية غير المشروعة، والتطفل على الشبكات، والاستغلال الجنسي الذي أصبح يمثل ظاهرة كبيرة حين تحول إلى الإرهاب الإلكتروني.

وأشارت الإحصائيات الرسمية الخاصة بالجرائم الإلكترونية خلال الأعوام 2006-2011، إلى أن هذه الجرائم قد ازدادت على نحو ملحوظ بمعدل سنوي متوسط قدره (2.2%)، وتم ارتكاب معظم هذه الجرائم من قبل حاملي شهادة الثانوية بنسبة (4.6%)، وبالدرجة الثانية حاملي شهادة البكالوريوس بنسبة (8.27%)، والباقي بنسبة (8.8%). وكانت السرقة تمثل أعلى نسبة في حالات الجريمة الإلكترونية مقارنة بالحالات الأخرى، وقد شكلت

شريحة الشباب أعلى نسبة في هذا النوع من الجرائم، إذ إن إجمالي هذه الجرائم ارتكبها أشخاص تقل أعمارهم عن 24 عام بنسبة (8.4%)، وقد احتل الذكور النصيب الأكبر، فمن مجموع الجرائم الإلكترونية في العراق ارتكب الذكور ما نسبته (1.8%) **(Aboud, Sattar J,2012)**.

ومع مرور الوقت برزت ظاهرة الإرهاب الإلكتروني حينما استغلت الجماعات الإرهابية حالة الاضطراب السياسي والاقتصادي في العراق، مستعينة بالتطور التكنولوجي واستخدامات التقنية الحديثة، فقد أتاح لها الفضاء السيبراني غير المسيطر عليه من قبل الدولة، إنشاء المواقع الإلكترونية والمنتديات التحاورية وما يسمى بالكيانات الالكترونية المفتوحة، وهي مواقع الكترونية تقوم الجماعات الإرهابية من خلالها بممارسة نشاطاتها المختلفة في العراق من دعاية وتجنيد ونشر الأفكار المتطرفة بواسطة الشبكة العنكبوتية، وعلى وجه الخصوص منذ سيطرة تنظيم داعش الارهابي على مدينة الموصل في حزيران 2014 حينما حقق هذا التنظيم الإرهابي وجود عسكري كبير وسيطرة ميدانية على أراضي واسعة من العراق)**أسعد طارش عبد الرضا, علي إبراهيم المعدومي, 2020)**.

وهنا وجدت الحكومة العراقية إن عليها التعامل بجدية مع عدد من السبل لمكافحة ذلك النوع من الإرهاب، حيث جرى التعاطي مع:

1. التوجهات الدولية الساعية لمكافحة الإرهاب بصورة عامة والإرهاب الإلكتروني بصورة خاصة، الأمر الذي فرض إيجاد تقارب بين جهود الحكومة العراقية مع الجهود الدولية ومساعي المنظمات الدولية التي تعمل باستمرار لمواكبة التطورات في شأن أمن المعلومات، ولاسيما بعد أن تأسست مجموعات عمل لوضع استراتيجية مكافحة جرائم الإنترنت.
2. التثقيف على مفهوم الأمن السيبراني الذي يهتم بنشاطات مختلفة كجمع المعلومات ووضع السياسات العامة والتدابير الأمنية، والمبادئ التوجيهية، وطرق إدارة المخاطر، والحماية، والتدريب، وهو بمثابة دليل لأفضل الممارسات المهنية، ومختلف التقنيات التي يمكن استخدامها لحماية شبكة الإنترنت.
3. اتباع سياسة أمن المعلومات وأجهزة الكمبيوتر، والأفراد، والبنية التحتية، وبرامج المعلوماتية، والخدمات، ونظم الاتصالات السلكية واللاسلكية، ومجمل المعلومات المنقولة أو المخزنة في الاجهزة الإلكترونية وذلك لضمان تحقيق سلامة المؤسسات والأفراد في مواجهة المخاطر الأمنية وكل ما يتعلق بعمل المؤسسات ضمن شبكة الانترنت.

لقد تطلبت عمليات مكافحة الإرهاب الإلكتروني في العراق اتباع مجموعة من التدابير التشريعية والقانونية، وعند تتبع موقف المشرع العراقي لم نلحظ وجود تشريع يجري من خلاله التعاطي مع الجرائم الإلكترونية فضلًا عن مكافحة الإرهاب الإلكتروني، وعلى الرغم من ذلك فقد وجدت بعض المحاولات التي لم يجري المصادقة عليها من قبل مجلس النواب، ومنها مشروع قانون الجرائم المعلوماتية لسنة 2012، ثم شرع مجلس النواب في إعداد مشروع قانون خاص بالجريمة المعلوماتية عام 2018 الذي جاء فيه **(مشروع قانون الجريمة المعلوماتية 2018)**.

أ. توفير الحماية القانونية للاستخدام المشروع للحاسب وشبكة المعلومات

ب. تحقيق الأمن المعلوماتي وتوفير أقصى درجات ممكنة من الحماية لشبكات المعلومات واجهزة الحاسوب وبرامج الحاسوب من الاعتداءات وسوء الاستخدام والهجوم الإلكتروني.

ج. معاقبة مرتكبي جرائم المعلومات.

د. حفظ الحقوق على الاستخدام القانوني المشروع للحاسبات والشبكات المعلوماتية.

هـ. حماية المصلحة العامة والاخلاق والآداب العامة.

و. حماية الاقتصاد الوطن.

أما في ما يتعلق بإجراءات الحكومة العراقية في مجال مكافحة الإرهاب بصورة عامة بما فيها ظاهرة الإرهاب الإلكتروني، فيمكن الإشارة إلى أهم تلك الاجراءات:

أولا: دستور عام 2005

أشار دستور جمهورية العراق لعام 2005 إلى تجريم الإرهاب، وذلك من خلال النصوص الآتية **(دستور جمهورية العراق, 2005):**

(1) يحظر كل كيان أو نهج يتبنى العنصرية أو الإرهاب أو التكفير أو التطهير الطائفي أو يعرض أو يمهد أو يمجد أو يروج له أو يبرر له وبخاصة البعث الصدامي في العراق ورموزه وتحت أي مسمى ولا يجوز أن يكون ذلك ضمن التعددية السياسية وينظم ذلك بقانون.

(2) تلتزم الدولة بمحاربة الإرهاب بجميع أشكاله، وتعمل على حماية أراضيها من أن تكون مقرًا، أو ممرًا، أو ساحةً لنشاطه.

ثانيا: قانون جهاز مكافحة الإرهاب لعام 2005:

تناول قانون جهاز مكافحة الارهاب أهداف هذا الجهاز والقوات التابعة له التي تدور حول الآتي **(قانون جهاز مكافحة الإرهاب, 2005):**

(1) مكافحة الإرهاب بجميع أشكاله والقضاء علية.

(2) وضع سياسات استراتيجية شاملة لمكافحة الإرهاب وتطويرها.
(3) التعاون مع الجهات الامنية ذات الصلة بمكافحة الارهاب.
(4) انقاذ الرهائن وتحريرهم عن طريق التفاوض السلمي أو الاقتحام المباشر لمكان الحدث الإرهابي.
(5) التنسيق مع الأجهزة الاستخباراتية المتخصصة لتنفيذ خطط مكافحة الإرهاب.
(6) تبادل المعلومات وتداولها وتقيمها الخاصة بمكافحة الإرهاب داخل العراق وخارجة.
(7) تنفيذ أي مهمات أخرى يطلبها رئيس الجهاز وبمصادقة الهيئة الوزارية للأمن.

ثم شرعت الأجهزة الحكومية المختصة بإطلاق استراتيجية الأمن السيبراني في العراق بالاستناد إلى مجموعة من الأهداف الرئيسية، التي كان من أبرزها: ضمان الوضع الأمني وحماية وجوده في الفضاء السيبراني، وحماية بنية أمن المعلومات، وبناء مجتمع شبكة الاتصالات العنكبوتية الموثوق به، والتعامل مع التحديات السيبرانية التي تهدد الأمن الوطني وسلامته، وذلك عن طريق تبني مجموعة من الاجراءات القادرة على حماية فضاء العراق السيبراني والدفاع عنه **(مصطفى إبراهيم سلمان الشمري,2021)**.

الخاتمة

ظهر مفهوم الإرهاب الإلكتروني بالتزامن مع مخرجات ثورة تكنولوجيا المعلومات IT Revolution، بعد تسارع الاكتشافات العلمية Scientific Discoveries خلال العقد الأول من القرن الحادي والعشرين في مجال الاتصالات Telecommunications، وأضحى عنصرًا فاعلًا في العلاقات الدولية، نظرًا إلى ما يحمله من أدوات تكنولوجية متطورة، تلعب دورًا وتؤثر في أنماط (القوة/ الأمن)، فضلًا عن التأثير في القيم السياسية الموصلة للأزمات لدى الفاعلين البارزين في الفضاء السيبراني، وبات استخدام كثير من الدول الكبرى للقدرات التي يوفرها هذا الفضاء أمرًا مفروغًا منه في مجالات الأمن والقوة العسكرية، إذ ظهر بُعد جديد في الأزمات الدولية والإقليمية والمحلية، هو البعد السيبراني The Cyber Dimension، حيث يستطيع أحد أطراف الأزمة أن يوقع خسائر كبيرة في الطرف الآخر، وأن يتسبب في شل البنية المعلوماتية والاتصالية الخاصة به، وهو ما يسبب خسائر عسكرية واقتصادية فادحة.

وقد عُدّ دخول مفهوم الإرهاب الإلكتروني ضمن الكتابات التي سادت حول الأمن السيبراني Cyber Security منذ نهاية القرن العشرين، من المحاولات الأولية والمهمة للتعبير عن الحاجة الملحة في توسيع مفهوم الإرهاب الدولي، بحيث لا يقتصر هذا المفهوم على التهديدات التقليدية المتعلقة بالأبعاد العسكرية والاقتصادية، أما القضايا الجديدة التي ظهرت على الساحة، مثل: الأمن الشخصي، والأمن البيئي، والأمن الصحي، والأمن الغذائي، والأمن الثقافي، وبالطبع الأمن السيبراني، فجميعها قضايا مستحدثة تندرج في نطاق الأمن غير التقليدي الذي يمكن استغلالها من قبل العناصر المتطرفة وتحويلها إلى الإرهاب.

وأفصح الواقع العملي في العراق أن عمليات الإرهاب الإلكتروني (موضوع هذه الدراسة) انطلقت على شكل تهديدات سيبرانية تجاه الأفراد، حيث شكلت تحديات غير مرئية أخذت تؤثر في منظومة الأمن الوطني العراقي، خاصة مع الانفتاح على العالم والتطور التكنولوجي الذي شهدته البلاد لاسيما في مجال الاتصالات والمعلومات بعد عام 2003، لكن الأمر اللافت للنظر يبرز عن الوقوف على البنية التحتية الخاصة بالحماية الإلكترونية التي يعاني منها العراق على المستوين الرسمي والشعبي، مما جعل العراق يصبح مكشوفًا للكثير من الفاعلين في مجال الأمن السيبراني وبالتالي تعرضه للاختراق والتجسس عليه وعلى شعبه، لاسيما من المنظمات التي تتبع المنهج الإرهابي.

نتائج الدراسة ومناقشتها

تتفق البعض من النتائج مع ما توصلت اليه نتائج الدراسات السابقة مثالا على ذلك: دراسة مسلم (2021): الجرائم السيبرانية وأثرها في الأمن السيبراني التي تعدّ الدراسة مرجعًا هامًا في سياق البحث الحالي حول "دور الحكومات في مواجهة الإرهاب الإلكتروني"، حيث تعزز فهم العلاقة بين الجريمة السيبرانية والأمن السيبراني، وهذا يتماشى مع أهمية رؤية التهديدات المحتملة التي تواجهها الحكومة العراقية في سياق الإرهاب الإلكتروني. تنبثق مشكلة البحث عن الحاجة إلى استكشاف كيف يمكن للجرائم الإلكترونية أن تشكل تهديدًا للأمن القومي، وهو ما جرى طرحه في جوانب الدراسة السابقة.

ودراسة علي (2017): إشكاليات تداخل الصراعات السيبرانية والتقليدية التي تمثل إطارًا لفهم كيفية تداخل الإرهاب الإلكتروني مع الصراعات التقليدية في السياق العراقي، حيث أن العراق واجه صراعات عنيفة تقليدية ناتجة عن التوترات الداخلية والخارجية. يمكن عدّ الإرهاب الإلكتروني كأداة تضاف إلى أشكال الصراع التقليدية التي تعاني منها البلاد، مما يبرز الحاجة لدراسة دور الحكومة العراقية في التصدي لهذه الأنماط المتداخلة من الصراع. حيث يمكن تطبيق الأساليب والمستخلصات الخاصة بدراسة الصراعات على التعامل مع الإرهاب الإلكتروني.

دراسة عبد الصبور (2017) الصراع السيبراني طبيعة المفهوم وملامح الفاعلين، حيث تُعد الصراعات السيبرانية أحد الأبعاد المحورية لفهم كيفية تطور الإرهاب في العصر الرقمي. تُظهر الدراسة كيف أن الفاعلين في الصراع السيبراني، بما في ذلك الدول والجماعات الإرهابية، يمكنهم استخدام التكنولوجيا لتعزيز قوتهم وتأثيرهم. كما أن تحليل نجاح ونتائج هذه الصراعات يساهم في فهم كيفية استجابة الحكومة العراقية لتحديات الإرهاب الإلكتروني، مما يعكس ضرورة تطوير استراتيجيات شاملة تعكس تداخل الصراعات التقليدية والسيبرانية. على وجه الخصوص، يُظهر البحث كيف أن الفهم العميق لطبيعة الصراع السيبراني يمكن أن يُمكّن الحكومة العراقية من تصميم سياسات وتكتيكات مؤثرة لمكافحة أنشطة الإرهاب الإلكتروني.

وكشفت دراسة حسين (2017): فرص وقيود الأطراف المتنازعة على المجال العام السيبراني , إن توظيف المجال العام السيبراني يمثل أحد الأدوات الأساسية التي يمكن استخدامها من قبل الجماعات الإرهابية لنشر أفكارها، وتجميع الدعم. تظهر النتائج أن الرقابة أو التقييد الممارس من قبل الأنظمة السياسية على هذا المجال يمكن أن يؤثر في ديناميكيات الصراعات السياسية، وهذا ينطبق أيضًا على كيفية استجابة الحكومة العراقية للإرهاب الإلكتروني.

وبينت دراسة حرب الفضاء الالكتروني (التهديد التالي للأمن القومي و كيفية التعامل معه) ريتشارد كلارك, روبرت ديك ,2010) إبراز المخاطر المرتبطة بحروب الفضاء الإلكتروني وأهمية الوعي العام بها. إن التصدي للإرهاب الإلكتروني يتطلب أكثر من مجرد استراتيجيات حكومية؛ بل ينبغي أن يتضمن أيضًا نشر الوعي بين السكان المدنيين والشركات حول التهديدات الإلكترونية. وتشير دراسة الأمن السيبراني و الحرب السيبرانية (P.W Singer and Allan Friedman, 2014 إذ أن الهوة المعرفية بين الأجيال المختلفة في فهم الأمن السيبراني وأخطار الحرب السيبرانية تعكس تحديات إضافية تواجه الحكومات، بما في ذلك الحكومة العراقية، في استجابتها للتهديدات الرقمية. وأن الفجوة المعرفية بين القادة الذين نشأوا في عصر تقني حديث والمهاجرين الرقميين تسهم في توجيه استراتيجيات الأمن السيبراني. يحتاج القادة الحكوميون إلى تكوين فهم شامل للأدوات والتقنيات الرقمية من أجل اتخاذ قرارات مستنيرة تتعلق بمكافحة الإرهاب الإلكتروني. في حالة العراق، حيث تتقاطع التحديات التقليدية مع التهديدات السيبرانية، فإن الوعي بمستوى المعرفة التكنولوجية بين الجهات المسؤولة أمر بالغ الأهمية.

كما اظهرت الدراسة في هذا الجانب النتائج التي جرى التوصل إليها وفقًا للأسئلة المطروحة في مشكلة الدراسة وكالآتي:

- **نتائج السؤال الأول:** ما مراحل تطور الإرهاب الإلكتروني؟

يتضمن تطور الإرهاب الإلكتروني عدة مراحل، استنادا الى المبحث الاول بدءًا من استخدام الإنترنت كوسيلة للتواصل ونشر الأفكار، مرورًا بتطوير أساليب جديدة للهجوم، وانتهاءً بتعزيز الشراكات العابرة للحدود للإفادة من التكنولوجيا في تنفيذ عمليات إرهابية معقدة.

- نتائج السؤال الثاني: ما أبرز أساليب الجرائم الإلكترونية في الإرهاب الإلكتروني؟

النتيجة: تشمل أبرز أساليب الجرائم الإلكترونية: القرصنة، الهجمات الموزعة الحرمان من الخدمة تعدّ هجمات حجب الخدمة الموزعة DDoS (Distributed Denial of Service)، نوعًا جديدًا من هجمات حجب الخدمة العادية التي تعتمد على استخدام برامج معينة في الهجوم السيبراني وتستخدم ايضا البرمجيات الخبيثة للتجسس، والابتزاز الإلكتروني، كما جرى توضيحه في المبحث الثاني مما يساهم جميعه في تعزيز نشاطات الإرهاب الإلكتروني.

- **نتائج السؤال الثالث:** ما دور الجرائم الإلكترونية في انتقال الإرهاب العادي إلى الإرهاب الرقمي؟

لوحظ أن الجرائم الإلكترونية تسهم في انتقال الإرهاب العادي إلى الإرهاب الرقمي من خلال تمكين الجماعات الإرهابية من توسيع نطاق عملياتها واستراتيجياتها، مما يعزز من قدرتها على تنفيذ عمليات معقدة من مسافة بعيدة. تتوافق هذه النتيجة مع ما جرى ذكره في المبحث الثاني.

- نتائج السؤال الرابع: ما أهم السبل المتبعة من قبل الحكومة العراقية لمكافحة الإرهاب الإلكتروني؟

توصلت الدراسة إلى أن الحكومة العراقية تتبنى عدة سبل لمكافحة الإرهاب الإلكتروني، كما جرى تفصيله في المبحث الثالث منها تطوير تشريعات قانونية، التعاون مع الجهات الدولية والمحلية، وزيادة الاستثمار في تكنولوجيا المعلومات والاتصالات لتعزيز الأمن السيبراني.

نتائج السؤال الخامس: ما أهم وسائل خلق حالة من الوعي الأمني المعلوماتي القادرة على مكافحة الإرهاب الإلكتروني؟-

استنادا الى المبحث الثالث يتضح من النتائج أن خلق وعي أمني معلوماتي يتطلب تعزيز المناهج التعليمية، تنظيم ورش عمل للتوعية، وإشراك المجتمع المحلي في برامج توعوية حول مخاطر الإرهاب الإلكتروني وسبل مواجهته.

- **نتائج السؤال السادس:** ما الإجراءات المتخذة من قبل الحكومة العراقية في حماية بيانات المجتمع المعلوماتي العراقي؟

اتخذت الحكومة العراقية عدة إجراءات لحماية بيانات المجتمع المعلوماتي، منها صوغ سياسات وطنية للأمن السيبراني، إنشاء هيئات مختصة لمراقبة أمن المعلومات، وتنفيذ برامج تدريبية للكوادر الأمنية المختصة في هذا المجال, تتلاءم هذه النتيجة مع ما جرى استنباطه من المبحث الثالث.

تظهر النتائج في الخلاصة هنا أهمية التصدي لظاهرة الإرهاب الإلكتروني عبر استراتيجيات شاملة تتضمن قانونية، تقنية، وتوعوية، مما يسهم في توفير بيئة آمنة للمجتمع العراقي في ظل التحديات الرقمية المتزايدة.

الاستنتاجات

وبموجب ما تقدم في مباحث هذه الدراسة فقد جرى التوصل إلى الاستنتاجات الآتية:

1. أدت التحولات التكنولوجية الكبيرة التي عرفها العالم إلى إحداث تغيرات جذرية في حياة الشعوب والمجتمعات وخلفت أثارًا وانعكاسات كبرى.
2. أصبحت المعلومات والمعرفة مظهرًا ومؤشرًا ومصدرًا هامًا للقوة والأمن، فاستخدام هذه التكنولوجيا وشبكة الشبكات العنكبوتية لم يقتصر فقط على جانب إيجابي بل له مظاهر خطيرة سلبية أثرت في المجتمعات والدول، ومن بينها العراق.
3. سمح التطور التقني الذي شهده العالم إلى بروز فئات مختلفة، (أفراد، منظمات إجرامية وإرهابية) استغلت هذا التطور سلبيًا عبر مجموعة من الجرائم المستحدثة التي تعتمد على أساليب متطورة، كان من أبرزها الإرهاب الإلكتروني الذي ظهر نتيجة تزايد وتصاعد استغلال الجماعات الإرهابية للتكنولوجيا الحديثة، الأمر الذي دفع الحكومة العراقية لاتباع مجموعة من الإجراءات الكفيلة لمكافحة هذا النوع من الإرهاب.

المصادر والمراجع

اباداي، م. (1987). *القاموس المحيط*. القاهرة: مؤسسة الرسالة.

بدوي، أ. (1993). *معجم مصطلحات العلوم الاجتماعية*. (ط2). بيروت: مكتبة لبنان.

البشرى، م. (2000). التحقيق فى جرائم الحاسب الالي والانترنيت. *المجلة العربية للدراسات الامنية*، 15(30)، 317-380.

البيطار، ل. (2014). ماذا يعني الأمن السيبراني؟. جريدة الأنباء الإلكترونية.

الجوهري، إ. (1979). *الصحاح تاج اللغة وصحاح العربية*. (ج1). بيروت: دار العلم للملايين.

حسين، ا. (2017). فرص وقيود الأطراف المتنازعة على المجال العام السيبراني. *مجلة السياسات الدولية*، 52(208)، 12.

دستور جمهورية العراق لعام 2005.

الدويك، ع. (2018). مستقبل الصراع السيبراني العالمي في القرن الـ 21. *مجلة السياسة الدولية*، 314، 30- 45.

سرور، أ. (2008). *المواجهة القانونية للإرهاب*. القاهرة: دار النهضة العربية.

شعيب، م.. (2004). *الإرهاب صناعة عالمية*. القاهرة: دار نهضة مصر للنشر والتوزيع.

الشمري، م. (2021). الأمن السيبراني وأثره في الأمن الوطني العراقي. *مجلة العلوم القانونية والسياسية، جامعة ديالى*، 10(1).

شوقي، إ. (2015). الحرب السيبرانية: حرب المستقبل المفزعة. شبكة الاخبار العربية. 19 شباط.

عبد الرضا، ا.، والمعدومي، ع. (2020). الأمن السيبراني ودوره في انتشار الإرهاب في العراق بعد عام 2003. *مجلة دراسات دولية، جامعة بغداد*، 80.

عبد الصبور، س. (2017). الصراع السيبراني: طبيعة المفهوم وملامح الفاعلين. *مجلة السياسة الدولية*، 52(، 5-10.

عبيدات، خ. (2006). *الإرهاب يسيطر على العالم دراسة موضوعية سياسية علمية نافذة غير منحازة*. عمان: المطابع العسكرية.

عطية، أ. (1975). *القاموس السياسي*. (ط2). القاهرة: دار النهضة العربية.

علي، خ. (2017). إشكاليات تداخل الصراعات السيبرانية والتقليدية. مجلة السياسة الدولية، 208.

كلارك، ر.، روبرت، ن. (2010). *حرب الفضاء الالكتروني والتهديد التالي للامن القومي و كيفية التعامل معه*. أبو ظبي: مركز الامارات للدراسات والبحوث الاستراتجية.

مركز الامارات للدراسات والبحوث الاستراتيجية. (2014). *الحروب المستقبلية في القرن الحادي و العشرين*. ابو ظبي: مركز الامارات للدراسات والبحوث الاستراتيجية.

مسلم، نبراس إبراهيم. (2021). الجرائم السيبرانية وأثرها في الأمن السيبراني. *مجلة القادسية للقانون والعلوم السياسية*، 1(12).

مصطفى، عدنان ياسين واخرون. (2015). تحولات المجتمع العراقي بعد الغزو2003. بحث القي في مؤتمر دولي نشر في كتاب (سنوات هزت العالم). قطر: المركز العربي للأبحاث ودراسة السياسات.

وثيقة قانون جهاز مكافحة الارهاب لسنة 2005.

وثيقة قانون مكافحة الإرهاب العراقي رقم 13 لسنة 2005.

وثيقة مشروع قانون الجريمة المعلوماتية لعام 2018.

References

Abaday, M. (1987). *The perimeter dictionary*. Cairo. Al-Raha Foundation.

Badawi, A. (1993). *A lexicon of social science terminology*. (2nd ed.). Beirut: Lebanon Library.

Al-Bushrah, M. (2000). Investigation of Computer and Internet Crimes. *Arab Journal of Security Studies*,15(30), 317-380.

Bitar, L. (2014). What does cybersecurity mean? Electronic News Newspaper.

Al-Jawhari, I. (1979). *Health is the crown of Arabic and Arabic*. (1st ed.). Beirut: Dar al-Alam for millions.

Hussein, E. (2017). The opportunities and limitations of disputing parties to the cyberspace. *Journal of International Politics*, 12(208), 52.

Constitution of the Republic of Iraq of 2005.

Doek, Ab. (2018). The future of global cybercrime in the 21st century. *Journal of International Politics*, 314, 30-45.

Srour, A. (2008). *Legal confrontation of terrorism*. Cairo: Arab Renaissance House.

Shoaib, M. (2004). *Terrorism is a global industry*. Cairo: Egypt's Renaissance House for Publishing and Distribution.

Al-Shamri, M. (2021). Cybersecurity and its impact on Iraq's national security. *Journal of Legal and Political Sciences, Diyala University*, 10 (1).

Shawqi, I. (2015). Cyberwarfare: The horrific war of the future. Arab News Network. 19 February.

Abdel Reza, A., & Al-Maadoumi, A. (2020). Cybersecurity and its role in the spread of terrorism in Iraq after 2003. *Journal of International Studies, University of Baghdad*, 80.

Abdul Sabor, S. (2017). Cyber conflict: the nature of the concept and the features of the actors. *International Policy Journal*, 52(208), 5-10.

Obeidat, Kh. (2006). *Terrorism dominates the world's impartial political and scientific substantive study*. Amman: Military Printers.

Attiya, A. (1975).*Political dictionary*. (2nd ed.). Cairo: Arab Renaissance House.

Ali, Kh. (2017). Problems of overlapping cyber and traditional conflicts. *Journal of International Politics*, 208.

Clark, R. & Robert, N. (2010). *Cyberwarfare and the next threat to national security and how to deal with it*. Abu Dhabi: Emirates Centre for Strategic Studies and Research.

Emirates Center for Strategic Studies and Research. (2014). Future wars in the 21st century. Abu Dhabi: UAE Center for Strategic Studies and Research.

Muslim, N. (2021). Cybercrime and its impact on cybersecurity. *Qadisiyah Journal of Law and Political science*, 1(12).

Mustafa, A.et.al. (2015). Transformations of Iraqi society after invasion 2003. Research at an international conference published in a book (Years Shaken the World). Arab Center for Research and Policy Study. Qatar.

Anti-Terrorism Authority Act 2005.

Iraqi Counter-Terrorism Act No. 13 of 2005.

Information Crime Bill Document 2018.

Aboud, S. (2012). An Overview of Cybercrime in Iraq**.** *The research bulletin jordan ACM. Jordan, Center of Innovations in Computing and Engineering Machinery*, 2(2).

Rosenzweig, P. (2013). *Cyber warfare how Conflicts in cyberspace are challenging America and changing the World*. Oxford: Praeger Security International.

Singer, P.W., & Allan, F. (2014). *Cybersecurity and cyberwar what everyone needs to know*. New York: Oxford University press.

Theohary, C. & John, W. (2013). Cyber warfare and Cyber terrorism: In Brief, Comparative Strategy, 12(2).

Valeriano, B., & Ryan C. Maness. (2014). The Dynamics of Cyber Conflict Between Rival Antagonists. Journal of Peace Research**.** 51(3).