E-ISSN : 2790-2404
P- ISSN 2070-9250
Qadaya siyasiyyat

Ministry of Higher Education
& Scientific Research
Al-Nahrain University
College of Political Science

وزارة التعليم العالي والبحث العلمي
جامعة النهرين
كلية العلوم السياسية

قضايا سياسية

Political Issues

مجلة فصلية محكمة

Arab Impact Factor
معامل التأثير العربي
2022:(2.11)
معامل تأثير (Arcif)
2022:(0.1712)

العدد ٧١
Issue 71

تشرين الاول - تشرين الثاني - كانون الاول / ٢٠٢٣
Oct. - Nov.- Dec. / 2023

جدول المحتويات

التسلسل	اسم البحث	رقم الصفحة
1	الصين و إدارة الصراع في القارة الآسيوية منذ عام 2011 م.م إياد مالك عبد المجيد أ.م.د عبد القادر دندن	1_ 12
2	ادارة المخاطر في استراتيجية الامن القومي الامريكي في الشرق الاوسط الباحث جمعة عادل علي فيحان	13_27
3	المقومات الجغرافية والسكانية وتأثيرها في قوة روسيا الاتحادية الباحثة حنين إبراهيم عبدالله ا.م.د احسان عدنان عبدالله	28_36
4	التوجهات المصرية لصياغة دور جديد في منطقة شرق المتوسط دموع قاسم كريم أ.م.د باقر جواد كاظم	37_49
5	صنع السياسة العامة في العراق بعد العام 2005 الباحث داخل عبد الحمزه هنين أ. د. فراس عبد الكريم البياتي	50_ 65
6	حراك تشرين الاجتماعي في لبنان وأثاره على الاستقرار وهشاشة الدولة م. م . سالي سعد محمد أ.د. أحمد عبد الله ناهي	66 _ 75
7	مرتكزات القوة الناعمة الإيرانية علياء حميد خيون أ.م.د نور عبدالاله عجرش	76_84
8	التكنولوجيا الخضراء وأهمية اعتمادها كسياسة عامة في العراق م.م علي عبد الرزاق شنشول	85_ 96
9	الحوار الوطني وتحويل النزاع في السودان بعد عام 2022 م.م. مصطفى صادق عواد	97_114
10	المعايير الدولية للحكم الصالح د. محمد عامر حسن	115 _ 126
11	الاستراتيجية الصينية لتحقيق أمن الطاقة أ.م.د الاء طالب خلف الباحث: محمد عبدالعزيز مقداد	127_138
12	الارهاب السيبراني وأثره على الأمن القومي "العراق إنموذجاً" م.م قمر ثامر صبري	139_ 147
13	التوصيف الجيواستراتيجي لدول شبه القارة الهندية م.م. نسرين سمير جبار	148_ 161
14	انعكاسات تطوير القوى الكبرى لأجيال الحروب الجديدة على العلاقات الدولية م.م نظير سامي عبد الواحد أ.م.د. عباس سعدون رفعت	162_ 171
15	دوافع التوجه التركي أزاء منطقة المشرق العربي الباحثة: نهى مثنى نجم الدين أ.د. محمد ياس خضير	172_188
16	مكافحة الفساد وآليات معالجته في العراق م.م سارة عبد زاير	189_ 204
17	جهاز مكافحة الارهاب ودوره في تحقيق الامن المستدام ودور الاستراتيجية الوطنية في بناء السلام في العراق م.م ضحى فيصل علي	205_217

18	الرقابة على اللامركزية الادارية في العراق بعد عام 2003 م.م عفاف ظافر هادي	232_218
19	السلوك السياسي للجماعة الإسلامية في مصر بعد عام 2011 م.م علياء محمد طارش	250_233
20	التنمية السياسيَّة في العراق مابعد عام 2003 م. م. محمد مجيد حسين	267_251
21	تجربة اقليم كردستان العراق التنموية م.م أسامة محمد صاحب	277_268
22	معضلة الأمن في منطقة الشرق الأوسط " دراسة في مضامين مكافحة الارهاب " م. م ليث علاء خضير	297_278
23	تطور الحرب الروسية الاوكرانية و أنعكاساتها على القارة الافريقية (نماذج مختارة) م.م. مناسك عبد الوهاب حكمت	314_298
24	معادلات الامن الإقليمي في منطقة الشرق الأوسط والتوجه نحو السلام م.م نبأ إحسان شريف	330_315
25	تحديات المشاركة الانتخابية للمرأة في العراق بعد عام 2005 م.م نور مشتاق حسن	345_331
26	دور النظم الادارية في السياسة المحلية (دراسة حالة العراق) م. م. نور موفق عبد الغني	361_346
27	سياسة تركيا الخارجية في ليبيا وتحدياتها (2011_ 2021) م.م هبه حميد شمخي الكناني	381-262
28	أثر الثقافة السياسية للأحزاب الكردية على الهوية الوطنية وانعكاساتها على بناء الدولة العراقية بعد الاحتلال الأمريكي 2003 م.م هدى عبد الحسين فياض	396-382
29	تطور الحروب واثرها على الامن الوطني للدول (الحرب الهجينة انموذجا) م.م. هناء رحيم زيدان	411-397
30	أثر الفساد السياسي على الأنتخابات بعد عام 2003 (أنتخابات 2021 أنموذجاً) م.م. هند احمد عبد	425-412
31	توحيد السياسات في المؤسسات الحكومية بعد العام (2014) في العراق (الذكاء الاصطناعي أنموذجاً) م.م. هند شاكر محمود	438-426
32	الصين ومستقبل الصراع في بحر الصين الجنوبي م.م حسين حسن عزيز أ.د هيثم كريم صيوان	455-439
33	الحزب الشيوعي الصيني في العصر الجديد م.م منار شاكر محمود	473-456

الارهاب السيبراني وأثره على الأمن القومي "العراق إنموذجاً"

The impact of cyber terrorism on the national security

" Iraq as a model"

م.م قمر ثامر صبري*

Qamar Thamer Sabri

- **الملخص:**

يعد الانتشار الواسع لخدمات الانترنت الذي نتج عن ثورة التكنولوجيا والمعلومات والاتصالات منذ الثمانينيات الى عصرنا الحالي، العمود الفقري للحياة العصرية لما له من فائدة كبيرة على كافة الاصعدة وما يوفره من تسهيلات في حياتنا، ولكن هنالك جانب آخر مظلم يتعلق بإستخدام الثورة المعرفية والانترنت والذي يتمثل بالاعمال الارهابية التخريبية واستخدام الوسائل التقنية بطرق غير مشروعة سواء على مستوى الافراد او الدول، وابرزها ما يعرف بـ"الارهاب السيبراني" الذي استغل الفضاء السيبراني واصبح مهدداً خطيراً لأمن الافراد والدول واستقرار أمنها القومي، من خلال اتباع اساليب الاختراق الحواسب وسرقة المعلومات منها، وبذلك شكل ازمة تفاقمت واصبح أمر مواجهتها والحد منها موضع إهتمام العديد من الدول والمنظمات الدولية من خلال تبني اجراءات وسياسيات وقوانين تتيح لها مواجهة هذا الخطر، والحث على التعاون الدولي والوطني لفهم آليات التعامل مع الارهاب الالكتروني ومواجهته بما يعرف "بـالامن السيبراني".

- **الكلمات المفتاحية :(الارهاب السيبراني، الارهاب الالكتروني، الامن القومي، الفضاء السيبراني،الامن السيبراني).**

- **Abstract:**

The wide spread of Internet services, which resulted from the revolution of technology, information and communication since the eighties to the present time, is the backbone of modern life because of its great benefit to all levels and the facilities it provides in our lives, but there is another dark side using the knowledge revolution and the Internet, which is represented by sabotage terrorist acts and the use of technical means in illegal ways, whether at the level of individuals or countries, most notably what is known as "cyberterrorism", that For the security of has exploited cyberspace and become a serious threat individuals and countries and the stability of their national security, by following methods of hacking computers and stealing information from them, and thus constitutes a crisis that has worsened and the matter of confronting and reducing it has become the subject of interest of many countries and international organizations by adopting procedures, policies and laws that allow them to confront this danger, and urging international and national cooperation to

* كلية العلوم السياسية - جامعة النهرين.Qamar.thamer96@gmail.com

understand the mechanisms for dealing with electronic terrorism and confronting it with what is known as "cybersecurity" .

- **Key Words:(Cyber terrorism, electronic terrorism, national security, cyberspace, cyber security).**

المقدمة:

يمثل الإرهاب بجميع أشكاله تهديداً للأمن القومي للدولة، لما له من تأثيرات كبيرة على أمن المواطنين واستقرارهم وتأثيره على أمن الدولة وسيادتها في محيطها الإقليمي والدولي، ومع تطور العلم وتوالي الاختراعات التي ابتكرها العقل البشري وظهور التكنولوجيا معبراً عنها بالتقنيات الحديثة التي اعتبرت أحد العوامل الاستراتيجية التي تمكن التنظيمات الإرهابية من استخدام الإنترنت استخداماً متزايداً في مجموعة متنوعة وواسعة من الأغراض مثل (التجنيد، التمويل من خلال عمليات غسيل الأموال، التحريض على ارتكاب أعمال إرهابية، جمع المعلومات .. ألخ) والتي اعتبرت مهدداً خطيراً لامن الدولة على الصعيد القومي والدولي، ومن هنا ظهر مصطلح الإرهاب السيبراني أو الإرهاب الإلكتروني الذي يمثل شكلاً جديداً من أشكال الإرهاب ويعتقد الخبراء أن الإرهاب السيبراني أكثر ضراراً من الإرهاب التقليدي إذ يكمن الخطر في حقيقة أن الإرهاب الإلكتروني يمكنه أن يستهدف البنية التحتية المتعلقة في السجلات الحكومية ومراقبة الحركة الجوية والسيطرة على السدود والسجلات الطبية وكذلك البنية التحتية المالية والتجارية.

- **أهمية البحث :**يستمد البحث أهميته من أهمية الإرهاب السيبراني المعتمد في أنشطته على التكنولوجيا وبذلك اصبح يشكل خطراً وتهديداً على الأمن القومي للدول بنحو يجعل أي عمل إرهابي في ظل هذا المفهوم يخلف دماراً للأمن القومي المتكون من عدة أجهزة فعالة داخل الدولة تعمل على التصدي لهذه الهجمات الإلكترونية.
- **هدف البحث:** يهدف البحث إلى بيان ماهية الإرهاب السيبراني وأهم أنواعه وآليات عمله وبيان مدى تأثيره على الأمن القومي للدول بدراسة حالة تأثيره على الأمن القومي لدولة العراق.
- **مشكلة البحث:** أصبحت ظاهرة الإرهاب السيبراني مشكلة في اغلب الدول لماتسبب به من تأثير على الأمن القومي لدول العالم وما شكله من خطر عليها، من هنا يثار لدينا تساؤل أساسي وهو كيف يؤثر الإرهاب السيبراني على الأمن القومي للدول؟ وما مدى استجابة الدول هذا التأثير؟ الذي يمكن فهمه من خلال الإجابة عن التساؤلات الفرعية التالية:

1- ما هو مفهوم الإرهاب السيبراني؟ وما هي طرائق استخدام الإرهاب السيبراني؟

2- ما هي دوافع ارتكاب الإرهاب السيبراني؟

3- ما مدى تأثير الإرهاب السيبراني على الأمن القومي؟

4- ما هي سبل مواجهة الإرهاب السيبراني دولياً؟

5- كيف أثر الإرهاب السيبراني على الأمن القومي لدولة العراق؟

- **فرضية البحث:** يهدف البحث إلى اختبار ومعرفة صحة الفرضية التالية وهي، ظهور الإرهاب السيبراني وتزايد التعامل به نتج عنه تهديد وخطر أثر سلبياً على الأمن القومي للدولة أي أن العلاقة عكسية بين التعامل بالارهاب السيبراني واستقرار الأمن القومي للدول.
- **الاطار المنهجي للبحث :** طبقاً لبحثنا هذا سنقوم بإستخدام المنهج الوصفي التحليلي لغرض شرح ماهية الارهاب السيبراني وتحليل دوافعه واسباب ارتكابه وتحليل مدى تأثيره على الامن القومي مع دراسة حالة العراق كنموذج للبحث.

اولاً : الإطار المفاهيمي

شكل الإرهاب السيبراني نوعاً من النزاعات السيبرانية حمل معه مشاكل و تعقيدات النشاطات الإنسانية الى الفضاء السيبراني حتى سمي عصرنا الحالي بـ"عصر الفضاء الإلكتروني" لكون الإنترنت هو العمود الفقري لكل الأنشطة في الحياة اليومية سواء على مستوى الجماعات أو الأفراد وحتى الحكومات وذلك نتيجة الاعتماد على الذكاء الاصطناعي، وقد وظف إرهابيو الانترنت الوسائل التقنية الحديثة لخدمة أعمالهم التخريبية وتحقيق أهدافهم حيث اصبح الإنترنت وسيلة مهمة لممارسة هذه الأنشطة المتطرفة غير المشروعة، لتوضيح ذلك سنتطرق إلى مفهوم الإرهاب السيبراني و أنواعه و الطرائق المستخدمة فيه وأسباب ظهوره.

1- مفهوم الإرهاب السيبراني (Cyber terrorism)

أول شخص صاغ مصطلح الإرهاب السيبراني هو (Barry Colin)* في فترة الثمانينيات والتي اكد فيها إلى صعوبة ايجاد تعريف شامل للإرهاب التكنولوجي ولكنه تبنى تعريف للإرهاب الإلكتروني مقتضاه بأنه "هجمه إلكترونية غرضها تهديد الحكومات أو العدوان عليها سعياً لتحقيق أهداف سياسية أو دينية أو أيديولوجية وأن الهجمة يجب أن تكون ذات أثر مدمر وتخريبي مكافئ للأفعال المادية للارهاب"[1].

وعرفه (Dorothy Dennningg) "الهجوم القائم على مهاجمة الحاسوب وأن التهديد به يهدف إلى الترويع او إجبار الحكومات أو المجتمعات لتحقيق أهداف سياسية أو دينية أو عقائدية وينبغي أن يكون الهجوم مرمراً وتخريباً لتوليد الخوف، بحيث يكون مشابه للأفعال المادية للإرهاب"[2].

2- طرائق استخدام الارهاب السيبراني [3] :-

أ- الاستخدام المباشر للانترنت : ويشمل (التهديد السيبراني، حرمان الخدمة، تدمير الأنظمة والبيانات والمعلومات، إنشاء مواقع عبر الإنترنت، الدعاية لأغراض التجنيد و التحريض والحث على التطرف، التمويل، التدريب ،التخطيط والتنفيذ).

---

* Barry Colin: باحث في معهد الامن والاستخبارات في كاليفورنا ، فترة الثمانينيات

(1) محمود المراغي، تقرير امريكي عن حالة الارهاب في العالم، مجلة السياسية الدولية، العدد3، مؤسسة الاهرام، القاهرة، تشرين الاول 2001،ص2.

(2) الارهاب الالكتروني – Cyber Terrorism، الموسوعة السياسية، على الرابط: (political-encyclopedia.org) .

(3) نسرين الصباحي، الحروب السيبرانية وتحديات الامن العالمي، المركز العربي للبحوث والدراسات، 2017/12/26، متاح على الرابط: المركز العربي للبحوث والدراسات: الحروب السيبرانية وتحديات الامن العالمي (acrseg.org).

ب- الاستخدام غير المباشر للانترنت: وتشمل (الاتصالات، الخدمات اللوجستية وإدارة العمليات التقليدية).

3- اسباب الارهاب السيبراني

أ- **الاسباب السياسية**: أن الدافع السياسي من أهم الأسباب المحفزة على الإرهاب التكنولوجي وذلك بسبب ممارسة السلطة السياسية من قبل شخص واحد وتغييب الكثير عن المشاركة السياسية وغياب حرية التعبير عن الرأي، من شأنه أن يولد تشكيل حركات ومنظمات سرية وردود أفعال غاضبة بإستخدام أساليب شتى منها الإرهاب السيبراني ومن الأسباب السياسية هي النزاعات القائمة بين دولتين غالباً ما تؤدي إلى تبادل العمليات الإرهابية السيبرانية بينها وكذلك دوافع على الجماعات المتطرفة التكفيرية بنشر مبادئهم على نطاق أوسع وتحقيق مطامع استعمارية باتباع هذا الأسلوب كوسيلة فعالة لتحقيق الهدف[1].

ب- **الاسباب الاقتصادية**: يعد الاقتصاد المحور الأساس في البيئة الدولية كونه القوة الرئيسة في تحديد انماط التفاعلات وتوزيع مراكز القوى والتأثير على التوازنات الدولية وأن التفاوت في توزيع الموارد الاقتصادية سواء بين الدول أو بين أفراد الدولة الواحدة، تولد معاناة لدى الأفراد مسببة مشاكل اقتصادية تتعلق بالفقر والبطالة كل هذه العوامل التي تولد روح التذمر ودفع الأفراد والجماعات للجوء إلى وسائل الإرهاب سواء من خلال الانضمام إلى الجماعات الارهابية أو ارتكاب جريمة تندرج ضمن الإرهاب السيبراني[2].

ت- أسباب تتعلق بالميزات التي تقدمها التكنولوجيا والآليات الحديثة ويمكن تشخيصها بالآتي[3]:

- انخفاض تكلفة الآليات الإلكترونية مقارنة مع الأدوات التقليدية التي تهتم بها العمليات الارهابية.
- غياب الحدود الجغرافية والحواجز المكانية في الفضاء الإلكتروني.
- قابلية بنية الشبكات المعلوماتية للاختراق يوفر سبيل مهاجمتها لتحقيق اهداف الإرهاب الإلكتروني، فقد تقوم الجماعات الارهابية بمهاجمة الحاسوب الآلي الخاص بالحكومات أو الشركات الخاصة أو الأفراد.
- غياب السيطرة والرقابة على الشبكات المعلوماتية.

ثانياً: تأثير الارهاب السيبراني على الامن القومي للدولة و سبل مواجهته دولياً

يشهد المجتمع الدولي في عصرنا الحالي العديد من التغيرات الناتجة عن معطيات الثورة التكنولوجية، وقد نقلت هذه الثورة المجتمعات التقليدية إلى مجتمعات حديثة وذكيه وهو ما نعيشه اليوم في ظل ظاهرة الفضاء السيبراني ويتضمن هذا الفضاء كثيراً من الإيجابيات والسلبيات، من ناحية الإيجابيات نجد بأنه قد اسهم بصورة كبيرة في تسهيل الحياة اليومية على كافة الأصعدة خاصة في مجال الاتصال ومعرفة الأخبار، اما سلبيات فإنه أصبح مجال للصراع والقيام بأعمال غير مشروعة تهدد الأمن القومي البلدان.

1- **تأثير الارهاب السيبراني على الأمن القومي**: شكل الإرهاب السيبراني تهديداً مباشراً لأمن الدولة وتمثل هذا التهديد بأشكال عدة، فمن حيث تغير طبيعة خصائص الإرهاب السيبراني من ناحية الآليات وقوة التأثير ادى إلى ضرورة إيجاد وسائل أمنية وطنية جديدة من أجل مواجهة هذا النوع من الإرهاب

---

(1) غريب حكيم، الارهاب السيبراني والامن الدولي: التهديدات العالمية الجديدة واساليب مواجهتها، المجلة الجزائرية للدراسات السياسية، المدرسة الوطنية العليا للعلوم السياسية، بن عنكون-الجزائر، المجلد5-العدد2، كانون الاول 2018.، ص120.

(2) غريب حكيم، المصدر السابق نفسه، ص123.

(3) استخدام الانترنت في اغراض ارهابية، مكتب الامم المتحدة المعني بالمخدرات في فيينا، الامم المتحدة ،ص3.

وأصبحت الدولة بحاجة إلى ما يسمى (الأمن السيبراني)* ، مع تزايد العلاقة بين الأمن والتكنولوجيا وهذا يؤثر اقتصاديا على الدولة لأن الأمن السيبراني يحتاج إلى زيادة أنفاق الدولة على سياسات الدفاع الإلكتروني وحماية شبكتها الوطنية من خطر التهديدات وبناء مؤسسات وطنية للحماية الإلكترونية[1]، وكذلك يؤثر الإرهاب السيبراني على سيادة الدول لانه يعرض الأمن القومي إلى خطر التهديد الذي يعنى بحماية قيم المجتمع الأساسية وإبعاد مصادر التهديد عنها لكون الإرهاب السيبراني يتميز بالتفوق التكنولوجي والقدرة على تنفيذ العمليات الإرهابية غير المشروعة في الأرض والبحر والجو معتمدا على نظام التحكم عن بعد والسيطرة التكنولوجية المتطورة، ومن أمثلة ذلك نشر المعلومات المظلة والتأثير على توجهات الرأي العام داخل الدولة وعمليات تستهدف المعنويات "الحرب النفسية" وعمليات القرصنة[2]، وهناك وجه آخر لتأثير الإرهاب السيبراني على أمن الدولة تتمثل في ظهور انماط جديدة من الصراع ولكون الفضاء الإلكتروني هو مجال تنشأ فيه النزاعات بين الفواعل المختلفة تعبيرا عن تضاد مصالحهم وتعارض القيم سواء أن كانت هذه الفواعل المتنازعة داخل الدولة نفسها أو خارجية بين دولتين، ولكون الفضاء الإلكتروني عابرا للحدود اتسعت دائرة الصراعات السيبرانية وازداد عدد ارهابيو الإنترنت لدرجة قد يصعب السيطرة عليها والتصدي لها[3].

2- مواجهة الارهاب السيبراني دولياً

عملت الدول بالتعاون مع المنظمات الدولية لمواجهة الإرهاب بصفة عامة و الإرهاب السيبراني بصفة خاصة وعقدة العديد من الاتفاقيات والمعاهدات التي تهتم بتسليم المطلوبين وتقديم المشورة القانونية والتعاون في تنفيذ الأحكام، سنتطرق الى أهم الدول والمنظمات التي تصدت للارهاب السيبراني هي:-

أ- "دولة المانيا لها دور حيوي في مجال الحد من مكافحة الإرهاب الإلكتروني ووفقا لقرار أصدره القضاء الألماني في 30 أيار 2018 تستطيع بموجبه أجهزة الاستخبارات الألمانية الاستمرار في التجسس على كبار مزودي خدمة الانترنت لدواعي حماية الأمن القومي الألماني وذكرت المحكمة الفدرالية الإدارية في بيان أنها رفضت اعتراض شركة دو - سيكس الألمانية التي كانت تحتاج إلى شرعية الرقابة التي تمارسها عليها منذ سنوات أجهزة الاستخبارات الخارجية"[4].

ب- "المملكة العربية السعودية في تشرين الاول 2017 صدر الأمر الملكي السامي بإنشاء هيئة الأمن السيبراني لتؤكد اسرار المملكة على كتابة تاريخ جديد وملهم تتم صناعته للأجيال السعودية القادمة وفي 18 كانون الاول 2017 عقدت الورشة التحضرية الأولى للاتحاد السعودي للأمن السيبراني والبرمجة، بهدف استقصاء آراء والمقترحات المتخصصين السعوديين في استشراف مستقبل الاتحاد وتأسيس المعالم الرئيسية لانطلاق الاتحاد بحيث شهد عام 2018 الانطلاقة الحقيقية للاتحاد من أجل العمل على تعزيز حماية الشبكات وأنظمة تقنية المعلومات و أنظمة التقنيات التشغيلية و مكوناتها من أجهزة وبرمجيات وما تقدمه من خدمات وما تحوي من بيانات مع مراعاة الأهمية الحيوية المتزايدة

* الأمن السيبراني: هو عملية حماية الأنظمة والشبكات والبرامج ضد الهجمات الرقمية، التي تهدف الى الوصول للمعلومات الحساسة او تغييرها او تدميرها لغرض الاستيلاء على المال من المستخدمين او مقاطعة عمليات الاعمال العادية.

[1] طالب جبار حسن وزينب كاطع ناهض، الارهاب الالكتروني اسبابه وطرق علاجه، مركز البيان للدراسات والتخطيط، بغداد، 2019، ص11.

[2] Abdulrahman Alqahtani, The Potential Impact of Cyberterrorism on National Security, University of hull, 2012, p20.

[3] طالب جبار وزينب كاطع ناهض، مصدر سبق ذكره، ص16.

[4] راجي يوسف محمود البياتي، الارهاب السيبراني (نماذج من الجهود الدولية للحد منه)، كلية القانون والعلوم السياسية، جامعة كركوك، 2022، ص24.

للأمن السيبراني في حياة المجتمعات في سبيل التأسيس لصناعة وطنية في مجال الأمن السيبراني تحقق للمملكة العربية السعودية الريادة في هذا المجال"[1].

ت ـ الأمم المتحدة (United Nations) : عملت الأمم المتحدة بالتنسيق مع دولها الأعضاء على مواجهة خطر الإرهاب السيبراني من خلال أجهزة عدة، متمثلة بمركز الأمم المتحدة لمكافحة الإرهاب (UN counter terrorism center) ويعمل المركز على تعزيز التعاون الدولي لمكافحة الإرهاب ويدعم الدول الأعضاء في تنفيذ الاستراتيجية العالمية لمكافحة الإرهاب وهنالك فرقة تابعة للأمم المتحدة المعنية بمكافحة الإرهاب منها فرقة العمل المعنية بتنفيذ تدابير مكافحة الإرهاب التابع الأمين العام التي تهدف إلى مكافحة استخدام الإنترنت لأغراض إرهابية وكذلك يشارك مكتب الأمم المتحدة المعني بالمخدرات والجريمة (United Nations office on drugs and crime) بصفته كيانا رئيسيا من كيانات الأمم المتحدة المعنية بتقديم المساعدات القانونية في مجال مكافحة الإرهاب والمساعدة التقنية ذات الصلة ويعد الاتحاد الدولي للاتصالات هيئة مسؤولة عن متابعة مكافحة الإرهاب السيبراني[2].

ث ـ الانتربول منظمة الشرطة الجنائية (Organization International Criminal Police): تهتم الانتربول في مواجهة الجرائم الإلكترونية سيما الإرهاب السيبراني كما أنه هذه المنظمة تعمل على متابعة وتحليل وسائل التواصل الاجتماعي للوصول إلى البيانات والأدلة التي تدين الإرهابيين وتدل على أماكن تواجدهم لتسهيل الوصول إليهم ومنع هذه العمليات الإرهابية سواء التي تتم على أرض الواقع او عبر الإنترنت[3].

ح ـ المجلس الأوروبي لمكافحة الإرهاب: اهتم المجلس بمكافحة الإرهاب السيبراني بشكل متعدد الأطراف وتناول قضية الاستخدام الارهابي للإنترنت حيث تمت صياغة اتفاقية الجريمة السيبرانية (convention on cyber-crime)* وقد تم اعتمادها في اجتماع اللجنة الوزارية للمجلس في تشرين الثاني عام 2001 لاتخاذ تدابير فعاله في التعاون الدولي ضد الجرائم السيبرانية[4].

خ ـ منظمة الدول الامريكية (Organization of American states) :عقدت لجنة مكافحة الإرهاب في نيويورك اجتماع استثنائي في 6 آذار 2003 تعهدت بموجبه المنظمات في جميع الدول وخصوصا منظمة الدول الأمريكية ان تقاسم خبرتها في إطار التعاون الإقليمي لمكافحة الأنشطة الإرهابية السيبرانية وزيادة الوعي في مكافحة الإرهاب السيبراني على الصعيدين الدولي والإقليمي وذلك بالتعاون مع منظمة الطيران المدني والمنظمات الدولية، الشرطة الجنائية والمنظمة البحرية الدولية[5].

ثالثاً: تأثير الارهاب السيبراني على الامن القومي العراقي

---

[1] راجي يوسف محمود البياتي، مصدر سبق ذكره، ص24-25.
[2] غريب حكيم، مصدر سبق ذكره، ص106.
[3] Gabriel Weimann, Cyberterrorism How Real Is the threat?, United States institute of peace, special report, December 2004, p9.
* إتفاقية الجريمة السيبرانية: وهي اتفاقية الجرائم الإلكترونية رقم 185 وقعت في بودابست، المجر، عام 2001 وتم خلالها تشكيل ملف استجابة العدالة الجنائية الدولية للجرائم الإلكترونية والأدلة الإلكترونية، https://rm.coe.int/special-edition-budapest-convention-en -2022/1680a6992.
[4] رانيا سليمان، فاتن فايز ونهى الدسوقي، سياسات مكافحة الإرهاب الإلكتروني .. مصر والسعودية نموذجاً، المركز العربي للبحوث والدراسات، 2020، متاح على الرابط: المركز العربي للبحوث والدراسات: سياسات مكافحة الإرهاب الإلكتروني .. مصر والسعودية نموذجاً(acrseg.org) .
[5] غريب حكيم، مصدر سبق ذكره ، ص22.

لا يقتصر الإرهاب السيبراني في العراق على صورة واحدة ومحددة، حيث يرى مختصون أن هذا النوع من الإرهاب يبدأ من الجرائم الإلكترونية التي تتم بإستخدام الإنترنت كنوافذ للتخطيط والتنفيذ وصولاً إلى جرائم الاتجار بالبشر عن طريق الإنترنت ثم تجارة المخدرات بإستخدام الشبكة المعلوماتية، وحتى إلى ارتكاب الجريمة المنظمة والقرصنة الإلكترونية، وانتحال صفة عن الأشخاص، وجرائم الإحتيال المالي إضافة إلى تزوير البيانات وهي من الجرائم السيبرانية الأكثر انتشاراً داخل العراق، واتخذ الإرهاب السيبراني داخل العراق أشكال عدة منها عمليات الإحتيال المالي والإختلاس المصرفي التي تعرض لها العديد من الأفراد بصورة يصعب السيطرة عليها والابتزاز والتشهير الإلكتروني بحسابات وهمية على مواقع التواصل الاجتماعي لأغراض ودوافع مادية مما تسبب بمشاكل اجتماعية كبيرة راح ضحيتها العديد من الأفراد سيما النساء[1]، وقد تعددت مخاطر الإرهاب السيبراني على الاقتصاد القومي ولكون الوجود الاقتصادي الرقمي للبلد يعتمد على الأداء الفعال للبنية التحتية الرقمية في الفضاء السيبراني فإن البلد يكون مترابط مع بلدان أخرى وجهات فاعلة في الفضاء السيبراني من خلال شبكات مترابطة للبنى التحتية المعلوماتية، وبالتالي فإن البلد معرض لمخاطر يمكن التنبؤ بها وأخرى لا يمكن التنبؤ بها مثل عمليات غسل الأموال، الجرائم المالية عبر الإنترنت وسرقة الأصول الفكرية..الخ، كل هذه العمليات لها أثر اقتصادي قد يكون الكفيل بتدمير أي دولة، وبهذا الصدد شرع البرلمان العراقي قانون الجرائم المعلوماتية بهدف توفير الحماية القانونية وإيجاد نظام عقابي لمرتكبي جرائم الحاسوب وشبكة المعلومات، حيث تبنى العراق استراتيجية الأمن السيبراني العراقي ووضع آليات فعالة للاستجابة لمثل هذه التهديدات إضافة إلى العمل على تشريعات شاملة لمكافحة الإرهاب السيبراني والتدابير المضادة لتحديد الجرائم السيبرانية، ولكن امكانيات الدولة العراقية في المجال السيبراني لا تزال ضعيفة وتحتاج الكثير من الجهد المعرفي والاداري والقانوني والتقني لتكون قادرة على التأثير في مجال الأمن السيبراني من جهة وقادرة على توفير حماية أمنية محكمة ضد التهديدات السيبرانية من جهة أخرى[2].

- **الخاتمة:**

تكمن خطورة الإرهاب السيبراني في اعتماده على التقنيات المتقدمة مثل أجهزة التنصت على شبكات الاتصال وبرمجيات التشفير وبرمجيات اختراق أنظمة أمن الشبكات والحاسبات كما أن الشبكة الآلية الواحدة قد تضم عشرات او مئات الآلاف أو ملايين الحواسيب أو الأجهزة المتصلة بالأنترنت التي يمكن استخدامها علشان هجمات متنوعة لأغراض إجرامية تخريب والإرهاب والتهديد والابتزاز وبما أن العصر الحاضر هو عصر رقمي تتحكم فيه تكنولوجيا المعرفة والمعلومات ووسائل الاتصالات فمن يمتلك المعرفة يتحكم في كل شيء وأصبح الفضاء السيبراني واقع والحروب السيبراني حقيقة والتي تعتبر الجيل الخامس من الحروب وأصبحت الرقم من هي الصياغة السائدة في العصر الحالي من النقود والحكومات وزيادة السيب رانيا واماسي براني ودبلوماسية سيبراني وكل شي يتعامل عبر الفضاء الإلكتروني وقد قامت العديد من الدول بوضع خطة واستراتيجيات لتجنب الوقوع في المخاطر تصيد الشبكة والجماعات الارهابية بما فيها دولة العراق التي وعلى الرغم من أن شغال الاجهزة والقوات الأمنية لمكافحة الإرهاب التقليدي على مر السنوات أولا أهمية لمكافحة الإرهاب السيبراني مستفيدة من الخبرات والتجارب التي مرت بها سابقا رغم ضعف البنية التحتية المعلوماتية ما زالت القوات الامنية تواصل تحقيق الانتصارات في التصدي ومكافحة الإرهاب.

---

[01] مستشارية الأمن الوطني امانة سر اللجنة الفنية العليا لإمن الاتصالات والمعلومات، استراتيجية المن السيبراني العراقي، ص3.

[02] باسم علي خريسان، الامن السيبراني في العراق قراءة في مؤشر الامن السيبراني العالمي 2020، مركز البيان للدراسات والتخطيط، بغداد، 2021، ص9-10.

- **الاستنتاجات:**

في ضوء ماتقدم نصل إلى جملة من الإستنتاجات أهمها :-

1- الإرهاب السيبراني من اخطر انواع الإرهاب خاصة وان ظاهرة الفضاء الإلكتروني اصبح لها دور استراتيجي في المجتمع الدولي على الصعيد الاقتصادي والسياسي والثقافي والأمني.
2- تستفيد الجماعات الارهابية من الثغرات التكنولوجية والأمنية لدولة معينة لشن الهجمات الإلكترونية الخبيثة.
3- ضعف وهشاشة البنية التحتية المعلوماتية في العراق يساعد على سهولة ارتكاب الجرائم الالكترونية.

- **التوصيات:**

نقترح جملة من التوصيات وهي:-

1- مواجهة الإرهاب الإلكتروني فكرياً من خلال الوصول إلى عقول الشباب ونشر الوعي بشأن خطورة هذا الموضوع.
2- غلق المواقع وصفحات والمنتديات التي تحرض على ارتكاب الجرائم إلكترونية.
3- تشريع قوانين مكافحة الجرائم الإلكترونية ووضع أحكام صارمة.
4- العمل على إجراء تعاون دولي مع الدول التي تعتبر إنموذجاً ناجحاً في الأمن السيبراني والتصدي للإرهاب السيبراني مثل دولة الإمارات العربية المتحدة.

- **Sources**

1- Mahmoud Al-Maraghi, American Report on the State of Terrorism in the World, Al-Siyasiya Al-Dawliya Magazine, Issue 3, Al-Ahram Foundation, Cairo, October 2001.

2- Electronic terrorism-Cyber Terrorism, the political encyclopedia, at the link: (political-encyclopedia.org).
3- Nisreen Al-Sabahi, Cyberwars and Global Security Challenges, Arab Center for Research and Studies, 12/26/2017, available at the link: Arab Center for Research and Studies: Cyberwars and Global Security Challenges (acrseg.org).
4- Gharib Hakim, Cyberterrorism and International Security: New Global Threats and Methods to Confront Them, Algerian Journal of Political Studies, Higher National School of Political Sciences, Ben Ankoun - Algeria, Volume 5 Issue 2, December 2018.
5- The Use of the Internet for Terrorist Purposes, United Nations Office on Drugs in Vienna, United Nations.
6- Talib Jabbar Hassan and Zainab Katea Nahed, Electronic terrorism, its causes and methods of treatment, Al-Bayan Center for Studies and Planning, Baghdad, 2019.
7- Raji Yousef Mahmoud Al-Bayati, Cyberterrorism (models of international efforts to reduce it), College of Law and Political

Science, University of Kirkuk, 2022.
8- Gabriel Weimann, Cyberterrorism How Real Is the threat?, United States institute of peace, special report, December 2004.

9- Abdulrahman Alqahtani, The Potential Impact of Cyberterrorism on National Security, University of hull, 2012.
10- Rania Suleiman, Faten Fayez and Noha El-Desouki, Policies to Combat Cyberterrorism... Egypt and Saudi Arabia as a Model, Arab Center for Research and Studies, 2020, available at the link: The Arab Center for Research and Studies: Policies to Combat Cyberterrorism ... Egypt and Saudi Arabia as a Model (acrseg.org).
11- National Security Advisory Secretariat of the Higher Technical Committee for Communications and Information Security, Iraqi Cybersecurity Strategy.
12- Bassem Ali Khreisan, Cybersecurity in Iraq, a reading of the Global Cybersecurity Index 2020, Al-Bayan Center for Studies and Planning, Baghdad, 2021.