مجلة تكريت للعلوم السياسية

**اسم المقال:** الأمن الوطني العراقي والتهديدات السيبرانية... الإرهاب السيبراني إنموذجاً
**اسم الكاتب:** م.د. شيماء تركان صالح
**رابط ثابت:** https://political-encyclopedia.org/index.php/library/7897
**تاريخ الاسترداد:** 2026/11/02 11:55 +03

الموسوعة السياسيّة هي مبادرة أكاديمية غير هادفة للربح، تساعد الباحثين والطلاب على الوصول واستخدام وبناء مجموعات أوسع من المحتوى العلمي العربي في مجال علم السياسة واستخدامها في الأرشيف الرقمي الموثوق به لإغناء المحتوى العربي على الإنترنت.
لمزيد من المعلومات حول الموسوعة السياسيّة - Encyclopedia Political، يرجى التواصل على info@political-encyclopedia.org

استخدامكم لأرشيف مكتبة الموسوعة السياسيّة - Encyclopedia Political يعني موافقتك على شروط وأحكام الاستخدام المتاحة على الموقع https://political-encyclopedia.org/terms-of-use

تم الحصول على هذا المقال من موقع مجلة تكريت للعلوم السياسية جامعة تكريت ورفده في مكتبة الموسوعة السياسيّة مستوفياً شروط حقوق الملكية الفكريّة ومتطلبات رخصة المشاع الإبداعي التي ينضوي المقال تحتها.

: https://doi.org/10.25130/tjfps.v4i33.279

TJFPS
ISSUE 33

IRAQI Academic Scientific Journals
العراقية المجلات الاكاديمية العلمية
ISSN: 2663-9203 (Electronic)
ISSN: 2312-6639 (print)

Contents lists available at:
http://tjfps.tu.edu.iq/index.php/poiltic
Tikrit Journal For Political Science

Tikrit Journal For Political Science
SINCE 2014

# الأمن الوطني العراقي والتهديدات السيبرانية... الإرهاب السيبراني إنموذجاً

# Iraqi National Security and Cyber Threats… Cyber terrorism as a model

Shaymaa Tarkan Salih [a]
Nahrain University-College of Political Science [a]

م.د. شيماء تركان صالح [a] *
جامعة النهرين/ كلية العلوم السياسية [a]

**A r t i c l e i n f o.**

**Article history:**
- Received 19 Sep. 2023
-Received in revised form 07 Oct. 2023
- Final Proofreading 01 Nov. 2023
- Accepted 18 Nov. 2023
- Available online 31 Dec. 2023

**Keywords:**
- Iraqi National Security
- Cyber
- Cyber Terrorism
- Cyber Security

©2023. THIS IS AN OPEN ACCESS ARTICLE UNDER THE CC BY LICENSE
http://creativecommons.org/licenses/by/4.0/

**Abstract:** The massive spread of the use of Internet networks in Iraq led to a (major revolution) that left its effects on all aspects of life, including the national security of the Iraqi state, which is now facing new challenges, represented by cyber threats. The technological development that Iraq witnessed in the field of information and communications during the second decade of the third millennium, which coincided with the weakness of securitization in the national infrastructure (security, banking, or personal), led to Iraq becoming exposed to threats in all its forms. It is noted that most Iraqi institutions contract to supply their information from satellites with a service resource located outside the Iraqi borders, which leads to the passage of that information in the servers of those countries, and its return to Iraq, and therefore this procedure constitutes a breach of the Iraqi information security.

*Corresponding Author: Shaymaa Tarkan Salih ,E-Mail: dr.shayma@nahrainuniv.edu.iq ,Tel: +9647700614375 , Affiliation: Nahrain University-College of Political Science.

**معلومات البحث :**

**تواريخ البحث:**
- الاستلام: 19 أيلول2023
-الاستلام بعد التنقيح 01 تشرين الأول 2023
- التدقيق اللغوي 01 تشرين الثاني 2023
- القبول: 18 تشرين الثاني 2023
- النشر المباشر: 31 كانون الأول 2023

**الكلمات المفتاحية :**
- الأمن الوطني العراقي.
- السيبرانية.
- الإرهاب السيبراني.
- الأمن السيبراني.

**الخلاصة** : أدى الانتشار الهائل في استعمال شبكات الانترنت في العراق إلى إحداث (ثورة كبرى) تركت تأثيراتها على جوانب الحياة كافة، ومن بينها الأمن الوطني للدولة العراقية الذي أصبح يواجه تحديات جديدة، تمثلت بالتهديدات السيبرانية. فالتطور التكنولوجي الذي شهده العراق في مجال المعلومات والاتصالات خلال العقد الثاني من الألفية الثالثة والذي تزامن مع ضعف الأمننة لدى البنية التحتية الوطنية (أمنية أو مصرفية أو شخصية) أدى إلى أن يصبح العراق منكشفاً أمام التهديدات بمختلف أشكالها. ومن الملاحظ إن أكثر المؤسسات العراقية تتعاقد لتجهيز معلوماتها من أقمار صناعية ذات مورد خدمة واقع خارج الحدود العراقية، الأمر الذي يؤدي إلى مرور تلك المعلومات في خوادم تلك الدول، ورجوعها إلى العراق، وبالتالي فإن هذا الإجراء يشكل خرقاً لأمن المعلومات العراقي. وعليه، لا بد لاستراتيجية الأمن السيبراني العراقي أن تنطلق من مبدأ أساس هو ضمان أمن العراق وحماية وجوده في الفضاء السيبراني، وحماية بنية معلوماته الحيوية، وبناء مجتمع انترنت موثوق به ورعايته والتعامل مع التحديات السيبرانية التي تهدد أمن العراق وسلامته، عن طريق تبني مجموعة من الإجراءات التي تعمل على حماية فضاء العراق السيبراني والدفاع عنه.

## المقدمة :

رتبّت المتغيرات الدولية المتدفقة منذ نهاية الحرب الباردة في العقد الأخير من القرن العشرين، ثم أحداث 11 أيلول 2001م، الكثير من التحديات، التي تعدّت حدودها الأدائية في الكشف عن مخاطرها، لاسيما بعد أن تتابعت الرؤى المولّدة لها مع حقائق التطور التكنولوجي التي ساهمت وبشكل مباشر في جعل تلك التحديات توزن بميزان التهديد المباشر، نظراً لتأثيراتها، لتدخل تلك التحديات، مرحلة جديدة وصفت بكونها سيبرانية بامتياز.

فثمة تهديدات سيبرانية وحروب سيبرانية لا تناظرية، ذات تكلفة متدنية تعطي للمهاجم أفضلية واضحة، نظراً لما تتميز به من سرعة ومرونة ومبادأة، وعدم جدوى اشتغال نظم الردع التقليدية حيالها. وهنا بدا (الإرهاب السيبراني) أكثر حدة وأقسى أثراً وأوسع انتشاراً من مثيله التقليدي. الأمر الذي صعّب من جهود التصدي لتهديداته الظاهرة والخفية.

لقد تزامن مع قدرة الإرهاب على التخفي زيادة قسوة الأثر التكنولوجي وتطوراته في سرعة انتشاره واختفاءه وانتقالاته السريعة في كل أرجاء المعمورة. ذلك الإرهاب الذي تحمل صناع القرار الاستراتيجيين

حسابه بأنماط تصدٍ مختلفة غلب عليها صفة الإدارة بالمخاطر، إلا أنه استدعى أيضاً ارتفاعاً في تلك الإدارة لصالح المواجهة الكلية لتتزاحم مع قدرة الإرهابيين على استغلال منظومات التحكم الآلي في تصديره، لا سيما في ظل سيادته في مجتمعات هشة يتعرض فيها الأمن الوطني إلى تحديات مقوّضة لوجود المجتمع والدولة معاً، كما هو الحال في العراق. إذ بدت قوى الإرهاب المختلفة فيه، تُجدد وسائلها باتجاه استيعاب التقنيات السيبرانية، حتى بدت أفعالها مزدوجة بين التقليدية على الأرض والتقنية عبر الفضاء الواسع، الأمر الذي أعطاها زخماً واسعاً، صار من الصعب الحد منها دون الارتفاع بموجبات القدرة الشاملة للتصدي لأفعاله وغزواته الإلكترونية، لا سيما في ظل القاعدة التقنية البسيطة في العراق، التي تم الانتباه إليها فعلياً بعد عام 2017م إذ تحرير الموصل من (داعش). تلك الموجبات التي حتمت التحقق من تطور العقيدة الاستراتيجية بما يجعلها متوائمة مع ما تتطلبه مواجهة ذلك الإرهاب من إدامة لدورة الاتصال والتواصل، بين القابليات والأفعال الميدانية والسيبرانية معاً.

**أهمية البحث:** تتأتى أهمية البحث من كون الإرهاب في العراق، لم يكن ليصف وضعه الحالي، لولا التكنولوجيا الرقمية التي حاولت قواه استيعابها ولتخوض عن عمد حرباً إلكترونية متعددة الفواعل والساحة والأنماط في آن واحد، جعل من الصعب مواجهتها واقعياً، تشترك جميعاً بوصفها القانوني كونها جرائم موصوفة يستغل مرتكبوها من الأفراد والجماعات الفضاء السيبراني للقيام بعمليات التجنيد والدعاية وجمع الأموال والمتطوعين، فضلاً عن جمع المعلومات حول الأهداف العسكرية بقصد تدميرها، الأمر الذي أعطاها زخماً قوياً لأفعاله وغاياته، لاسيما في ظل غياب الرقابة على أنظمة الاتصال المادية المتدفقة عبر العالم لا عبر العراق فحسب.

**إشكالية البحث:** حمل ويحمل الفضاء السيبراني تهديدات ومخاطر جمة على الأمن الوطني العراقي تمثل بالإرهاب السيبراني جنباً إلى جنب مع الإرهاب بشكله التقليدي، والذي تمثل بتنظيم (داعش) الإرهابي، من دون أن يتوفر غطاءً سياسياً ألكترونياً وطنياً أو حتى خريطة طريق لتأسيس بنية الكترونية فوقية للبلاد من أجل وضع العراق على قدم المساواة مع نظرائه الدوليين والإقليميين. لذا كان لزاماً على البحث الإجابة على الأسئلة الفرعية الآتية:

- ما المقصود بالأمن الوطني؟ وما المقصود بالسيبرانية والإرهاب السيبراني؟.

- متى انتشرت السيبرانية في العراق؟ متى ظهر الإرهاب السيبراني في العراق وما هي مظاهره؟.
- ما واقع الأمن السيبراني في العراق؟ وما هي مكامن الخلل في الأمن السيبراني العراقي؟.
- ما هي متطلبات استراتيجية مكافحة الإرهاب السيبراني في العراق؟.

**فرضية البحث:** دخلنا عالم الفضاء السيبراني وصار كل شيء يدار الكترونياً وعبر شاشات رقمية في الميادين كافة السياسية والاقتصادية والاجتماعية والعسكرية والأمنية، وهذا الفضاء ينطوي على مهددات جديدة تتمثل بسهولة توظيفه من أجل ضرب البنى التحتية الحيوية للدولة. لذا لا بد من توافر إدراك لدى الجميع وخاصة النخب الأمنية والعسكرية العراقية بأن هناك مهددات وحروب تتم في الفضاء السيبراني تستهدف شبكات الحوسبة التي توجه وتدير مؤسسات الدولة وبناها التحتية الحيوية المدنية والعسكرية. كما يتحتم على صانع القرار العراقي التحوط منها مستقبلاً من خلال الاتجاه لوضع استراتيجية تضمن الأمن السيبراني بعدّه من الأساسيات التي لا يمكن إغفالها إذا ما أراد الارتقاء بمستوى الأداء الاستراتيجي للدولة العراقية.

ومن أجل بناء رؤية تحليلية لانتشار آثار السيبرانية على الأمن الوطني العراقي ومن بينها الإرهاب السيبراني، سنقدم دراستنا هذه لملاحقة أصول هذا الإرهاب وغاياته ووسائله، وصولاً إلى رصف بعض المعالجات للتقليل من زخم تأثيره ضمن سياق استراتيجية مكافحة الإرهاب العراقية، وذلك وفق الهيكلية التي تتضمن ثلاثة مباحث، وهي على النحو الآتي:

- المبحث الأول: اطار مفاهيمي.
- المبحث الثاني: طبيعة التهديدات السيبرانية في العراق.
- المبحث الثالث: تحليل استراتيجية مكافحة الإرهاب السيبراني في العراق.

## المبحث الأول: اطار مفاهيمي

يتطلب التعامل مع العلوم الإنسانية ذات الظواهر المختلفة، تحديد المفاهيم المستعملة في الدراسة، وذلك بغية تحقيق هدفين. يتمثل الأول بتحقيق الاتفاق على مدلول محدد وشامل إزاء أي ظاهرة من ظواهر هذه العلوم. أما الهدف الثاني، فيتمثل في تأسيس مدخل فكري وتحديد الأسس النظرية التي يتم الانطلاق منها. وبقدر تعلق الأمر بموضوع بحثنا، فقد وجدنا أنه من المناسب أن يتم تحديد المقصود بالمفاهيم المستعملة فيه، وذلك من أجل تفادي الاختلاط والتداخل مع غيرها من المفاهيم الأخرى، ولاسيما تلك التي تبدو متقاربة أو متداخلة من بعضها أو المترادفة في أحيان أخرى، خاصة وأن درجة التقدم العلمي والحضاري لها دور في غاية الأهمية في تشكيل مدركات الباحثين وصنّاع القرار على حدٍ سواء وطرق إدراكهم لطبيعة وأسباب الظاهرة وكيفية تحقيقها. لذا سوف يتم تناول مضمون هذا المبحث عبر المطالب الثلاثة الآتية:

### المطلب الأول: تعريف الأمن الوطني ومفهومه

تلتقي أغلب وجهات النظر حول(الأمن، Security) عند قاسم مشترك هو إدراكها إن الأمن إن دل على شيء فإنما يدل على التحرر من الخوف[1]. وعلى الرغم من هذا الاتفاق إلا أن تعريف (الأمن) يواجه العديد من المصاعب المختلفة، وذلك لأنه يعّد ظاهرة اجتماعية نسبية ومتغيرة وتتداخل فيها مجموعة من العناصر والعوامل المختلفة، فضلاً عن حداثة دخوله قاموس المصطلحات السياسية والاجتماعية، ولتعرضه لتحديات متباينة، مباشرة وغير مباشرة، ومن مصادر مختلفة إرادية وغير إرادية[2]. ونظراً لارتباطه ببقاء الأفراد والشعوب والدول واستمرارها، فقد عّد مصطلح (الأمن) من أكثر المصطلحات السياسية إثارة للجدل، كما أنه من المفاهيم ذات الثراء اللغوي في المعنى، لذا تعددت تعريفاته من ناحية المضمون ومستوى التحليل والوسائل والأطراف المعنية به.

فمن الناحية اللغوية، فإن لفظة (الأمن) مشتقة من (الأمان) و(الأمانة). وتأتي كلمة (الأمن) في صيغ متعددة مثل: (أستأمن) و(الأمين). وقد وردت في لسان العرب، نقيضاً للخوف أي (الاطمئنان). وفي

---

[1] إبراهيم مصحب الدليمي، المخدرات والأمن القومي العربي: دراسة من منظار سوسيولوجي، دراسات استراتيجية، العدد (84)، 2003، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي – دولة الإمارات العربية المتحدة، ص56.

[2] علي عبد العزيز الياسري، الأمن القومي العراقي: الأبعاد الفكرية السياسية لاستراتيجية الأمن القومي في العراق، بلا دار نشر، بغداد – العراق، كانون الثاني 2010، ص56.

ضوء ذلك فإن (الأمن) يعني غياب العنف والمخاطر التي تهدد الشخص وحقوقه، أي عدم خوف الشخص من التعرض للإكراه أو الأذى الحسي وتوفير الطمأنينة والاستقرار[1]. وفي معاجم اللغة الإنكليزية، فإن كلمة (الأمن) تقابل كلمة (Security) التي تعني (الأمان، Safety) وهي عكس كلمة (الخوف، Fear). وفي قاموس (Webster's) فإن (الأمن) يعني التخلص من الخطر والخوف وعدم اليقين والعمل على توفير الطمأنينة والسلام[2].

وقد أوجبت جميع الأديان السماوية توفير الأمن للبشر، بعّده حاجة إنسانية، ولا يمكن للعنصر البشري أن يعيش بدونه. ففي القرآن الكريم ذُكرت ألفاظ (الأمن، والأمان، وأمنوا) في (390) موضعاً مما يدلل على أهميتها الاجتماعية في بناء الإنسان والمجتمع، كقوله تعالى(( وإذ جعلنا البيت مثابةً للناس وأمناً واتخذوا من مقام إبراهيم مصلى وعهدنا إلى إبراهيم وإسماعيل إن طهرا بيتي للطائفين والعاكفين والركع السجود))[3]، كما أن (الأمن) في القرآن الكريم هو نعمة من عند الله سبحانه وتعالى يمنُ بها على عباده الصالحين ويسحبها حين ينتقم منهم، كما أنه يوجب عليهم الشكر حين ينعمون بها[4]، وهو أمر واضح في قوله تعالى ((وعد الله الذين آمنوا منكم وعملوا الصالحات ليستخلفنهم في الأرض كما استخلف الذين من قبلهم وليمكنن لهم دينهم الذي ارتضى لهم وليبدلنهم من بعد خوفهم أمناً يعبدونني لا يشركون بي شيئاً ومن كفر بعد ذلك فأولئك هم الفاسقون))[5].

لقد صار للأمن مفهوماً مزدوجاً فهو لا يعني فقط وسيلة للتحرر من الخطر بل هو أيضاً وسيلة لإرغام الخطر على أن يكون محدوداً. وبما أن الأمن أوجده الخوف لذا فمن الضروري القيام بإجراءات مضادة للتحكم في الخوف وتحييده واحتوائه[6]. وبالتالي صار ينظر إلى الأمن بعدّه أمراً موضوعياً وذاتياً في آن واحد. فالأول يشير إلى واقع الحال، فيما إذا كان الشخص مهدداً فعلاً وتتوافر له الحماية الكافية، أما الآخر فيشير إلى تصور المرء عن الوضع ورغبته لا في التحرر من التهديد فحسب، بل في الشعور بالحرية

---

[1] فهد بن محمد الشقحاء، الأمن الوطني: تصور شامل، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض – السعودية، 2004، ص12.

[2] New Webester's Dictionary and the Source of English lang. Levicon Publishing inc, 1996, p.903

[3] القرآن الكريم، سورة البقرة، الآية (125).

[4] بشير الوندي، الأمن المفقود: دور الاستخبارات والتنمية في استتباب الأمن، دار الصفار، بيروت – لبنان، 2013، ص24.

[5] القرآن الكريم، سورة النور، الآية (55).

[6] بشير الوندي، مصدر سبق ذكره، ص28.

والرفاه[1]. وهنا يشير علماء الاجتماع، إلى أن الشعور بالخوف بحد ذاته واقع حيوي لتحقيق الأمن، وإن ردة فعل الخوف عند الإنسان تولد أحد نوعين من الأمن، فأما أمناً سلبياً ويعني قيام الإنسان باتقاء الشر، أو أمناً إيجابياً يتمثل في سعي المرء المستمر والمتواصل للحصول على حقوقه وتحسين أحواله وتأمين مستقبله وضمان كل ذلك. على أن الشكلان متصلان اتصالاً وثيقاً، فهما وجهان لعملة واحدة، وغايتهما واحدة هي العيش بسعادة وأمان وسلام[2].

ووفقاً لما تقدم، سارت كل النشاطات الإنسانية وفق منهج يؤكد أولوية الأمن وتقدمه على كل مطلب واحتياج آخر، ليصير هذا المطلب الجوهر الدائم للحياة، والمحور الذي تدور حوله أفكارها وأنشطتها، بحكم ضرورته وأولويته، إذ لا يعني الأمن حماية الحياة وضمان شروط ديمومتها فحسب، بل ويمثل أيضاً الشرط اللازم لتطورها وتقدمها، بما يوفر للفرد والمجتمع شروط الاستمرار والاستقرار اللازمة للإبداع وتداول المعرفة والخبرة وتطويرهما ومراكمتهما، والقدرة على التخطيط للمستقبل القريب والبعيد، وتلبية الاحتياجات، وتحقيق الأهداف، وهو الأمر الذي يبرر انشغال الإنسان الدائم بالأمن، نظرياً وعملياً، وفي كل زمان ومكان[3].

وانطلاقاً من أن الأمن حقيقة ملازمة للفرد كما هو الحال بالنسب للدولة، فإن كل ما قيل عن أمن الفرد، بعده أصغر وحدة تحليلية، يمكن أن ينطبق على أكبر وحدة تحليلية وهي الدولة في النظام الدولي. فيشير اصطلاح (الأمن الوطني/القومي)[4] إلى أمن الدولة داخلياً ودفع التهديدات الخارجية عنها، بما يكفل

---

[1] بول روبنسون، قاموس الأمن الدولي، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي – دولة الإمارات العربية المتحدة، 2009، ص269.

[2] هايل عبد المولى طشطوش، الأمن الوطني وعناصر قوة الدولة في ظل النظام العالمي الجديد، على الموقع الإلكتروني: iefpedia.com

[3] علي عباس مراد، الأمن والأمن القومي: مقاربات نظرية، أبن النديم للنشر والتوزيع ودار الروافد الثقافية – ناشرون، وهران – الجزائر، بيروت – لبنان، 2016، ص18.

[4] يستعمل بعض الباحثين مصطلح (الأمن القومي) ليعبر عن (الأمن الوطني)، استناداً إلى أن الأمن ارتبط بالدولة/الأمة التي نشأت في أوروبا في العصر الحديث خلال القرنين السادس عشر والسابع عشر الميلادي وأسست لها معاهدة ويستفاليا عام 1648م، إذ بدأت كلمة (Nationalism) تأخذ مكانها، وأخذ تطبيق القانون يعّد رقّي وحضارة، فظهرت مصطلحات كثيرة ترجمت تلك المشاعر القومية ومنها الأمن الوطني/القومي، الذي يقصد به أمن الدولة الوطنية/القومية. حيث لا تناقض بين الوطنية والقومية فالدولة قد تضم ضمن حدودها معظم الأمة. وبالتالي فإن الأمن قد يكون وطنياً يرتبط بإقليم الدولة أو قومياً يرتبط بالجماعة أو الأمة التي قد تكون متحدة في دولة واحدة كالأمة الفرنسية أو الانكليزية، أو قد تكون مجزأة كالأمة العربية. وهناك من الباحثين من لا يرى فرقاً بين المصطلحين ويستعملهما كمترادفين، إذ يقرون بواقع نسبة القومي إلى القوم (الجماعة) والوطني إلى الأرض، ولا يرون فرقاً أو عدم دقة في اطلاق لفظ (القومي) على ما هو من الأمة، وعلى ما هو وطني من الأرض، ما دام مفهوم الأمن القومي لديه لا يتعلق بعدد الدول التي تشترك فيه، ولكن يتعلق بالمجالات التي يهتم بها. كما أن تبني مفهوم الأمن القومي أو الأمن الوطني ينبع من ثقافة البيئة المجتمعية التي تعالج المفهوم

حياة مستقرة. وقد وردت الكثير من التعريفات الخاصة بمصطلح الأمن الوطني في أدبيات العلوم السياسية، يمكن أن نورد بعضاً منها. فقد عُرف من قبل مجموعة من خبراء الأمم المتحدة، على أنه (حالة ترى فيها الدولة على أنه ليس ثمة خطر في هجوم عسكري أو ضغط سياسي أو إجبار اقتصادي مما يمكنها من المضي بحرية في تنميتها الذاتية)[1]. كما عُرف من قبل دائرة المعارف البريطانية على أنه (حماية الأمة من خطر القهر على يد قوة أجنبية)[2]، وعرفه (باري بوزان، Barry Buzan) على أنه (عدم تعرض حرية الدول للتهديد)، وعرفه مستشار الأمن القومي الأمريكي(هنري كيسنجر، Henry Alfred Kissinger) على أنه (أي تصرف يسعى المجتمع عن طريقه لتحقيق حقه في البقاء)[3].

ويستدل من التعريفات أعلاه، بأن الأمن الوطني هو قدرة الدولة على رد أي عدوان قد تتعرض له من قبل دولة أخرى، سواء باستعمال الدفاع العسكري أو أي أسلوب آخر يساهم في المحافظة على توفير الأمن الخارجي والداخلي للدولة دون وجود أي سيطرة أو سلطة من دولة أو أي جهة أخرى. بمعنى آخر، يشير الأمن الوطني إلى قدرة الدولة على حماية أراضيها وشعبها ومصالحها وعقائدها وثقافتها واقتصادها من أي عدوان خارجي فضلاً عن قدرتها للتصدي لكل المشاكل الداخلية، والعمل على حلها واتباع سياسة متوازنة تمنع الاستقطاب وتزيد من وحدة الكلمة وتجذير الولاء والانتماء للوطن والقيادة[4]. تلك المهام، التي تولت تحقيقها الدول كمعطى وكوجود، كونها ظلت، حسب الطبيعة النهائية لسلطتها، الجهة الرئيسة والفاعلة في

---

سواءً كانت بيئة غربية أو عربية أو شرقية، إذ إن جوهر الأمن يرتبط بالمصلحة وطريقة تحقيقها داخلياً وخارجياً، ومن ثم فإن تبني المفهوم يتوافق مع تحقيق المصلحة العليا للبلاد وفق الفكر الاستراتيجي لدولة أو أمة ما. ينظر: منذر سلمان، نحو إعادة صياغة مفهوم الأمن القومي العربي ومرتكزاته، العدد 1544، السنة الثامنة، فلسطين، 2008، ص3. وكذلك ينظر: مصطفى عبد الله خشيم، تأثير مؤتمر برشلونة على الأمن الاقتصادي العربي – الأمن العربي التحديات الراهنة، نظرية السياسة العامة، جامعة قاريونس، ليبيا، 2007، ص460.

[1] نقلاً عن: رتيبة برد، السياسة الأمنية الأمريكية في المتوسط، مجلة دفاتر السياسة والقانون، العدد (15)، جوان 2016، (pdf)، على الموقع الإلكتروني: www.dspace.univ-ouargla.dz

[2] نقلاً عن: نسيمة طويل، المثلثاتية الاستراتيجية في شمال شرق آسيا، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، ألمانيا – برلين، 2017، ص26.

[3] نقلاً عن: لخميسي شيبي، الأمن الدولي والعلاقة بين منظمة حلف شمال الأطلسي والدول العربية فترة ما بعد الحرب الباردة (1991-2008)، المكتبة المصرية للنشر والتوزيع، القاهرة – مصر، 2010، ص14.

[4] خالد علي محمد الأميري وأحمد فلاح العموش، الأمن الوطني: المفهوم، الأبعاد والنظريات، مجلة الآداب، ملحق العدد 133، حزيران 2020، ص532، pdf، على الموقع الإلكتروني: https://www.researchgate.net

حماية حياضها ومواطنيها وحقوقهم، على الرغم من الاختلاف البيّن بين التقليديين والحداثيين حول تعريف تلك الطبيعة وربطها بما يقدمه سلوك صناع القرار بهذا الصدد من تضحيات وتكاليف أو ما يجتهدون به من تدابير. وعليه فإن الأمن، مفهوماً وجوهراً، لا يتم تحقيقه أو ضمانه دون استحضار خمسة ركائز، هي[1]:

1. ادراك التهديدات سواءً الخارجية منها أو الداخلية.
2. رسم استراتيجية لتنمية قوة الدولة والحاجة إلى الانطلاق المؤمن لها.
3. توفير القدر على مواجهة التهديدات ببناء القوة المسلحة القادرة على التصدي لها.
4. اتخاذ إجراءات متصاعدة تتناسب مع تصاعد التهديدات سواءً الداخلية أو الخارجية.
5. محاربة العنف الذي يستهدف حقوق الإنسان والتمييز العنصري وعدم وجود العدالة.

وهنا يأتي المفهوم الشامل للأمن الذي يتمثل بالقدرة التي تتوفر لدى الدولة، والتي تمكنها من تأمين انطلاق مصادر قوتها الداخلية والخارجية في شتى المجالات في مواجهة مصادر التهديد الداخلية والخارجية وتمكنها من تهيئة الأوضاع والمناخ الملائم لتأمين مصالحها بوصفها متطلبات رئيسة داخلياً وخارجياً بالشكل الذي يدفع عنها التهديدات باختلاف أبعادها، وبالقدر الذي يكفل لشعبها حياة مستقرة توفر له أقصى طاقة للنهوض والتقدم[2].

وتجدر الإشارة إلى أن مهمة صناعة الأمن بالنسبة لأية دولة، تعّد أساس سياساتها المحلية والدولية، إذ يتعلق الأمن أساساً ببقائها الفعلي، كونها ترغب في حماية نفسها من الإطاحة بها أو من الغزو الخارجي، فأمن أراضيها وسيادتها وقيمها الأساسية ورخائها العام تعد متطلبات أساسية، كما تعدّ مرجعية الشرعية لاستمرار الحكومات في حكم شعوبها. ولهذه الاعتبارات كلها، عادةً ما تخصص الحكومات موارد كبيرة لقضايا الأمن[3]، وسواء تم تناول الأمن الوطني باسم الدفاع أو السيادة أو المصلحة الوطنية، فإنه يحظى بأولوية التفكير الاستراتيجي، سياسياً وعسكرياً واقتصادياً.

---

[1] منعم صاحي العمار وشيماء تركان صالح، الأمن الوطني العراقي ومكافحة الإرهاب (دراس في إشكالية الإدارة)، مجلة دراسات دولية، العدد 61، نيسان 2015، مركز الدراسات الدولية، جامعة بغداد، بغداد – العراق، ص33– 35.

[2] علي عبد العزيز مرزة، الديمقراطية والأمن القومي: دراسة نظرية تحليلية، اطروحة دكتوراه غير منشورة، كلية العلوم السياسية، جامعة بغداد، بغداد – العراق، 2014، ص72.

[3] عامر مصباح، المنظورات الاستراتيجية في بناء الأمن، دار الكتاب الحديث، القاهرة – مصر، 2013، ص351.

ومنذ انتهاء الحرب الباردة وتحديداً منذ عام 1990م، طرأ على مفهوم الأمن الوطني تغيرات جمة في عالم السياسة وفي المجالين العسكري والأمني، بحكم ما طرأ من ظروف سياسية وتطورات تكنولوجية ومن وعي إنساني، إذ انفتح العالم أمام معنى واسع للأمن الوطني حتى صرنا في المواجهة أو التعامل مع تيارين. تضمن التيار الأول، توسيعاً لمعنى الأمن الوطني باتجاهات أفقية يتضمن المفهوم أفكاراً عن التهديدات القائمة والكامنة، سواء كان متضمناً لقضايا سياسية أو اقتصادية أم اجتماعية، أم بيئية، فضلاً عن القضايا العسكرية. أما التيار الثاني، فقد ذهب إلى التعمق بمعنى الأمن الوطني باتجاه رأسي أو عمودي، يتضمن توسيعاً لكل مصادر التهديد التي يتعرض لها الأفراد والمجتمع والمؤسسات والدولة[1]. أي أن المفهوم الحديث للأمن لا يقتصر على الجوانب العسكرية، بل يواكب كل التهديدات والتحديات التي يمكن أن تشكل حجر عثرة أمام الدولة واقتصادها الرقمي وتدفق المعرفة، ولاسيما بعد أن أسقطت تكنولوجيا المعلومات والاتصالات مفهوم الحدود الجغرافية بين الدول، الأمر الذي يضع السيادة الوطنية على المحك مع اختراق المواقع الحكومية والتجسس المعلوماتي على الدول.

[1] محمد رضا فودا، الاستراتيجية والأمن القومي، المكتب العربي للمعارف، القاهرة – جمهورية مصر العربية، 1995، ص18.

**المطلب الثاني: تعريف السيبرانية ومفهومها**

تعدّ (السيبرانية، Cybernetic) مصطلحاً مشتقاً بالأصل من المصطلح الأغريقي (Kybernetes) الذي يعني الطيار أو قائد الدفة أو الحاكم. على أن أصل الكلمة مأخوذاً من الكلمة الانكليزية (سيبر، Cyber) وهي صفة لأي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي/التخيلي[1]. وبشكل عام، فإن كيان السايبر يتشكل من ثلاثة عناصر أساسية هي: (الأجهزة الصلبة، Hardware) و(البرمجيات الرقمية، Software) والعامل البشري من مبرمجين ومستخدمين.

وفي مجال تكنولوجيا المعلومات والاتصالات كثر استعمال مصطلحات معينة كـ(الفضاء السيبراني، Cyber Space)، الذي يعبر عن مجموعة من الوسائل المستعملة لإنتاج واستغلال وتوزيع المعلومات بكل أشكالها المكتوبة والمسموعة والمرئية، والتي تعدّ البنية التحتية التي تُمكن التواصل الاجتماعي وتُؤمن انتقال الرسالة من المرسل إلى المتلقي[2]. وبذلك يعدّ الفضاء السيبراني التعبير التكنولوجي الفائق السرعة لانتقال وانتشار المعلومات بين رواد هذا الفضاء.

وكان عالم الرياضيات (نوربرت وينر، Norbert Wiener) أول من استعمل مصطلح السيبرانية وذلك في كتابه الشهير (التحكم والتواصل عند الحيوان والآلة، Cybernetics or control and communication in the Animal and Machine) الصادر في عام 1948م، عندما كان يدرس موضوع القيادة والسيطرة والاتصال في عالم الحيوان، فضلاً عن الهندسة الميكانيكية. أما (وليام جيبسون، Wiliam Gibson) فهو أول من أستعمل كلمة (Cyber) مقترنة بكلمة (Space) ليظهر في عام 1984م، مصطلح (الفضاء السيبراني، Cyber Space)[3]، الذي اقترن بانعدام الجغرافيا وظهور جغرافية الإبحار

---

[1] صالح بن علي بن عبد الرحمن، الأمن الرقمي وحماية المستخدم من مخاطر الانترنت – رؤية 2030، هيئة الاتصالات وتقنية المعلومات، المملكة العربية السعودية، 2017، ص6.

[2] توامي يعقوب، أثر استخدام تكنولوجيا المعلومات والاتصال على الأداء المالي للمؤسسة الاقتصادية– دراسة حالة مجمع المؤسسة الوطنية للاشغال في الآبار (E.N.T.P.)) خلال الفترة 2010–2012، رسالة ماجستير غير منشورة، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة قاصدي مرباح، الجزائر، 2013، ص6.

[3] عادل عبد الصادق، الإرهاب الإلكتروني – القوة في العلاقات الدولية (نمط جديد وتحديات مختلفة)، مركز الدراسات السياسية والاستراتيجية بالأهرام، القاهرة – جمهورية مصر العربية، 2009، ص37.

المعلوماتي في كل الاتجاهات، الأمر الذي جعل من ظاهرة الفضاء السيبراني أهم خصائص عصر المعلومات والاتصالات بدون منازع.

لقد عُرف الفضاء السيبراني من قبل الاتحاد الدولي للاتصالات، وهو إحدى الوكالات المتخصصة للأمم المتحدة في مجال تكنولوجيا المعلومات والاتصالات على أنه (الحيز المادي وغير المادي الذي ينشأ أو يتكون من جزء أو كل العناصر الآتية: حواسيب أجهزة ممكنة وشبكات ومعلومات محوسبة وبرامج ومضامين ومعطيات مرور ورقابة والذين يستخدمون كل ذلك)[1]. أما الوكالة الفرنسية لأمن أنظمة الإعلام فقد عرفته على أنه (فضاء التواصل المشّكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية)[2]. كما يمكن أن يُفهم الفضاء السيبراني على أنه (امتداد للوسائط الرقمية عبر خطوط نقل مختلفة، معدنية وألياف بصرية ولاسلكية، وقنواتها على شبكات الانترنت)[3].

وهكذا فإن الفضاء السيبراني، يعّد بمثابة المستودع الكبير الذي تُجرى فيه جميع عمليات التواصل الاجتماعي، عبر شبكات الحواسيب أو الهواتف النقالة. وبتعبير أكثر اتساعاً، هو منظومة من العناصر المتفاعلة فيما بينها، والمتكونة من أجهزة الكومبيوتر، وأنظمة الشبكات وبرمجيات، حوسبة المعلومات، ونقل وتخزين البيانات، ومستخدمي كل هذه العناصر. وتتداخل بنية الفضاء السيبراني بأنظمة البرمجيات والعناصر المادية والفضاء الرقمي، لتشكل منظومة معلوماتية في اطار برمجيات التواصل الإلكتروني[4]. ولعل أهم سمات الفضاء السيبراني ما يلي[5]:

---

[1] نقلاً عن: خالد وليد محمود، الهجمات عبر الانترنت– ساحة الصراع الإلكتروني الجديد، سلسلة دراسات ودراسة السياسات، المركز العربي للأبحاث، الدوحة – قطر، 2013، ص4.

[2] نقلاً عن: قادير إسماعيل، إدارة الحروب النفسية في الفضاء الإلكتروني – الاستراتيجية الأمريكية الجديدة في الشرق (الأوسط، الندوة الدولية الموسومة بعنوان (عولمة الإعلام السياسي وتحديات الأمن القومي للدول النامية)، قسم العلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، الجزائر، 2007/3/7، ص4.

[3] Khalid Walid Mohmoud, Cyber attacks: the electronic Battlefield, Series: Research Paper, Arab Center for research and Policy Studies, 2013, p.3.

[4] محمد وائل القيسي، مستقبل الأمن الاستراتيجي العالمي في ظل التحديات التكنو – معلوماتية والفضاء السيبراني، مجلة (دراسات إقليمية، السنة 14، العدد 44، نيسان 2020، جامعة الموصل، الموصل – العراق، ص154.

[5] صالح بن علي بن عبد الرحمن، مصدر سبق ذكره، ص7.

1. أنه مجال عملياتي إذ يعّد ميدان التفاعلات المدنية والعسكرية.
2. تعدّ البنى التحتية لأنظمة الاتصالات وتقنية المعلومات جزءً أساسياً من الفضاء السيبراني.
3. الفضاء السيبراني لا يقتصر على شبكة الانترنت فقط وإنما هي شبكات عالمية وخاصة مثل ( GPS, ACARS, SWIFT, PSTN).

لقد صارت المجتمعات الحديثة، مجتمعات ثقافية بالدرجة الأولى، الأمر الذي شّكل (الوطن الرقمي) الذي يشير إلى العالم الإلكتروني الذي انتجته شبكات المعلومات، إذ أضحى بمقدور الناس التواصل مع بعضهم البعض في فضاء إلكتروني عالمي بكل سهولة ويسر وبتكلفة زهيدة وحتى وصل الأمر في بعضها خارج رقابة الحكومات وسيطرتها[1]، وهو الأمر الذي رتب وجهين للمتغير التكنولوجي. وكالآتي[2]:

فالوجه الأول وهو الفرص التي تتمثل بالخدمات الجليلة التي قدمتها التكنولوجيا للإنسان، إذ أسهمت بتوفير وسائل الراحة له بفضل التطور الهائل في تقنيات المعلومات والاتصالات، فضلاً عن النقلة النوعية في المجالات الطبية سواءً الدوائية منها أو على صعيد الأجهزة الطبية. ومن الأوجه الإيجابية الأخرى التي وفرتها التقنية على الصعيد الاقتصادي، هي الحوالات بين البنوك في أماكن بعيدة جغرافياً قد تكون بين قارات مثلاً، هذا من جهة ومن جهة أخرى، ساهمت التطورات التكنولوجية وبشكل كبير في زيادة الفاعلية الدولية بين وحدات النظام السياسي الدولي ومن ثم تنامي فاعلية وحدات أخرى إلى جانب (الدولة) في تشكيل التفاعلات الدولية وتأثيرها وتأثرها بالنظام الدولي، ومن أبرزها الشركات المتعددة الجنسية والمنظمات الدولية الحكومية وغير الحكومية...الخ.

أما الوجه الثاني، فيتمثل بالتحديات، والتي يأتي في مقدمتها الآثار السلبية للتكنولوجيا على واقع (سيادة الدول). فتقنية المعلومات المتطورة أوجدت وضعاً وصفه (ولتر رستون) بـ(أفول السيادة) نظراً لما خلفته هذه التطورات من مخاطر قاسية فقدت عبرها الدول قدسية حدودها السياسية وذلك بسبب عدم قدرتها على الوقوف بوجه الموجة العارمة التي أطلق عليها (ألفن توفلر) بـ(الموجة الثالثة). ومن النقاط السلبية

---

[1] سمية أوشن، الدولة المعاصرة والعولمة الثقافية – بين توطين قيم الثقافة العالمية وعولمة قيم الثقافات المحلية، أطروحة دكتوراه غير منشورة، كلية الحقوق والعلوم السياسية، جامعة باتنة –الحاج لخضر، الجزائر، 2019، ص111.

[2] محمد وائل القيسي، مصدر سبق ذكره، ص154-155.

الأخرى للعصر التكنولوجي هو ظاهرة اختراق منظومة شبكات الانترنت العالمية من قبل بعض الأشخاص، كما حدث في عام 2008م، مع الشاب الألماني الذي اخترق منظومة الشبكات العالمية محدثاً بذلك عطب كبير أثر على الوضع الدولي بأسره لأيام وما نجم عن ذلك من إيقاف لمفاعلات ومنشآت وبرامج عالمية تعتمد على المنظومة العالمية. وكذلك الحال في اختراق شاب ياباني في العام ذاته لمنظومة الدفاع الأمريكية (البنتاغون) وهو ما أحدث ضجة عالمية إلى أن تمكنت سلطة الانتربول الدولية من إلقاء القبض عليه.

فانطلاقاً من القناعة التي مفادها، إن المعلومة في ظل التطور التكنولوجي لم تعّد حكراً على الدول، أخذ العالم يشهد تحولات في الفواعل التي تستعمل القوة، فالقطاع الخاص أخذ يساهم بنسبة كبيرة في امتلاك وإدارة التكنولوجيا الحديثة ووسائل الاتصالات والمعلومات. لذا يمكن القول بأن الفضاء السيبراني يضم نوعين من الفواعل ويمكن تقسيمهم إلى مستويين. يضم المستوى الأول الفواعل الدولية، وهنا تعدّ الدولة فاعلاً محورياً في تسيير الفضاء السيبراني انطلاقاً من إمكاناتها المادية والبنيوية والبشرية والقانونية. أما المستوى الثاني، فيضم الفواعل من غير الدول، وهنا تأتي المنظمات غير الحكومية والشركات فضلاً عن الجماعات والأفراد[1]، العاديون الذين يكون بمقدورهم امتلاك وسائل القوة السيبرانية ويتمتعون بمهارات فنية وتقنية تمكنهم من ابتكار وتطوير برامج الكترونية رقمية معقدة لاختراق المواقع والشبكات وشن الهجمات السيبرانية، وهو ما اصطلح على تسميتهم بـ(الهاكرز أو القراصنة أو الميليشيات السيبرانية)[2].

**المطلب الثالث: تعريف الإرهاب السيبراني ومفهومه**

يعدّ (الإرهاب، Terrorism) من المصطلحات التي كثر الخلاف في بيان معناها وتحديد مدلولها. فعلى الرغم من أنه من أكثر الكلمات استعمالاً في مختلف وسائل الإعلام العالمية ولاسيما منذ أحداث 11 أيلول 2001م، إلا أن الباحثين لم يتفقوا على تعريف دقيق ومحدد له، وذلك نظراً لطبيعة الأعمال الإرهابية

[1] قادير إسماعيل، إدارة الحروب النفسية، مصدر سبق ذكره، ص5.

[2] محمد محمد سعيد الشعيبي ونادية محمد سعيد النقيب، أنسنة الحرب الالكترونية، مجلة العلوم التربوية والدراسات الإنسانية، العدد 25، سبتمبر 2022، ص543، pdf، على الموقع الالكتروني: hesj.org

واختلاف وجهات النظر لمثل هذه الأعمال[1]. ومن أجل وضع تعريف محدد للإرهاب السيبراني، فقد ارتأينا قبل ذلك بيان تعريف الارهاب، بشكل عام.

يأتي (الإرهاب) في اللغة العربية من الفعل (رَهبَ، يَرهبُ، رهبةً) بمعنى خاف. والرهبة، هي الخوف والفزع. وهو راهب من الله، أي خائف من عقابه. وترهبه أي توعده[2]. أما في اللغة الأجنبية، فإن كلمة الإرهاب تأتي بمعنى (العنف، Terror) التي تعني الخوف أو القلق المتناهي أو تهديد غير مألوف أو غير متوقع[3]. وفي القرآن الكريم، قال تعالى ((وأعدوا لهم ما استطعتم من قوة ومن رباط الخيل ترهبون به عدو الله وعدوكم))[4]. فـ((ترهبون)) أي تخوفون. والإرهاب من الرهبة أي الخوف، وهو التخويف وإشاعة عدم الاطمئنان وبث الرعب والفزع، وغايته إيجاد حالة من عدم الاستقرار المستمر بين الناس في المجتمع لتحقيق أهداف معينة[5]. وأوضح المجّمع اللغوي إن (الإرهابيين) وصف يطلق على اللذين يسلكون سبيل العنف لتحقيق أهداف سياسية، كما أقر المجّمع ذاته إن كلمة (إرهاب) تعدّ حديثة الاستعمال في اللغة العربية ولا وجود لها في الأزمنة القديمة[6].

وفي الاصطلاح، فعلى الرغم من تباين التعريفات حول مفهوم الإرهاب، إلا أن جميعها تشير إلى أنه يهدد الاستقرار السياسي والمجتمعي عن طريق استعمال العنف على وجه غير مشروع لتحقيق مكاسب وأهداف مرسومة. فقد عُرف في معجم مصطلحات العلوم الاجتماعية على (أنه عبارة عن الطريقة التي تحاول بها جماعة أو حزب أن تحقق أهداف عن طريق استخدام العنف)[7]. وفي الموسوعة السياسية، فإن الإرهاب يعني (استخدام العنف أو التهديد به، بكافة أشكاله المختلفة، كالاغتيال والتعذيب والنسف، بغية

---

[1] سليماني مباركة، الارهاب الالكتروني وطرق مكافحته، مجلة الحقوق والعلوم السياسية، جامعة خنشلة، العدد 8، الجزء الأول، جوان 2017، ص341، pdf ، على الموقع الالكتروني: www.asjp.cerist.dz

[2] أبن منظور المصري، معجم لسان العرب، المجلد الأول، بيروت للطباعة والنشر، ص1374.

[3] محمد عبد المحسن سعدون، مفهوم الإرهاب وتجريمه في التشريعات الجنائية والوطنية، العدد السابع، 2008، ص135، pdf، على الموقع الالكتروني: www.iasj.net

[4] القرآن الكريم، سورة الأنفال، الآية (60).

[5] محمد عبد الجبار السماوي اليمني، الموسوعة العربية في الألفاظ الضدية والشذرات اللغوية، دار الآداب – بيروت، مركز الدراسات والبحوث اليمني – صنعاء، المجلد الثاني، 1989، ص190.

[6] مجمع اللغة العربية، المعجم الوسيط، الجزء الأول، المكتبة الإسلامية للطباعة والنشر والتوزيع، ص376.

[7] أحمد زكي بدوي، معجم مصطلحات العلوم الاجتماعية، مكتبة لبنان، القاهرة – مصر، 1975، ص423.

تحقيق هدف سياسي معين، مثل كسر روح المقاومة، وهدم معنويات الأفراد والمؤسسات أو كوسيلة للحصول على معلومات أو مكاسب مادية أو لإخضاع طرف مناوئ لمشيئة الجماعة الإرهابية)[1].

أما (الإرهاب السيبراني، Cyber Terrorism)، فهو الإرهاب الذي ارتبط وجوده بوجود الفضاء السيبراني، وذلك نتيجة التوسع في الاعتماد على الاتصالات والمعلومات في تسيير الشؤون الحياتية للأفراد والمؤسسات والدول، اي أنه يرتبط بنوع البيئة التي يمارس فيها[2]. وكانت بداية استعمال مصطلح (الإرهاب الالكتروني) في ثمانينات القرن العشرين على يد المختص بالشؤون المعلوماتية والوقاية والأمن (باري كولن، Barry Collin) الذي أقرّ بصعوبة وضع تعريف شامل للإرهاب التكنولوجي، ولكنه تبنى تعريفاً له مقتضاه (أنه هجمة الكترونية غرضها تهديد الحكومات أو العدوان عليها سعياً لتحقيق أهداف سياسية أو دينية أو إيديولوجية، وإن الهجمة يجب أن تكون ذات أثر مدمر تخريبي مكافئ للأفعال المادية للإرهاب)[3]. كما يُعرف الإرهاب السيبراني على (أنه عمل إجرامي يكون السلاح فيه وسائل اتصال ينتج عنه عنف وتدمير أو بث الخوف، تجاه المستهدف سواءً كان فرداً أو مؤسسة أو دولة، والهدف منه هو التأثير على الحكومة أو السكان، وعادةً ما يمثل أجندة سياسية أو اجتماعية أو فكرية معينة)[4].

وتعرف جماعات الإرهاب الالكتروني، على أنها الفاعلون العنيفون في النظام الدولي من غير الدول، وهم الجماعات أو التنظيمات التي تلجأ إلى استعمال أدوات العنف المادي والنفسي بطريقة جماعية، من أجل تحقيق غايات معينة، ولا تنتمي لأجهزة الدولة الرسمية[5]، مثل الحركات الراديكالية والجماعات الأصولية،

---

(1) عبد الوهاب الكيالي، موسوعة السياسة، الجزء الأول، الطبعة الثانية، المؤسسة العربية للدراسات والنشر، بيروت – لبنان، 1985، ص34.

(2) محمد زهير عبد الكريم، الإرهاب السيبراني: أزمة عالمية جديدة، مجلة قضايا سياسية، كلية العلوم السياسية، جامعة النهرين، بغداد – العراق، ص282.

(3) محمد مهني، تأثير الإرهاب الإلكتروني على تغير مفهوم القوة في العلاقات الدولية – توظيف المنظمات الإرهابية لمواقع التواصل الاجتماعي انموذجاً، رسالة ماجستير غير منشورة، قسم العلوم السياسية والعلاقات الدولية، جامعة محمد بو ضياف، الجزائر، 2018، ص21.

(4) نقلاً عن: حازم حمد الشمري، توظيف القوة السيبرانية في استراتيجيات الدول الكبرى: الولايات المتحدة وروسيا الاتحادية (إنموذجاً، الطبعة الأولى، بغداد – العراق، 2022، ص52.

(5) نقلاً عن: صباح عبد الصبور عبد الحي، استخدام القوة الإلكترونية في التفاعلات الدولية – تنظيم القاعدة انموذجاً، الجزء الثاني، المعهد المصري للدراسات السياسية والاستراتيجية، تركيا، 2016، ص5.

التي تعمل بمتلازمة البؤر في تنفيذ مخططاتها أينما وجدت مرفأ يؤيد أفكارها، فهي تبحث عن المؤيدين والمناصرين لها في العالم[1]. وتعدد خصائص الإرهاب السيبراني بما يلي[2]:

1. غياب جهة السيطرة والرقابة على الشبكة المعلوماتية، أي لا توجد جهة مركزية موحدة تتحكم فيما يعرض على الشبكة وتتحكم في مدخلاتها ومن ثم مخرجاتها.
2. عابر للدول والقارات أي غياب الحدود الجغرافية بين الدول، إذ تربط شبكة المعلومات العالمية أعداد هائلة لا حصر لها من الحواسيب عبر العالم، ويغدو أمر التنقل والاتصال فيما بين المجموعات الإرهابية أمراً سهلاً. بمعنى آخر، فإن الشبكة المعلوماتية تتميز بسهولة الاستعمال والدخول إليها من أي مكان في العالم، فهي تتجاوز الحدود الجغرافية للدول.
3. تدني مستوى المخاطر، إذ يتميز الاتصال المعلوماتي بعدم وضوح الهوية الرقمية للمستخدم المستوطن في بيئته المفتوحة مما تعد فرصة مناسبة للإرهابيين إذ يستطيع الإرهابي أن يقدم نفسه بالهوية والصفة التي يرغب فيها أو التخفي تحت شخصية وهمية ومن ثم يشن هجومه الإلكتروني من دون مخاطر مباشرة.
4. صعوبة الإثبات، إذ يعدّ استعمال الوسائل الفنية والتقنية أمراً بالغ الصعوبة في التوصل إلى الدليل المادي للجريمة المرتكبة من قبل المجموعات الإرهابية، فضلاً عن التباعد الجغرافي. وبالتالي صعوبة تحديد هوية المتصل وملاحقة مرتكبي العمليات الإرهابية مما يساعدهم على الحركة بحرية داخل المواقع التي يستهدفها قبل أن ينفذ جريمته.
5. أنه قوة ناعمة، إذ لا يحتاج إلى المواجهة العسكرية أو استعمال الأسلحة التقليدية، وأنها جريمة لا تحتاج إلى مجهود عضلي كالقتل والسلب.
6. ضعف بنية الشبكات المعلوماتية وقابليتها للأختراق، إذ أنها مصممة في الأصل بشكل مفتوح دون قيود أو حواجز أمنية عليا رغبة في التوسع وتسهيل دخول المستخدمين وتحتوي الأنظمة الإلكترونية

---

[1] سيف نصرت توفيق، فواعل النظام في القرن الحادي والعشرين، مجلة تكريت للعلوم السياسية، العدد 11، جامعة تكريت، صلاح الدين – العراق، 2017، 149.

[2] لبنى خميس مهدي وتغريد صفاء، أثر السيبرانية في تطور القوة، مجلة حمورابي، العدد 33-34، السنة الثامنة، شتاء – ربيع 2020، ص158.

والشبكات المعلوماتية على ثغرات معلوماتية يمكن للجماعات الإرهابية استغلال هذه الثغرات في التسلل إلى المعلوماتية والبيانات من أجل تحقيق أهدافها التخريبية والإرهابية.

7. سهولة الاستعمال التقني وقلة التكلفة، الأمر الذي هيأ للإرهابيين فرصة من أجل الوصول إلى أهدافهم غير المشروعة من دون الحاجة إلى مصادر تمويل ضخمة، فضلاً عن سهولة التواصل بين العناصر الإرهابية والتخطيط لتنفيذ عملياتهم، التي تتميز بشدة أثرها وضررها.
8. ضعف التشريعات والقوانين الرادعة لهذا النوع من الجرائم في بعض الدول، كما هو الحال في العراق، فتطور العمليات الإرهابية الإلكترونية بشكل سريع لم يسايره تطوير تشريع وآليات رادعة.

وتنقسم أهداف هجمات الإرهاب الإلكتروني لثلاثة هي[1]:

1. القيام بهجمات رقمية الطابع عبر الفضاء الإلكتروني، إذ يتم شن عمليات التدمير والهجوم إلكترونياً.
2. يعدّ الفضاء الإلكتروني عامل مساعد في العمل الإرهابي عن طريق تسهيل الحصول على المعلومات والتنسيق والتجنيد والتعبئة وغيرها.
3. يتمثل في العمل على شن الحرب النفسية ونشر المعلومات المظللة والكراهية الدينية وما يقابل ذلك من انتهاكات لحقوق الإنسان كحجب المواقع أو تنفيذ الاعتقالات للخصوم السياسيين.

وفيما يتعلق بأدوات الإرهاب السيبراني، والتي يمكن أن نطلق عليها، بأسلحة الهجوم الإلكتروني، فهي على النحو الآتي[2]:

1. الفايروسات، Virus: والتي تعد من أخطر آفات الشبكة المعلوماتية، وتتميز بقدرتها على ربط نفسها بالبرامج الأخرى وسرعة التضاعف والانتشار. وتعمل على تعطيل الخدمة مؤقتاً لا على تدمير قاعدة

---

[1] عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، المركز العربي لأبحاث الفضاء، الإسكندرية– جمهورية مصر العربية، بلا تاريخ، ص127.

[2] وليد عبد الحي وآخرون، فهم الأمن القومي الجزائري من مدخلي الأمن الوطني والدفاع الوطني، دار الحامد للنشر والتوزيع، عمان – الأردن، 2015، ص448. وكذلك ينظر: عبد الهادي محمود الزيدي، التجسس الإسرائيلي الإلكتروني على الدول العربية، مجلة دراسات دولية، العدد 58، مركز الدراسات الدولية والاستراتيجية، جامعة بغداد، بغداد – العراق، ص141. وكذلك ينظر: كرار عباس متعب فرج، الحرب السيبرانية: دراسة في استراتيجية الهجمات السيبرانية بين الولايات المتحدة الأمريكية وإيران، مجلة حمورابي للدراسات، العدد 40، السنة العاشرة، شتاء 2021، ص205، pdf، على الموقع الالكتروني: https://www.iasj.net

البيانات والمعلومات. ويتم من خلال هذا النمط اطلاق حزمة كبيرة من البيانات والمهمات خادم (Server) على جهاز الطرف المتضرر وبشكل يفوق قدرته على الاستجابة والمعالجة مما يؤدي إلى توقف وشل مصالحه بصورة كلية أو جزئية، وتعطيل نظم المعلومات الإلكترونية لديه.

2. برنامج الدودة، Worms Program: وهي التي تقوم باستغلال أية فجوة في أنظمة التشغيل من نظام إلكتروني لآخر، أو من شبكة لأخرى عبر الوصلات التي ترتبط بها. وتتكاثر هذه البرامج تلقائياً في أثناء عملية انتقالها، وتعمل على تقليل كفاءة الشبكة أو التخريب الفعلي للملفات والبرامج ونظم التشغيل.
3. أحصنة طروادة، Trojans: وهو عبارة عن فايروس ذا مقدرة على الاختفاء داخل برامج أخرى أصلية للنظام الإلكتروني. ينشط وينتشر هذا الفايروس عندما تبدأ برامج التشغيل بالعمل ليبدأ أعماله التخريبية. ويختلف هذا الفايروس عن الفايروس العادي بكونه لا يتكاثر في الملفات إنما هو برنامج مستقل بذاته، يحمل في ثناياه توقيت وأسلوب استيقاظه، وقد تصل أعماله التخريبية إلى تدمير النظام برمته. كما يمكن أن يقوم حصان طروادة بفتح أحد المنافذ في جهاز المجني عليه دون أن يشعر، وفتح القرص الصلب لجهاز المجني عليه والعبث به بحذف أو إضافة ملفات جديدة، كذلك يمكن للمخترق معرفة كلمة السر المخزنة في الجهاز ورقم بطاقة الائتمان، وكذلك يمكن للمخترق إذا كان لدى المجني عليه (ميكرفون أو كاميرا) أن يستمع ويرى كل ما يفعل في المساحة التي يغطيها الميكرفون أو الكاميرا.
4. هجمات انكار الخدمة Denial of service, Dos: وهي عبارة عن هجمات الكترونية تتم بإغراق الموقع بسيل من البيانات غير اللازمة يجري إرسالها ببرامج متخصصة تعمل على نشرها، وبالتالي سيؤدي إلى بطء في الخدمات أو ازدحاماً مرورياً على هذه المواقع، فيصعب بالتالي وصول المستخدمين إليها.
5. القنابل المنطقية (Logic Bombs): وهي عبارة عن برمجيات يتم زرعها داخل النظام أو البرنامج، أي أن يكون البرنامج أو النظام مصاباً منذ البدء بالبرنامج الضار أي بالسلاح السيبراني، إذ يبدأ عمل البرنامج الضار تحت ظروف معينة تكون في المحصلة والهدف النهائي هو التحكم بالجهاز بصورة تامة أو إتلافه.

6. الفايروسات الالكترونية (Electronic Viruses): كفايروس (ستاكس نت، Stuxnet) الذي يعدّ أخطر أنواع الأسلحة السيبرانية، والذي تم اكتشافه في عام 2009م ومثّل نقلة نوعية في خطورة الحرب السيبرانية، إذ انتقلت الحرب من تدمير البيانات وسرقتها إلى تدمير المكونات المادية نفسها ونظم التشغيل. وأيضاً فايروس (دوكو، Duqo) الذي تم اكتشافه في عام 2011م بواسطة معامل التشفير والأمن الالكتروني (Crysys Lab) التابع لجامعة بودابست. وفايروس (فليم، Flamp) الذي تم اكتشافه عام 2012م بواسطة فريق الاستجابة والطوارئ الإيراني فضلاً عن شركة (كاسبر سكي) ومعمل التشفير والأمن الالكتروني التابع لجامعة بودابست، إذ أصدرت الأمم المتحدة تحذيراً اعتبرت فيه هذا الفايروس بأنه الأكثر خطورة وتعقيداً بسبب أهدافه التدميرية.
7. البرمجيات الخبيثة مثل (أريد البكاء، Wanna Cry)، إذ تتميز هذه البرمجيات بكونها تستهدف الكيانات الاقتصادية وليست الأفراد، وذلك لأن هذه المؤسسات هي الأقدر على دفع الفدية. ويلاحظ أنه في عام 2017م قام مجموعة من القراصنة المجهولين بشن هجوم ضار باسم (أريد البكاء، Wanna Cry) وتمكن الهجوم من إصابة أكثر من (200.000) ضحية في أكثر من (150) دولة خلال أول (48) ساعة من الهجوم، والشيء المقلق إن هذه الهجمة اعتمدت على أسلحة وثغرات تم تسريبها من وكالة الأمن القومي الأمريكي، إذ أشارت بعض التحليلات إلى ضلوع الوكالة في تطوير هذا البرنامج قبل أن تتم سرقتها منها وتسريبها.

ولا بد من الإشارة إلى أن الخطر السيبراني يزداد يوماً بعد آخر، وذلك بسبب توفر سوق للبرامج والأدوات الخبيثة والخدمات غير المشروعة والبيانات الحساسة (غير المتاحة للعامة) بأسعار زهيدة. فعلى سبيل المثال، يمكن شراء برنامج خبيث مقابل دولار واحد فقط، كما يمكن اطلاق هجمات الحرمان من الخدمات (Dos) بأقل من ألف دولار، كما تتوفر هجمات برامج الفدية مقابل مئتي دولار وخدمات الرسائل الالكترونية غير المرغوبة (سيام) بمبلغ أربعمائة دولار تقريباً، كما يمكن أيضاً استهداف أسلحة معقدة من خدمات الاستخبارات الحكومية[1].

[1] أميرة عبد العظيم محمد عبد الجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، العدد الخامس والثلاثون، الجزء الثالث، 1442هـ-2020م، ص384، pdf، على الموقع الالكتروني:

## المبحث الثاني: طبيعة الإرهاب السيبراني في العراق

أدى الانتشار الهائل في استعمال شبكات الانترنت في العراق إلى إحداث (ثورة كبرى) تركت تأثيراتها على جوانب الحياة كافة، ومن بينها الأمن الوطني للدولة العراقية الذي أصبح يواجه تحديات جديدة، لذا توسع مفهوم الأمن الوطني العراقي ليتجاوز نطاق مواجهة التهديدات العسكرية وضمان حماية المواطن ووحدة وسلامة أراضيه وسيادته، إلى مجالات أخرى تشمل الاستقرار السياسي والاقتصادي والانسجام الاجتماعي وسلامة البيئة. وعليه، فإن موضوع هذا المبحث سيتم تناوله عبر المطلب الثلاثة الآتية.

### المطلب الأول: انتشار السيبرانية في العراق

شهد العالم عبر تاريخه الطويل تطورات متلاحقة وتحولات كبيرة في طرائق وأساليب الحياة والمعيشة والعمل، واستجدت لديه احتياجات عديدة. فبعد أن كان يعتمد على الزراعة لمدة طويلة من الزمن حتى حدثت الثورة الصناعية لتلبي احتياجاته، فتغيرت بشكل جوهري أنماط حياته، ثم ما لبثت المجتمعات وخاصة المتطورة اقتصادياً أن تطوي صفحة العصر الصناعي لتفتح صفحة جديدة، وهو عصر المعلومات الذي بات لا غنى عنه في ظل الاعتماد المتزايد على مخرجات المعلوماتية[1]، ولاسيما خلال عقدي الثمانينات والتسعينات من القرن العشرين، إذ شهدت هذه المدة تركيزاً ملحوظاً على المعرفة وعلاقتها بثورة التكنولوجيا والاتصالات من ناحية، وعلاقتها بتنامي المجتمع المعلوماتي بولادة شبكة الانترنت من ناحية أخرى. وقد جاء ذلك مصاحباً للوعي الكامل بالأهمية الوظيفية للمعرفة والناتج بدوره عن تغلغل تقنيات المعلومات والاتصالات في بنية الحياة الاجتماعية، وتحكمها بشكل عضوي في شبكة العلاقات الاجتماعية للإنسان المعاصر، مما ساعد على ظهور مفهوم مجتمع المعلومات إلى جانب عوامل دولية أخرى أهمها ظاهرة العولمة بتجلياتها الاتصالية والمعلوماتية والثقافية، التي شهدت هي الأخرى اهتماماً كبيراً لتأثيرها على وظائف الاتصال والاعلام في مجتمع المعلومات، إذ تقوم على الارتباط الشديد بين دول العالم عبر استعمال تكنولوجيا الاتصال. وقد أدى ذلك إلى تحويل العالم بطابعه المادي إلى عالم رقمي افتراضي، حيث انتقلت



[1] فراس جمال شاكر، الحروب المعلوماتية في المجال الأمني والعسكري: أمريكا والصين، الطبعة الأولى، العربي للنشر والتوزيع، القاهرة – مصر، 2023، ص24–25.

كافة مجالات الحياة لتأخذ طابعاً رقمياً يدور في فلك الفضاء السيبراني، تزامن ذلك مع ما شهده العالم خلال هذه المرحلة من اتجاه لانتشار الموجة الديمقراطية والتوجه نحو اقتصاد السوق[1].

ومع دخول العالم القرن الحادي والعشرين اكتسبت المعلوماتية أهمية كبيرة بسبب التقدم الهائل في البحوث والدراسات العلمية، وما صاحب ذلك من كم هائل من المعلومات التي تدفقت بشكل كبير كنتاج لتطور العلم والخبرة الإنسانية، إذ أصبح رصيد البشرية من المعلومات الناتجة عن انجازات العلم هائلة جداً سواء في نوعها أم في كمها وعلاقاتها المترابطة، الأمر الذي يهدد بعدم إمكانية ادراكها فضلاً عن عدم إمكانية السيطرة عليها، وأمام هذه الحقيقة كان لا بد من البحث عن وسائل غير تقليدية تستطيع المحافظة على التراكم المعلوماتي، لذلك ظهرت سلسلة من التطورات التقنية السريعة مثل التطورات الهائلة في مجال الحاسبات والالكترونيات المتناهية الصغر[2].

وبالتطور التكنولوجي وبتنامي الجهود نحو تطوير الاقتصاد المبني على المعرفة، أضحت تكنولوجيا المعلومات والاتصالات الأداة الرئيسة في توليد المعرفة، وحفظها، ومعالجتها، وتبادلها، فضلاً عن مساهمتها في تحقيق التنمية المستدامة، واتاحة فرص عمل جديدة للشباب، وتحفيز النمو الاقتصادي. وقد شهد هذا المجال ازدياداً كبيراً في أعداد مستخدمي الانترنت وفي انتشار الأجهزة النقالة الذكية، وزيادة الاعتماد على هذا النوع من التكنولوجيا في التنمية الاجتماعية والسياسية، وفي النفاذ إلى خدمات الحزمة العريضة النقالة[3].

وقد تزامن مع التقدم التكنولوجي، زيادة اعتمادية الدول كافة على تكنولوجيا المعلومات والذكاء الصناعي وشبكات الانترنت في إدارة كل البنى الحيوية داخل الدولة بما فيها القطاع العسكري والمدني. وتلك

---

[1] حنان بنت شعشوع الشهري، أثر استخدام شبكات التواصل الالكترونية على العلاقات الاجتماعية (الفيس بوك وتويتر نموذجاً)، مشروع بحثي مقدم ضمن متطلبات الحصول على درجة الماجستير في علم الاجتماع، قسم الاجتماع والخدمة الاجتماعية، كلية الآداب والعلوم الإنسانية، جامعة الملك عبد العزيز، الرياض – السعودية، 1433-1434هـ، pdf، على الموقع الالكتروني: home.moe.gov.om

[2] فراس جمال شاكر، مصدر سبق ذكره، ص24-25.

[3] خالد ظاهر عبد الله جابر السهيل المطيري، دور التشريعات الجزائية في حماية الأمن السيبراني بدول مجلس التعاون الخليجي، مجلة البحوث الفقهية والقانونية، العدد الثامن والثلاثون، اصدار يوليو، 2022، ص981، pdf، على الموقع الالكتروني: https://jlr.journal.ekb.eg

الاعتمادية والتشابك الإلكتروني في ما بين الدول صار السمة المميزة لعالم اليوم، فلا يمكن أن تبقى دولة بمعزل عن العالم ومتغيراته الأساسية وأهمها الفضاء السيبراني وما يجري به[1]. ويعدّ العراق واحداً من الدول التي شهدت تحولاً كبيراً في التعامل مع وسائل الإعلام بما فيها الانترنت، تمثلت بسياسة الانفتاح الكلي على الفضاء السيبراني.

ويمكن القول إن سياسة الانفتاح الكلي على الفضاء السيبراني، كانت قد دخلت العراق مع دخول القوات الأمريكية للعراق في عام 2003م، إذ أخذ العراق يشهد انفتاحاً واسعاً على البيئة السيبرانية التي كانت مغلقة في ظل النظام السابق. علماً إن تلك السياسة التي صاغتها سلطة الأئتلاف المؤقتة المنحلة في التعامل مع الفضاء السيبراني في العراق كانت متأثرة كثيراً بسياسة الفضاء المفتوح التي تتبناها الولايات المتحدة الأمريكية ذاتها، إذ اتخذت هذه السياسة محورين[2]:

الأول: حرية وسائل الإعلام وفتح الفضاء السيبراني ومنح الأفراد الحرية الكاملة في الوصول إلى محتوياته أو النشر من خلاله ومعاملته معاملة مساوية لوسائل الإعلام الأخرى، وقد اتخذت هذه السياسة بعداً تشريعياً من خلال إلغاء وزارة الإعلام وإنشاء المفوضية العليا للاتصالات والإعلام في آذار 2004م.

الثاني: تقليل الرقابة الأمنية على وسائل الإعلام، بما فيها الانترنت عن طريق إلغاء الأجهزة والمؤسسات الأمنية التي كان يستعملها النظام السابق لإحكام سيطرته على الدولة، وتم الاستعاضة عنها بإنشاء جهاز أمني موحد هو اللجنة الوزارية للأمن القومي في نيسان 2004م.

وهكذا بدأ عصر جديد في العراق في واقع قطاع الاتصالات بصورة عامة وفي الاتصالات اللاسلكية بصورة خاصة. فبعد أن كانت شركة الهواتف الأرضية شبه مدمرة وتحتاج إلى المزيد من الجهود والأموال لصيانتها لكي تقدم الخدمات للمواطنين توجهت سلطة الائتلاف المؤقتة آنذاك لشبكات الهواتف النقالة لتقديم

---

[1] هيثم كريم صيوان ومهند جبار عباس، الحرب السيبرانية بين التحديات واستراتيجيات المواجهة: العراق انموذجاً، مجلة قضايا سياسية، العدد 70، 2022، كلية العلوم السياسية، جامعة النهرين، بغداد – العراق، ص156-157.

[2] سامر محي عبد الحمزة، السياسة التشريعية العراقية لحماية الأمن الوطني السيبراني: دراسة في ضوء أحكام القانون الدولي العام، ص532، pdf، على الموقع الالكتروني: lark.uowasit.edu.iq

خدمات الاتصال والتواصل بعيداً عن تلف شبكة الهواتف الأرضية[1]. وفي البداية، كانت الهواتف عبر الأقمار الصناعية هي وسيلة الاتصال الوحيدة مع العالم الخارجي. وخلال تلك المرحلة انتشرت خدمات شركة الثريا للاتصالات عبر الأقمار الصناعية والتي كان مقرها دولة الإمارات العربية المتحدة، انتشار واسع النطاق في السوق العراقية. وقد اتفقت هذه الشركة مع خمسة مجهزين عالميين لتوزيع خدمة الهاتف عبر الأقمار الصناعية في العراق[2].

وهكذا زاد عدد المستخدمين لشبكة الانترنت والهواتف النقالة واستعمل معظم الشعب العراقي الانترنت في مجال الأعمال والتجارة والخدمات الحكومية والتعليم والصحة وغيرها من الأنشطة الاقتصادية والاجتماعية بل وحتى السياسية، أي أن هناك حالة من التزايد في التعاملات والخدمات الإلكترونية داخل العراق. ويكفي أن نشير بهذا الصدد إلى أن إجمالي خطوط خدمة الانترنت في العراق سواء المرتبطة بالهاتف النقال أو اللاسلكي بلغت (15.297.411) في عام 2018م، وهو مؤشر يدل بشكل واضح على مدى الاستعمال الواسع لشبكات الانترنت في العراق، لاسيما إذا أخذنا بالحسبان إن تعداد سكان العراق قد بلغ قرابة (40) مليون نسمة[3].

وأمام هذا التصاعد في استعمال شبكة الانترنت في العراق، تبرز تحديات ومهددات تستهدف البنى التحتية للاتصالات والمعلومات داخله، وتهدد تلك التعاملات والخدمات في الدولة العراقية، فقد تتعرض تلك البنى التحتية إلى خطر الاختراق والتخريب المتعمد من قبل هجمات الإرهاب السيبراني التي تستهدف إعاقة تقديم الخدمات الحيوية أو نشر برامج وفايروسات لتخريب كل البنى التحتية الحيوية للاتصالات وتكنولوجيا المعلومات فضلاً عن تدمير نظم التحكم الصناعي الحيوية وخاصة في مرافق الطاقة والغاز الطبيعي والكهرباء والطيران والنقل وقواعد المعلومات والبيانات القومية فضلاً عن اختراق البريد الإلكتروني ومواقع

---

[1] جعفر فهد عبد الرضا، واقع الاتصالات اللاسلكية في العراق الحديث، على الموقع الإلكتروني:
http://law.uos-college.com/news-details/44/artical

[2] عبد الستار عبد الجبار وراجي محيل، قطاع الاتصالات في العراق بعد عام 2003 والاصلاحات المطلوبة لتحقيق الرفاهية الاقتصادية، مجلة واسط للعلوم الإنسانية، جامعة واسط، واسط – العراق، 2018، ص937.

[3] مصطفى إبراهيم سلمان الشمري، الأمن السيبراني وأثره في الأمن الوطني العراقي، مجلة العلوم القانونية والسياسية، المجلد العاشر، العدد الأول، 2021، كلية القانون والعلوم السياسية، جامعة ديالى، ديالى – العراق، ص174.

الانترنت، مما يؤثر بشكل كبير على عمل المنشآت الحيوية داخل العراق والتي باتت منكشفة انكشافاً كبيراً أمام هجمات الإرهاب السيبراني[1].

**المطلب الثاني: ظهور الإرهاب السيبراني في العراق**

قدمت وسائل الاتصالات وأنظمة المعلومات الحديثة خدمة غير مقصودة للتنظيمات الإرهابية في العراق، إذ استغلت تلك التنظيمات هذا التطور لخدمة أغراضها غير المشروعة وإتمام عملياتها الإجرامية، أي أن الفضاء السيبراني مثّل عنصر جذب مهم للتنظيمات الإرهابية على تعدد أنواعها واختلاف إيديولوجياتها، وذلك لأن تطور وسائل الاتصال وشبكات المعلومات ومختلف الإمكانيات العلمية والتقنية جعل استغلالها في تنفيذ العمليات الإرهابية أكثر سهولة لتميزها بالدقة والسرعة، كما أن استهداف تدمير وتخريب البنية التحتية لشبكة المعلومات الحكومية أو العامة للمؤسسات الاقتصادية والشركات، قد يتم بكلف كبيرة جداً تتجاوز الخسائر التي تكون نتيجة العمليات الإرهابية بشكلها التقليدي، والأخطر من ذلك إن الجماعات الإرهابية قد تنفذ عملياتها التخريبية وهي في أماكن بعيدة وآمنة[2]، كما أتاحت رسائل البريد الإلكتروني وعمليات إرسال الفاكس والمواقع الإلكترونية والهواتف المحمولة والهواتف المرتبطة بالأقمار الصناعية للمنظمات الإرهابية القدرة على نشر الأفكار والبيانات والتوجيهات إلى خلاياها من الشبكات الإرهابية، كما أتاحت لهم نقل أفكارهم على المستوى العالمي. ومع إمكانية استفادة الجماعات الإرهابية في مجال الاتصالات المتطورة في تنفيذ تهديداتهم الإرهابية بحق المسؤولين الحكوميين لإلحاق الهزيمة النفسية بهم وثني إرادتهم، إلا أن الجانب الأبرز في استفادة الجماعات الإرهابية من مجال الاتصالات المتطورة تمثل في التعبير عن رسائلهم وقضيتهم والتمكن من تجنيد العناصر الجديدة في شبكاتهم الإرهابية والحصول على دعم وتمويل مستمر[3].

ومنذ عام 2006م، بدأ تسجيل احصائيات رسمية عن الجرائم السيبرانية في العراق، بسبب الانتشار السريع للخدمات والعمليات عبر الانترنت، فارتفعت معها نسبة جرائم الانترنت والأنشطة المضرة بالنظام

---

[1] هيثم كريم صيوان ومهند جبار عباس، مصدر سبق ذكره، ص159.

[2] علي إبراهيم المعموري، الأمن السيبراني وأثره في الأمن الوطني العراقي بعد العام 2003، رسالة ماجستير غير منشورة، كلية العلوم السياسية، جامعة بغداد – بغداد – العراق، 2019، ص101.

[3] حسين باسم عبد الأمير، التحديات الأمنية المستجدة، مركز الدراسات الاستراتيجية، جامعة كربلاء، 28يناير 2021، على الموقع الإلكتروني: http://kerbalacss.uokerbala.edu.iq

والمجتمع العراقي، بل أن نسبة القرصنة السيبرانية في العراق هي الأعلى في الشرق الأوسط، وتنوعت حالات الجرائم السيبرانية في العراق، منها الغش عبر الانترنت، وغسيل الأموال، وتزايد مواقع القرصنة والتجارة السيبرانية غير المشروعة، والتطفل على الشبكات، والجنس، فضلاً عن هجمات الإرهاب الإلكتروني على المؤسسات الحكومية. وعند الرجوع إلى سجلات مكتب التحقيقات الجنائية العراقي للأعوام 2006م-2011م الخاصة بالجرائم السيبرانية، نلاحظ إن حالات جرائم الانترنت في العراق زادت خلال تلك السنوات بمعدل سنوي متوسط قدره (2.246)%، فخلال هذه المدة شهد العراق نمواً سريعاً لمستخدمي الانترنت، وزادت بالوقت ذاته الجرائم السيبرانية[1].

وبالتزامن مع الحرب على تنظيم (داعش) الإرهابي منذ عام 2014م، رصدت شركات أمنية مختصة بالأمن السيبراني إن هناك حرباً سيبرانية في العراق يتم فيها استعمال وسائل التواصل الاجتماعي لحشد المؤيدين ونشر الدعاية ولجمع المعلومات الأمنية عن طريق مجموعة من قراصنة الانترنت الذين يعملون على خداع الناس بإرسال رسائل تحوي شفرات وبرامج ضارة عبر وسائل التواصل الاجتماعي، وما أن يتم فحتها حتى يبدأ المهاجمون على الفور بالتحكم الكامل بالجهاز وسرقة الملفات أو استخدام كاميرا الكومبيوتر أو الميكرفون لمراقبة ما يجري للشخص المستهدف. وفي هذا الخصوص قال (أندرو كوماروف، Andrew Komarov) وهو الرئيس التنفيذي لشركة (أنتل كراولر، Intel Crawler) الأمريكية المختصة في مكافحة التهديدات السيبرانية (إن هناك بعض الجماعات في العراق تستخدم برامج ضارة، ومن الصعب التأكد من هويتهم، وقد استهدفوا بالفعل مدناً وجماعات معينة وحتى عائلات معينة، أي أن كل الهجمات السيبرانية هي انتقائية للغاية وتتأثر في معظمها بالأطراف المحلية المتصارعة)، وأضاف (إن المهاجمين يستهدفون ضحاياهم باستخدام وسائل التواصل الاجتماعي ويقومون أيضاً بالبحث عن أجهزة التوجيه في داخل العراق لتخريبها بأدواتهم الخاصة، وقد تركزت غالبية هذه الهجمات في بغداد والبصرة والموصل وأربيل، وكانت الغاية منها جمع المعلومات عن المظاهرات المحلية والأحزاب والاتصالات بين السكان المدنيين أو الحكومة والعكس بالعكس)[2].

[1] مصطفى إبراهيم سلمان الشمري، مصدر سبق ذكره، ص171.

[2] نقلاً عن: مصطفى إبراهيم سلمان الشمري، مصدر سبق ذكره، ص171.

وفي ذات السياق أفاد تقرير لشركة (انتل كراولر) في عام 2014م إن هناك جهات فاعلة تتخذ من العراق مقراً لها وتشارك في انشطة غير مشروعة مختلفة في الفضاء السيبراني تعمل كمرتزقة وقد زادت بشكل كبير، ولديها علاقات بجماعات أخرى في كل من مصر ولبنان وليبيا وإيران وسوريا، فضلاً عن دور الجماعات الإسلامية المنتشرة في العديد من الدول[1].

وتم ملاحظة أنه في الانتخابات العراقية لعام 2018م، جرى نشر الكثير من التسجيلات الصوتية لعمليات شراء مقاعد في مجلس النواب كذلك في عام 2019م تعرض نحو 30 موقع الكتروني للحكومة العراقية لحالة من الاختراق منها جهاز الأمن الوطني العراقي ووزارة الداخلية والصحة، وقد قام بعملية الاختراق مجموعة تدعى (ماكس برو) وتسريب معلومات وبيعها تتعلق بالأمن الوطني العراقي[2].

وفي 26 و 27 أيلول 2019م كان العراق قد تعرض إلى هجوم سيبراني من قبل قراصنة طالت قرابة (30) موقعاً حكومياً، أبرزها مواقع وزارة الدفاع والداخلية والخارجية والأمن الوطني والصحة، وقد استغل المهاجمون بعض الثغرات فعملوا على تطبيق التغييرات على بيانات موقع البحث التي من شأنها توجيه المستخدمين إلى صفحة بحث مختلفة. وعلى الرغم من أن الجهات الحكومية نجحت في استعادة سريعة لبعض المواقع إلا أن بعضها استغرق وقتاً اطول. علماً إن المهاجمين تمكنوا من الدخول إلى أجهزة الحواسيب الحكومية واختراق قاعدة البيانات التي من المفروض أن تكون محمية بشكل جيد، مما سمح لهم بأخذ معلومات كثيرة[3].

وغالباً ما تُعطل الصفحات الرسمية الخاصة بالوزارات الأمنية مثل وزارة الداخلية ومستشارية الأمن الوطني وجهاز مكافحة الإرهاب، ولعل أخطرها كان في 25 تشرين الثاني 2019م عندما تم اختراق الموقع الرسمي لجهاز مكافحة الإرهاب والاعلان عن انقلاب ضد الحكومة استجابة لدعوة المتظاهرين، إلا أن جهاز

---

[1] مصطفى إبراهيم سلمان الشمري، مصدر سبق ذكره، ص172.

[2] هيثم كريم صيوان ومهند جبار عباس، مصدر سبق ذكره، ص159-160.

[3] مصطفى إبراهيم سلمان الشمري، مصدر سبق ذكره، ص174.

مكافحة الإرهاب أعلن في موقعه الالكتروني الرسمي لاحقاً عن تعرض الموقع للاختراق وإن ما نشر فيه ليس صحيحاً[1].

ويشير تعقب السلطات الأمنية العراقية لـ(تنظيم الدولة الإسلامية – داعش) إلى تلك العلاقة بين التأثيرات السلبية لمواقع الانترنت على الأمن الوطني، إذ تنوعت أساليب استعمال هذه الوسائل من قبل الجماعات الإرهابية بين التخطيط والتنفيذ لأعمالهم الإجرامية، ونشر أفكار التطرف والعنف والترويج لها واستقطاب أعضاء جدد، وإمكانية نشر توترات بين مكونات المجتمع إلى جانب إجبار الدولة على اتخاذ إجراءات للضبط قد تؤثر في صورتها على المستوى الدولي[2]. كما يشير تعقب السلطات الأمنية العراقية إلى أن لـ(تنظيم داعش) ما يزيد عن (50) ألف موقع الكتروني، و(90) ألف صفحة باللغة العربية على مواقع التواصل الاجتماعي (فيس بوك)، و (40) ألفاً بلغات أخرى، وهذا ما ساهم في تجنيده لحوالي (3400) شاب شهرياً عبر حملاته الالكترونية. كما استغل تنظيم (داعش) الإرهابي الانترنت في بث عمليات الإعدام التي كان يقوم بتنفيذها على الأسرى، وذلك لبث الرعب والفزع في نفوس أهالي المدن التي كان يرغب في السيطرة عليها، وهو الأمر الذي تحقق جزئياً في هروب واستسلام مدن وقرى لتنظيم (داعش) الإرهابي خوفاً من تعرضهم للمصير نفسه من قبلهم، كذلك استغل التنظيم في تجنيد العديد من الشباب حول العالم، إذ بلغ عدد البلدان التي انضم منها أفراد إلى تنظيم (داعش) إلى (70) دولة[3].

**المطلب الثالث: مظاهر الإرهاب السيبراني في العراق**

تتمثل أبرز مظاهر الإرهاب السيبراني في العراق، بالآتي:

أولاً: الابتزاز الإلكتروني، الذي يتم من خلال الحصول على معلومات سرية أو صور شخصية أو مواد فيديوية لاستغلالها لأغراض مالية أو القيام بأعمال غير مشروعة، وتعدّ تلك الأعمال من أشد الجرائم خطورة

---

[1] سامر محي عبد الحمزة، مصدر سبق ذكره، ص533.

[2] أمل صقر، مخاطر واقعية كيف يهدد (التواصل الاجتماعي) الأمن الوطني، على الموقع الإلكتروني:
http://futureuae.com

[3] صلاح مهدي هادي وزيد محمد علي إسماعيل، الأمن السيبراني كمرتكز جديد في الاستراتيجية العراقية، مجلة قضايا سياسية، العدد 62، تموز – آب – أيلول، 2020، كلية العلوم السياسية، جامعة النهرين، بغداد – العراق، ص283.

لأنها تهدد حقوق الإنسان من خلال اختراق خصوصيته وتجعله عرضة للكثير من الآثار النفسية والاجتماعية[1]. ومما يساعد على استعمال الانترنت كوسيلة للابتزاز إن التواصل عن بعد يتيح فرصاً لتقمص الشخصيات. كما تتيح هذه التكنولوجيا وسائل مبتكرة للابتزاز كالتهديد بالوثائق المزورة والصور الفاضحة التي يتم تزييفها إلكترونياً بدرجة يصعب التفريق بينها وبين الصور الحقيقية، هذا فضلاً عن مصادر التهديد بأشكال أخرى كالنفاذ إلى الحاسبات الشخصية أو السرقة من خلال استعمال بطاقات الائتمان الخاصة بالغير في المعاملات التجارية الإلكترونية[2].

لقد راح عدد غير قليل من العراقيين، ولا سيما النساء منهم، كضحايا لعمليات الابتزاز الالكتروني ، وذلك نتيجة التفاعل الكبير مع منصات التواصل الاجتماعي. فقد كشفت السلطات القضائية العراقية إن الأشهر الأولى من العام 2022م تم تسجيل نحو (2400) حالة ابتزاز الكتروني، وكان لبغداد النصيب الأكبر منها. بينما سجل العام 2021م وفق احصائية كشفت عنها مديرية الشرطة المجتمعية بوزارة الداخلية (1950) حالة ابتزاز الكتروني، كان معظم ضحاياها من النساء بينهن فتيات في سن المراهقة وأطفال دون سن الـ(14) سنة[3].

ثانياً: التجسس الإلكتروني، أي القدرة على الدخول غير المشروع والاطلاع على شبكات الخصم من دون أن يصاحب ذلك تدمير أو تخريب للبيانات والمعلومات، بهدف الحصول على المعلومات التي قد تشمل خطط عسكرية دفاعية أو هجومية، أو مخططات سرية حربية كانت أم سلمية، أو دراسات وأبحاث استراتيجية، فضلاً عن استطلاعات سياسية واستخباراتية. كما يمكن من خلال هذه العملية اعداد خرائط لشبكات الحاسب الآلي واستعمالها مستقبلاً لتنفيذ عمليات إرهابية في الفضاء السيبراني[4]. وتعدّ برامج التجسس نوع خاص من البرامجيات الخبيثة التي تعمل على مراقبة كل ما يكتب، إذ تقوم بتسجيل النقرات على لوحة المفاتيح وترسلها إلى المخترق وغيرها من الأعمال الخبيثة الأخرى. وتقوم هذه البرامج بتنفيذ مهامها عن طريق الاتصال

---

[1] عبد الرحمن عبد الله السند، جريمة الابتزاز، مكتبة الملك فهد الوطنية، الرياض – المملكة العربية السعودية، 2018، ص18.

[2] جعفر حسن الطائي، الإرهاب المعلوماتي وآليات الحد منه، مجلة العلوم القانونية والسياسية، كلية القانون والعلوم السياسية، جامعة ديالى، ديالى – العراق، 2015، ص499.

[3] وكالة يقين للأنباء، ضحايا الابتزاز الالكتروني في العراق (ملف)، 5 يوليو 2022، على الموقع الالكتروني: yaqinnews.net

[4] جعفر حسن الطائي، مصدر سبق ذكره، ص270.

بالشبكات الاجتماعية أو موقع ما على شبكة الانترنت، وتقوم بجمع المعلومات حول ما يقوم به المستخدم من أنشطة سواء عبر الانترنت أو في وضع عدم الاتصال بالانترنت على الجهاز الخاص بالضحية وإرسال هذه المعلومات للمخترق فور اتصال الحاسب الآلي الانترنت[1]. على إن أهم ما يهدف إليه التجسس الالكتروني هو زعزعة الأمن ونشر الخوف والرعب والإخلال بالنظام العام للدولة وتهديد الأشخاص والسلطات العامة والمنظمات الدولية والسطو وجمع الأموال، فضلاً عن جذب الانتباه والدعاية والإعلان.

لقد كشفت صحيفة أمريكية عن أن هاتف الرئيس العراقي السابق (برهم صالح) كان على قائمة تضم (50) ألف رقم أختيرت من أجل احتمال استهداف أصحابها بالمراقبة ببرنامج (بيغاسوس، Pegasus) للتجسس، وذكرت صحيفة (واشنطن بوست، Washington Post) إنه لم يتسن التحقق فيما إذا كان برنامج (بيغاسوس) الذي تنتجه شركة (إن إس أو، NSO) الإسرائيلية قد أصاب هاتف (برهم صالح) أو ما إذا كانت قد نُفذت أصلاً أي محاولة لذلك[2].

ثالثاً: الاختراق الإلكتروني، الذي يقوم به الإرهابيون المبرمجون، الذين يطلق عليه بـ(الهاكرز أو قراصنة الحاسوب) من خلال اختراق المواقع أو الحواسب الإلكترونية باستعمال برامج التجسس على الشبكات والأنظمة الإلكترونية، والاعتداء على البنية التحتية المعلوماتية للمؤسسات الحكومية والخاصة على حدٍ سواء بما في ذلك البريد الإلكتروني، واشتراكات المستخدمين، والأرقام السرية للبطاقات الائتمانية وما إلى ذلك[3]. وعليه فإن ارتكاب جرائم الأتلاف والتشويه للبيانات والمعلومات وبرامج الحاسب الآلي بإطار جرائم الإرهاب الإلكتروني، يتم باستعمال الفايروسات الإلكترونية بقصد الحصول على معلومات متعلقة بالأماكن والمنشآت الحيوية لاستهدافها بالعمليات الإرهابية أو من أجل تدمير أو تعطيل في برامج الحواسيب. ومن الأساليب المستعملة لتدمير المواقع أيضاً ضخ كميات هائلة من الرسائل الإلكترونية إلى الموقع المستهدف بالتدمير

---

[1] عبد الله اليوسف، التقنية والجرائم المستحدثة – الظواهر الإجرامية وسبل معالجتها، أكاديمية نايف العربية للعلوم الأمنية، الرياض – المملكة العربية السعودية، 1999، ص155.

[2] قناة الجزيرة، واشنطن بوست: رئيس العراق على قائمة أهداف برنامج التجسس الإسرائيلي، 2021/7/21، على الموقع الالكتروني: www.aljazeera.net

[3] عادل عبد الصادق، الإرهاب الإلكتروني – القوة في العلاقات الدولية – نمط جديد وتحديات مختلفة، مصدر سبق ذكره، ص135.

مما قد يؤثر على سعته التخزينية ويؤدي في نهاية المطاف إلى تفجير الموقع وتشتيت بياناته وانتقال معلوماته لجهاز الشخص الذي اخترقه[1].

في 28 أيلول 2016م تعرض موقع مستشارية الأمن الوطني في العراق للاختراق الالكتروني، إذ نشر المخترقون صورة (كاريكاتورية) لمستشار الأمن الوطني (فالح الفياض) مع كتابة عبارة في الموقع (إن موقعكم لم تقوموا بحمايته فكيف تحافظون على أمن الشعب). ويقدم الجدول الآتي اختراق المواقع الالكترونية لوزارات عراقية عدة بين عامي 2016م ومطلع عام 2017م[2].

جدول (1)

تواريخ اختراق مواقع الكترونية لوزارات عراقية بين عامي 2016م ومطلع عام 2017م

| اسم الوزارة | تاريخ الاختراق |
|---|---|
| موقع رئيس الوزراء العراقي | 2016/3/23م |
| موقع مجلس النواب العراقي | 2016/6/8م |
| موقع وزارة الداخلية | 2016/7/3م |
| موقع الاستمارة الالكترونية للتعيين على ملاك وزارة الصحة | 2016/8/22م |
| موقع وزارة الاتصالات | 2016/10/11م |
| الموقع الرسمي للمفوضية العليا المستقلة للانتخابات | 2017/2/12م و 2017/2/13م |
| موقع وزارة الشباب والرياضة | 2017/6/2م |

المصدر: صلاح مهدي هادي الشمري وزيد محمد علي إسماعيل، الأمن السيبراني كمرتكز جديد في الاستراتيجية العراقية، مجلة قضايا سياسية، العدد 62، السنة الثانية عشر، 2020، كلية العلوم السياسية، جامعة النهرين، بغداد – العراق، ص280.

ولنا في الانتخابات التي جرت في عام 2018م مثال على ذلك، فعملية التصويت تمت بالاعتماد على نظام الأقمار الصناعية والتي لا يمكن التحكم بها لأنها تدار من خارج العراق، لذا زادت احتمالية اختراقها والتلاعب بنتائجها من قبل جهات خارجية، فضلاً عن ذلك فإن العراق تبنى مشروعاً لتوطين

[1] عبد الرحمن بن عبد الله السند، وسائل الإرهاب الإلكتروني – حكمها في الإسلام وطرق مكافحتها، بلا، 2010، ص141.

[2] صلاح مهدي هادي الشمري وزيد محمد علي إسماعيل، مصدر سبق ذكره، ص280.

الرواتب الذي تديره الكثير من الشركات المالية والتي باتت تحتفظ بالمعلومات الشخصية للموظفين داخل أجهزة الكترونية خارج البلاد وكذلك أيضاً اختراق مواقع الكترونية مهمة تابعة للحكومة العراقية وأهمها موقع جهاز الأمن العراقي وكذلك أيضاً استخدام التكنولوجيا ومنصات التواصل الاجتماعي في التحشيد لتظاهرات تشرين في عام 2019م[1].

## المبحث الثالث: تحليل استراتيجية مكافحة الإرهاب السيبراني في العراق ومتطلباتها

تمثل تهديدات الأمن السيبراني، تحديات غير مرئية تؤثر على منظومة الأمن الوطني العراقي. فالتطور التكنولوجي الذي شهده العراق في مجال المعلومات والاتصالات خلال العقد الثاني من الألفية الثالثة والذي تزامن مع ضعف الأمننة لدى البنية التحتية الوطنية (أمنية أو مصرفية أو شخصية) أدى إلى أن يصبح العراق منكشفاً أمام التهديدات بمختلف أشكالها، كالتجسس على المعلومات الخاصة بالمؤسسات الأمنية، واستعمال العراق كساحة لشن الهجمات الالكترونية لضرب أمن معلومات أي دولة كانت واختراقه، فضلاً عن استراق أي معلومة واستعمالها لأغراض المساومة، أي لتنفيذ عمليات إرهابية وإسنادها. ومن الملاحظ إن أكثر المؤسسات العراقية تتعاقد لتجهيز معلوماتها من أقمار صناعية ذات مورد خدمة واقع خارج الحدود العراقية، الأمر الذي يؤدي إلى مرور تلك المعلومات في خوادم تلك الدول، ورجوعها إلى العراق، وبالتالي فإن هذا الإجراء يشكل خرقاً لأمن المعلومات العراقي[2]. وعليه، لا بد لاستراتيجية الأمن السيبراني العراقي أن تنطلق من مبدأ أساس هو ضمان أمن العراق وحماية وجوده في الفضاء السيبراني، وحماية بنية معلوماته الحيوية، وبناء مجتمع انترنت موثوق به ورعايته والتعامل مع التحديات السيبرانية التي تهدد أمن العراق وسلامته، عن طريق تبني مجموعة من الإجراءات التي تعمل على حماية فضاء العراق السيبراني والدفاع عنه[3]، لذا ارتأينا مناقشة موضوع هذا المبحث في المطالب الثلاث الآتية:

---

[1] هيثم كريم صيوان ومهند جبار عباس، مصدر سبق ذكره، ص158-159.

[2] علي زياد العلي، التحديات غير المرئية للأمن الوطني العراقي، مركز البيان للدراسات والتخطيط، على الموقع الالكتروني: https://www.bayancenter.org وكذلك : علي حسين حميد وعلي زياد عبد الله، تحليل البيئة الاستراتيجية العراقية من منظور أمني، مجلة حمورابي، العدد 33-34، السنة الثامنة، شتاء – ربيع 2020، ص222-223، pdf، على الموقع الإلكتروني: https://www.iasj.net

[3] مصطفى إبراهيم سلمان الشمري، مصدر سبق ذكره، ص170.

**المطلب الأول: واقع الأمن السيبراني في العراق**

تعددت التعريفات المقدمة من قبل الباحثين بشأن الأمن السيبراني فمنهم عرفه بأنه عبارة (عن مجموعة من الوسائل التقنية والتنظيمية والإدارية التي يتم استعمالها لمنع الاستعمال غير المصرح به وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي يحويها، وذلك بهدف ضمان توافر واستمرار عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية، واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من مخاطر الفضاء الإلكتروني)[1]. كما يمكن أن يشير الأمن السيبراني إلى (حماية المعلومات من الوصول غير المسموح به، ويشمل جميع المفاهيم والتقنيات والتدابير التقنية والإدارية المستعملة لحماية أصول المعلومات من الوصول غير المأذون به عمداً أو سهواً أو حيازتها أو الإضرار بها أو كشفها أو التلاعب بها أو تعديلها أو فقدها أو اساءة استعمالها). أي أن الأمن السيبراني هو حماية المعلومات وعناصرها المهمة بما في ذلك الأنظمة والأجهزة التي تستعمل هذه المعلومات وتخزنها وترسلها. ويركز أمن السيبراني على المحاور الآتية[2]:

1. حماية المعلومات من الضرر بأشكاله كافة، سواء كان مصدره أشخاص/مخترقين أو برامج/فيروسات، أو كان متعمداً أو عن طريق الخطأ.
2. حماية المعلومات من الوصول غير المصرح به، أو السرقة أو الالتقاط، أو التغيير، أو إعادة التوجيه، أو سوء الاستعمال.
3. حماية قدرة المؤسسات على الاستمرار وأداء أعمالها على أحسن وجه.
4. تمكين أنظمة تقنية المعلومات والبرامج التطبيقية من العمل بشكل آمن.

ومنذ عام 2004م، وهو العام الذي تم فيه إقرار قانون المفوضية العليا للاتصالات والإعلام وقانون اللجنة الوزارية للأمن القومي (كما تمت الإشارة إلى ذلك في الصفحات السابقة)، فإنه لم يحدث أي تغيير رئيس في هذه السياسة، بل أن قرارات سلطة الأئتلاف المؤقتة المنحلة بشأن القانونين السابقين لازالت نافذة

---

[1] نقلاً عن: علي أدهم، الأمن السيبراني، مركز النهرين للدراسات الاستراتيجية، تاريخ النشر2019/3/13، على الموقع الإلكتروني: http://www.alnahrain.iq

[2] ديب بن عايض القحطاني، أمن المعلومات، الرياض – المملكة العربية السعودية، 2015، ص58.

على الرغم من مرور ما يقارب العقدين منذ إلغاء سلطة الأئتلاف المؤقتة. وهو الأمر الذي يدل على تجاهل أخطار الواقع السيبراني كما أشار إلى ذلك تقرير المنظمة العربية للاتصالات والمعلومات عام 2021م[1]. الأمر الذي يدعونا إلى القول بأن العراق يعدّ في مراحله الأولية فيما يتعلق بمواجهة الجريمة السيبرانية، فهذه الجريمة ليست من اهتمامات المجتمع العراقي الرئيسة، علماً إن وزارة التخطيط العراقية أعلنت في عام 2013م إن الجزء الرئيس من الجرائم السيبرانية المرتكبة قد استعملت مواقع التواصل الاجتماعي وفي مقدمتها الفيس بوك، وشملت هذه الجرائم الاختطاف والتهديد واختراق المعلومات الشخصية والمخدرات والاحتيال وغيرها، وتم القبض على بعض الأشخاص الذين ارتكبوا جرائم الانترنت[2].

واستناداً إلى مؤشر الأمن السيبراني العالمي لعام 2017م ( Global Cybersecurity Index, GCI) الصادر عن الاتحاد الدولي للاتصالات التابع إلى الأمم المتحدة كونه الوكالة المختصة في مجال تكنولوجيا المعلومات والاتصالات، فقد احتل العراق المرتبة (158). وفي العام 2018م، احتل العراق وفق المؤشر ذاته المرتبة (107) على الصعيد العالمي من أصل (175) دولة شملها التقرير، والمرتبة (13) على صعيد الدول العربية[3]. الأمر الذي يدعو إلى القول بأن هناك تحسن يعزى إلى القائمين عليه، إلا أنه عاد وانتكس مرة أخرى في عام 2021م، إذ وفقاً لتقرير الاتحاد الدولي للاتصالات فإن العراق هو الـ(20) من مئة درجة، واحتل المرتبة (129) من أصل (182)، إذ يقع في ترتيب الدول الأضعف في الأمن السيبراني، تتفوق عليه غالبية الدول العربية حتى الدول الضعيفة في القدرات المالية والفنية مثل السودان ولبنان وسوريا وفلسطين[4]. وأشار التقرير ذاته، إلى أن العراق لم يقدم إجابات عن الاستبيان الذي جمعه فريق (GCI) الذي تضمن بعض المعلومات والبيانات، وهو الأمر الذي يجب معرفته حول سبب هذا التجاهل أو التهاون للجهات المسؤولة عن هذا الملف في العراق، وانعدام وجود مؤسسات متخصصة بالأمن السيبراني في العراق

---

[1] سامر محي عبد الحمزة، مصدر سبق ذكره، ص532.

[2] مصطفى إبراهيم سلمان الشمري، مصدر سبق ذكره، ص171.

[3] المصدر السابق نفسه، ص173.

[4] سامر محي عبد الحمزة، مصدر سبق ذكره، ص532.

كما في الدول العربية والإقليمية، وكل ما هو موجود هو عبارة عن أقسام في دوائر مختلفة تفتقد للتنسيق والتعاون المحترف في هذا الجانب، فكل جهة تعمل بصورة منفردة عن الأخرى[1].

إن احتلال العراق مكانة متدنية في مؤشرات الأمن السيبراني العالمي والعربي، وضعه أمام إشكالية خطيرة تتمثل بالانكشاف وسهولة اختراق أمنه السيبراني، وعليه يمكن أن نحدد ملامح البيئة السيبرانية للعراق وكالآتي[2]:

1. دولة مكشوفة أمام القوى السيبرانية والتنظيمات الإرهابية.
2. تدني البنى التحتية الرقمية فيه.
3. يعاني التخلف الأمني الرقمي ولاسيما في الميدان الاقتصادي والحوسبة المالية والمصرفية.
4. زيادة احتمالية تعرضه لشن هجمات سيبرانية عليه قد تستهدف المراسلات الحكومية أو سرقة الأسرار الأمنية والاقتصادية والاجتماعية للبلد.
5. تعاظم تعرضه للإرهاب الإلكتروني والتجسس والقرصنة الإلكترونية وعمليات غسيل الأموال واستعمال شبكات الانترنت لممارسة النصب والاحتيال والجريمة الإلكترونية والاتجار بالبشر والمخدرات.

وهكذا يتضح تأثير المخاطر السيبرانية على الأمن الوطني والاقتصاد العراقي من خلال مؤشرات عديدة، ومنها: عدم فعالية البنى الرقمية التحتية في العراق، الذي يعد متخلفاً في مجال التوبيب الرقمي وخصوصاً في المجال الاقتصادي. فالعراق في الفضاء المعلوماتي لا يعيش عصر العزلة، بل أنه مترابط مع دول أخرى في هذا الفضاء عبر شبكات ترابطية للبنى المعلوماتية التحتية، حتى صار بالإمكان عبر ذبذبات الاتصال الرقمي تنظيف خزينة العراق من أموالها بواسطة نظاماً حاسوبياً يتم إدارته من غرفة في قرية تبعد عن دولتنا آلاف الكيلومترات، فتلك الموجات الأثيرية تهاجم مركز الثقل في تطور الدولة وتسيطر على قدرات العراق

---

[1] ماجد صدام سالم، الأمن السيبراني وأثره في قوة الدولة، مجلة العلوم التربوية والإنسانية، العدد 18، ديسمبر 2022، ص76، pdf، على الموقع الالكتروني: www.jeahs.com

[2] هيثم كريم صيوان ومهند جبار عباس، مصدر سبق ذكره، ص159-160.

وتتحكم بكافة مقدراته، وتستهدف المراسلات الحكومية لتقوم بعملية تدمير تلك الوسائط الالتكترونية، وتستهدف الأسرار الأمنية والاقتصادية وأيضاً الاجتماعية للبلد[1].

**المطلب الثاني: مكامن الخلل في الأمن السيبراني العراقي**

يتمثل الخلل الكبير الذي يواجه تنظيم الفضاء السيبراني وشبكات الانترنت في العراق بالآتي[2]:

1. ضعف القوانين والتشريعات الحكومية الخاصة بالأمن المعلوماتي والسيبراني. بل عدم وجود قانون ينظم الأمن الوطني السيبراني. ويكفي أن نشير هنا إلى المخاض العسير الذي يمر به قانون الجرائم الإلكترونية الذي تم مناقشته في مجلس النواب منذ عام 2011م ولا يزال مشروعاً مطروحاً في مجلس النواب منذ أكثر من عشر سنوات ولم يرَ النور حتى هذه اللحظة بسبب سوء الصياغة والمبالغة في العقوبات التي وردت فيه.

2. عدم وجود هيئة مختصة بالأمن السيبراني: إذ لا توجد حالياً هيئة مستقلة للأمن السيبراني، على الرغم من ذلك نلاحظ إن العراق قد حاول أن يساير بعض الدول في موضوع الأمن السيبراني فأنشأ هيئة وحيدة للأمن السيبراني هي (فريق الاستجابة السريعة للأحداث السيبرانية) وهي هيئة تابعة لمستشارية الأمن الوطني (التي هي ذاتها تفتقر لقانون ينظمها) والفريق مازال في بداية تكوينه، كما أن موقعه الالكتروني يتعرض للاختراق أكثر من مرة. وتتهمه بعض وسائل الإعلام بالفساد الإداري وإن أعضاؤه يعملون في مكاتب خاصة تتقاطع مع عملهم في هذا الفريق. وعلى الرغم من أن الحكومة العراقية كانت قد حاولت تطوير عمل هذا الفريق حينما طلبت رسمياً من حلف شمال الأطلسي/ الناتو تدريب أعضاء الفريق البالغ عددهم (16) موظفاً للمدة من 21 تشرين الثاني لغاية 2 كانون الثاني 2016م، وكان البرنامج التدريبي قد تضمن جلسات نظرية ومختبرية عملية عن أساسيات الدفاع السيبراني وحماية البيانات من التسرب وتحليل الشفرات والأدلة الالكترونية ورفع مستوى الخبرة التقنية لحماية الشبكة الوطنية وزيادة الوعي بالأمن السيبراني، وستعمل هذه الدورات على تعزيز قدرات الدفاع السيبراني الوطنية العراقية، إلا أن إمكانيات الفريق تبقى متواضعة قياساً بحجم التحديات التي يفترض به مجابهتها.

---

[1] مروران سالم العلي، التحديات الاستراتيجية للأمن الوطني العراقي في ظل المتغيرات الدولية، مجلة تكريت للعلوم السياسية، العدد 20، 2020، جامعة تكريت، صلاح الدين – العراق، ص57.

[2] مصطفى إبراهيم سلمان الشمري، مصدر سبق ذكره، ص175. وكذلك ينظر: سامر محي عبد الحمزة، مصدر سبق ذكره، ص533.

3. ضعف القدرات المهنية المحلية وقلتها في مجال أمن المعلومات المقدمة والأمن السيبراني.

4. ارتباط منظومات الانترنت في العراق بالخارج، الأمر الذي يعني إن الأمن السيبراني مرتبط بالنتيجة بدول وشركات خارجية.

5. قلة إدراك الشركات المحلية في مجال تكنولوجيا المعلومات بحجم المخاطر الأمنية المعاصرة.

وفي عام 2017م، أصدر فريق الاستجابة السريعة للأحداث السيبرانية، ما أسماه بـ(استراتيجية الأمن السيبراني العراقي، ICS) في (11) صفحة. وعلى الرغم من أن نشر هذه الوثيقة يعدّ خطوة يجدر الإشادة بها لأنها تعرض للأولويات المتزايدة للمجال السيبراني كما أنها كانت بمنزلة أول جهد كبير وعام تبذله الدولة العراقية، من أجل تحليل مكامن الخلل في السياسة الالكترونية الوطنية، ولرسم خريطة طريق لتأسيس بنية تحتية الكترونية فوقية للبلاد لوضع العراق على قدم المساواة مع نظرائه الإقليميين والدوليين وحلفائه. بيد أن الاستراتيجية ذاتها يشوبها عيوب واضحة، إذ أنها فشلت، بالعموم، في تحفيز تطبيق الإطار الذي يقترحه. فكانت استراتيجية الأمن السيبراني المنشورة استراتيجية نظرية بالأساس، وتوضح تفصيلاً التهديدات العامة التي تواجه الجهات الفاعلة الخاصة والعامة في الفضاء السيبراني، بدلاً من التركيز على طبيعة التهديدات الالكترونية التي يواجهها العراق خصوصاً. ومن ثم، لم تحاول الاستراتيجية توفير ما يمكن عدّه تحليلاً أو مخططاً ملموساً لتصنيف البنية التحتية الحيوية التي يمكن أن تكون موضع استهداف متكرر[1].

ومن جهة ثانية، فإن استراتيجية الأمن السيبراني كانت قد تضمنت ما يفترض أنه يمثل جوهر سياسة الدولة المتعلقة بحماية الأمن السيبراني، فإنه يلاحظ بأن فريق الاستجابة السريعة للأحداث السيبرانية، لم ينشر تلك الاستراتيجية في موقعه، وإنما الورقة متاحة فقط على موقع الاتحاد الدولي للاتصالات ضمن قسم تقارير الدولة، وكأن الفريق أراد منها فقد اظهار رسالة للعالم مفادها وجود جهاز أمن سيبراني في العراق من غير اهتمام حقيقي بالموضوع. والاستراتيجية جاءت مخيبة للآمال كثيراً إذ لم تتضمن طبيعة المشاكل وتحديد المهام التي يجب انجازها لتعزيز الأمن السيبراني، إذ ورد فيها عبارات عامة تشير إلى التمني والرغبة وليس

[1] هاشم شبر، تنظيم الجهد المؤسسي والوزاري المشترك إزاء الأمن السيبراني في العراق، مركز البيان للدراسات والتخطيط، على الموقع الالكتروني: bayancenter.org

سياسة جادة لمواجهة المشكلة، كعبارة (ضرورة انشاء قوانين سيبرانية جديدة مثل قانون أمن الاتصالات) وعبارة (ضرورة انشاء منصة مركزية للعمل السيبراني) و(العمل على سد الفجوة الأمنية السيبرانية).

ومن جهة ثالثة، كانت استراتيجية الأمن السيبراني العراقي قد تضمنت مدد زمنية تتراوح بين عام وخمسة أعوام لانجاز المهام أعلاه، غير أنها لم تبين من هي الهيئة المكلفة بانجاز كل هذه المهمات الصعبة في ظل عدم وجود قانون للأمن السيبراني أو هيئة مستقلة له أو حتى بنية تحتية لهذا المشروع، وكيف يمكن إنشاء قوانين سيبرانية في وقت لم تتم المصادقة على قانون الجرائم المعلوماتية المطروح على مجلس النواب منذ أكثر من 10 سنوات. زد على ذلك، فشلت الوثيقة في تحديد الجهة أو المؤسسة الحكومية التي ستكون مسؤولة عن تنفيذ توصياتها أو خططها أو أهدافها، كما أنها لم تقدم برامج استراتيجية مفصلة أو مدد تنفيذ للاستراتيجية المذكورة[1]. لذا نحن مع الرأي القائل بأن هذه الاستراتيجية هي رؤية غير واقعية ولا يمكن الركون إليها لتحقيق الأمن السيبراني العراقي وهي إن دلت على شيء فتدل على انعدام رؤية واضحة للأمن السيبراني في العراق.

**المطلب الثالث: متطلبات استراتيجية مكافحة الإرهاب السيبراني في العراق**

لقد أضحى أمن الفضاء السيبراني من استراتيجيات الأمن القومي للكثير من دول العالم من أجل الاستحواذ على مصادر القوة داخل هذا الفضاء، وللدفاع عن البنية التحتية الحيوية ضد أي هجوم سيبراني مثل قطع خدمة الانترنت أو ضرب مواقعه أو توقيف رسائل البث التلفزيوني أو الإذاعي أو إيقاف موجهات الراديو أو تعطيل شبكات المحمول أو البث الفضائي، ليصل تأثيرها على كل مفاصل الدولة الحيوية[2]، لذا لا يمكن لأي دولة في العالم سواء كانت متقدمة أم نامية أن تهمل أو تتجاهل الأمن السيبراني. وإذا كان وجود استراتيجية للأمن السيبراني بهذه الأهمية للدول، فإن العراق هو بأمس الحاجة لمثل هذه الاستراتيجية، لاسيما وأنه يعدّ من أكثر الدول التي تتعرض للإرهاب السيبراني. يقتضي الأمر وضع وتنفيذ خطة وطنية للأمن السيبراني من خلال استراتيجية شاملة تشمل استعراضاً عاماً أولياً لمدى كفاية الممارسات الوطنية الحالية والنظر في دور جميع أصحاب المصلحة (الهيئات الحكومية، القطاع الخاص، والمواطنين) في هذه

[1] هاشم شبر، مصدر سبق ذكره.

[2] هيثم كريم صيوان ومهند جبار عباس، مصدر سبق ذكره، ص149-150.

العملية. ولأسباب تتعلق بالأمن القومي والرفاه الاقتصادي، تحتاج الحكومة إلى المساعدة في عملية حماية البنية التحتية لمعلوماتها الحيوية، وتعزيز هذه الحماية وضمانها لا يمكن الوصول إليه إلا من خلال وجود استراتيجية وطنية تعنى بالأمن السيبراني، في المجالات الآتي[1]:

- حماية خصوصية المواطن وغير ذلك من البيانات من الضياع والتغييرات الضارة والاستعمال غير المصرح به.
- مرونة الخدمات الحكومية والنظم والبنية التحتية للتهديدات الالكترونية.
- استمرارية الحكومة أثناء وبعد الحوادث السيبرانية الخطيرة.
- حماية أمن الخدمات الرقمية للمواطنين.
- تنسيق الاستجابة للتهديدات ضد البنية التحتية.
- أمن وسلامة البنية التحتية الأساسية للحكومة.

على إن استراتيجية مكافحة الإرهاب السيبراني في العراق لا بد لها وأن تقوم على المرتكزات الآتية[2]:

1. المرتكز التشريعي والقانوني والقضائي حول الأمن السيبراني: من خلال توفير معايير وأنظمة وطنية لأمن الفضاء الالكتروني في كل من القطاعين العام والخاص، ويوجد بيئة قانونية مواتية للمؤسسات وتفعيل بيئة ملائمة لملاحقة الجريمة السيبرانية والإرهاب السيبراني مع ضمان الحريات المدنية.
2. المرتكز التقني، من خلال توفير مؤسسات فنية وذات كفاءة عالية تستطيع التعامل مع التحديات السيبرانية.
3. المرتكز التنظيمي، من خلال إيجاد مؤسسات واستراتيجيات خاصة برسم وصناعة السياسات لتطوير الأمن السيبراني على المستوى المحلي.

---

[1] صلاح مهدي هادي وزيد محمد علي إسماعيل، مصدر سبق ذكره، ص285.

[2] هيثم كريم صيوان ومهند جبار عباس، مصدر سبق ذكره، ص163. وكذلك ينظر: فريق الاستجابة للأحداث السيبرانية، استراتيجية الأمن السيبراني 2022 – 2025 (مسودة نهائية)، ص15، pdf، cert.gov.iq . وكذلك ينظر: ماجد صدام سالم، مصدر سبق ذكره، ص77. وكذلك ينظر: هاشم شبر، مصدر سبق ذكره. وكذلك ينظر: حازم حمد موسى، الرؤية الاستراتيجية للأمن الوطني العراقي في الفضاء السيبراني، المجلة الجزائرية للعلوم القانونية والسياسية، المجلد 57، العدد 5، السنة 2020، pdf، على الموقع الالكتروني: www.asjp.cerist.dz

4. تأسيس (الهيئة الوطنية للأمن السيبراني العراقي)، كما في بعض الدول التي وعت قبل حين أهمية الأمن السيبراني، وتشكيل هيئة عالية المعرفة تشرف على هذا الأمن الخطير وتكون النواة الحقيقية للحوكمة الالكترونية التي طال انتظارها، وتكون هناك مديرية في كل المؤسسات بذات الاسم تتابع البرمجيات والمعدات التي يتم شراؤها من الأسواق المحلية والكشف عليها قبل دخولها الخدمة ومتابعة وسائل الحماية من برمجات مختلفة، يقودها مختصون في هذا المجال، يأخذون على عاتقهم التوسع في ادخال المعدات الحديثة ليمتلكوا الأهلية لقيادة تلك الهيئة مع بعض التدريب في الدول التي تمتلك القابليات في هذا المجال، فضلاً تهيئة الموازنة الكافية لتغطية نفقات تلك الهيئة التي ستكون في اطار وزارة الدفاع وجهاز الأمن الوطني العراقي.
5. ركيزة بناء قدرات العراق، إذ إنه ما زال يعاني من قلة التخصيص للبحث والتطوير والتعليم والتدريب التي تعمل على بناء تلك القدرات كي يستطيع أن يتعامل مع متغيرات الفضاء السيبراني.
6. المرتكز الاجتماعي، إن الفضاء الالكتروني للخدمات والتطبيقات ذو مساحة واسعة من اهتمام المجتمع العراقي، وكما فيه الكثير من الإيجابيات فهو يحمل الأخطار كذلك، لذا يتوجب زيادة توعية المجتمع والفرد تجاه الأفكار والمخاطر التي يمكن الوصول إليها والتأثير في مستواه المنطقي واستغلال ممتلكاته الرقمية الشخصية لحمايته، فهو النواة الأساسية في بناء المجتمع وحضارته، إذ تتوافر على منصات التواصل الاجتماعي الكثير من المواد والأفكار المتطرفة والإرهابية والأشخاص المتصيدين لقليلي الوعي عبر ابتزازهم واستغلال عدم تواصلهم مع الجهات المعنية في السيطرة وفرض القانون.
7. ضرورة بناء تعاونات وشراكات وتحالفات في مجال السيبرانية، إذ أن العراق لا يزال يعاني من عزلة إقليمية ودولية واغتراب في مجال الفضاء السيبراني، لذا لا بد له من إقامة شراكات تعاونية وشبكات لتبادل المعلومات، كما أنه لا يزال لا يملك اتفاقيات ثنائية مع الأطراف الإقليمية والدولية والعقود الاستراتيجية مع القطاع الخاص الدولي لتفعيل عمل حماية الأمن السيبراني.
8. العمل مع شركاء دوليين – من القطاعين الخاص والعام – لإطلاق قمر صناعي عراقي للاتصالات لتأسيس البنية التحتية الأساسية اللازمة لنظام أمن المعلومات المتكامل.

9. تحفيز قدرات القطاع الخاص في دول العالم الثالث بتوظيفهم في العراق، وذلك لسد الفجوة الحالية في الخبرة الفنية والمهنيين، وتهيئة قاعدة يمكن عن طريقها رعاية رأس المال البشري العراقي وتطويره وتشجيعه على المدى الطويل.

**الخاتمة**

على الرغم من الجوانب الإيجابية العديدة للفضاء السيبراني، المتمثلة في سهولة الحصول على المعلومات، وسرعة تبادلها، والمرونة في التعاملات على كافة المستويات الاجتماعية والتجارية والاقتصادية وغيرها، إلا أن الجوانب السلبية تفوق تلك المزايا بمراحل، إذ أن ما يميز شبكة الانترنت والفضاء السيبراني، بشكل عام، هو الانفتاح، كونه لا يعترف بالحدود القومية للدول، وهذه الميزة جعلته عرضة للنشاط الاجرامي وتعدياته. فلا توجد دولة مهما عظمت قدراتها العسكرية، ولا مؤسسة مهما عظمت قوتها الاقتصادية، في مأمن من خطر التهديدات السيبرانية، التي تتنوع ما بين تدمير أنظمة الكترونية لمنشآت حيوية عسكرية أو مدنية، وتعطيل أو اتلاف شبكات الدفاع العسكرية عن بعد، واختراق أو تعطيل أو تدمير شبكات القطاع الخاص، وتعطيل البنية التحتية للدول، والتدخل في سلامة البيانات العسكرية الداخلية لدول أخرى، ومحاولة إرباك أو التشويش على معاملاتها المالية.

وإذ أن مخاطر أمن المعلومات باتت ترقى إلى مستوى تهديد الأمن الوطني ككل، فإن وسائل المواجهة والحماية لا بد وأن تظللها منظومة أمن وطني، لأنه من غير المعقول أن تكون الأخطار والتهديدات شاملة وربما منسقة ومخططة أحياناً، ثم تأتي سبل ووسائل مواجهتها جزئية وعفوية وخالية من التخطيط وتفتقر للتنسيق والرشد، إذ ينبغي البدء بتنفيذ برنامج شامل على مستوى مؤسسات وهيئات الدولة والشركات الخاصة يستهدف التدريب على صد الهجمات الإلكترونية الشاملة بتنويعاتها المختلفة، سواء بالفيروسات أو والتجسس الاقتصادي أو التخريب الإلكتروني أو هجمات تعطيل شبكات الاتصالات والمعلومات.

**Conclusion:** Despite the many positive aspects of Cyberspace, that is the ease of obtaining information, the speed of its exchange, and the flexibility of dealing with all social, commercial and economical levels. However, the disadvantages are outweigh those advantages. Generally, what distinguishes the internet and Cyberspace is openness as it doesn't recognize the national borders of states, and this feature made it vulnerable to criminal activity and its transgressions. Furthermore, there is no state, no matter how great its military capabilities nor an institution with great economic power will be safe from the danger of cyberspace threats which vary from the destruction of electronic system to vital military or civilian installations, and disabling or damaging military defense networks remotely. Moreover, it also destroys private sector networks, disrupts the infrastructure of countries, and interfere with safety internal military data of other countries, and attempts to confuse or obfuscate their financial transactions. As the danger of information security is rising to the level of threatening national security as a whole, the means of confrontation and protection must be overshadowed by a national security system, because it is unreasonable for the dangers and threats to be comprehensive, coordinated and sometimes planned, then there are ways and means to confront them that are partial, spontaneous and empty.

Furthermore, It lacks planning , coordination and rationality, as a comprehensive program should be implemented at the level of institutions and agencies. The state and private companies aim to train in repelling all-out electronic attacks in their various forms. Whether by viruses, economic spy , electronic sabotage, or network disruption attack for communication and information.

**Sources**

First: the Holy Quran

Second: dictionaries, dictionaries and encyclopedias

1. Ibn Manzoor Al-Masry, Lexicon of Lisan Al-Arab, Volume One, Beirut for printing and publishing.

2. Ahmad Zaki Badawi, Dictionary of Social Sciences Terminology, Library of Lebanon, Cairo, Egypt, 1975.

3. Abd al-Wahhab al-Kayyali, Encyclopedia of Politics, Part One, Second Edition, Arab Institute for Studies and Publishing, Beirut - Lebanon, 1985.

4. The Arabic Language Academy, the Intermediate Dictionary, Part One, The Islamic Library for Printing, Publishing and Distribution.

5. Muhammad Abd al-Jabbar al-Samawi al-Yamani, The Arabic Encyclopedia of Opposite Words and Linguistic Fragments, Dar al-Adab - Beirut, Yemeni Studies and Research Center - Sana'a, Volume Two, 1989.

6. Paul Robinson, International Security Dictionary, Emirates Center for Strategic Studies and Research, Abu Dhabi - United Arab Emirates, 2009.

Third: Arabic books

1. Bashir Al-Wandi, Lost Security: The Role of Intelligence and Development in Establishing Security, Dar Al-Saffar, Beirut - Lebanon, 2013.
2. Hazem Hamad Al-Shammari, Employing Cyberpower in the Strategies of Major Powers: The United States and the Russian Federation as a Model, First Edition, Baghdad - Iraq, 2022.
3. Deeb bin Ayed Al-Qahtani, Information Security, Riyadh - Saudi Arabia, 2015.
4. Saleh bin Ali bin Abdul Rahman, Digital Security and User Protection from Internet Risks - Vision 2030, Communications and Information Technology Commission, Kingdom of Saudi Arabia, 2017.
5. Sabah Abdel-Sabour Abdel-Hay, The Use of Electronic Power in International Interactions - Al-Qaeda as a Model, Part Two, Egyptian Institute for Political and Strategic Studies, Turkey, 2016.
6. Adel Abdel Sadiq, Cyberspace Weapons in Light of International Humanitarian Law, Arab Center for Space Research, Alexandria - Arab Republic of Egypt, no date.
7. Adel Abdel Sadiq, Electronic Terrorism - Power in International Relations (a new pattern and different challenges), Al-Ahram Center for Political and Strategic Studies, Cairo - Arab Republic of Egypt.2009.

8. Amer Mesbah, Strategic Perspectives in Building Security, Modern Book House, Cairo - Egypt, 2013.
9. Abd al-Rahman bin Abdullah al-Sanad, Methods of Electronic Terrorism - Its Ruling in Islam and Ways to Combat It, No Publishing House, 2010.
10. Abdul Rahman Abdullah Al-Sanad, The Crime of Extortion, King Fahd National Library, Riyadh - Kingdom of Saudi Arabia, 2018.
11. Abdullah Al-Youssef, Technology and New Crimes - Criminal Phenomena and Ways to Address Them, Naif Arab Academy for Security Sciences, Riyadh - Kingdom of Saudi Arabia, 1999.
12. Ali Abbas Murad, Security and National Security: Theoretical Approaches, Ibn Al-Nadim for Publishing and Distribution and Dar Al-Rawafed Al-Thaqafa - Publishers, Oran - Algeria, Beirut - Lebanon, 2016.
13. Firas Jamal Shaker, Information Wars in the Security and Military Field: America and China, first edition, Al-Araby for Publishing and Distribution, Cairo - Egypt, 2023.
14. Fahd bin Muhammad Al-Shaqha, National Security: A Comprehensive Concept, Center for Studies and Research, Naif Arab University for Security Sciences, Riyadh - Saudi Arabia, 2004.
15. Lakhmisi Shaibi, International Security and the Relationship between the North Atlantic Treaty Organization and the Arab Countries in the Post-Cold War Period (1991-2008), The Egyptian Library for Publishing and Distribution, Cairo - Egypt, 2010.
16. Mohamed Reda Fouda, Strategy and National Security, Arab Bureau of Knowledge, Cairo - Arab Republic of Egypt, 1995.
17. Mustafa Abdullah Khushim, The Impact of the Barcelona Conference on Arab Economic Security, Arab Security, Current Challenges, Public Policy Theory, Garyounis University, Libya, 2007.
18. Nassima Tawil, Strategic Trigonometry in Northeast Asia, Arab Democratic Center for Strategic, Political and Economic Studies, Berlin - Germany, 2017.
19. Walid Abdel-Hay and others, Understanding Algerian National Security from the National Security and National Defense Entrances, Dar Al-Hamid for Publishing and Distribution, Amman - Jordan, 2015.

Fourth: Theses and university dissertations

1. Tawami Yacoub, The impact of the use of information and communication technology on the financial performance of the economic enterprise - a case study of the National Corporation for Works in Wells complex () during the period 2010-2012, unpublished master's thesis, Faculty of Economic and Commercial Sciences and an unpublished master's thesis in management, Kasdi Merbah University, Algeria , 2013.
2. Somaya Ocean, The Contemporary State and Cultural Globalization - Between the Localization of the Values of World Culture and the Globalization of the Values of Local

Cultures, unpublished PhD thesis, Faculty of Law and Political Science, University of Batna, Al-Hijaz Lakhdar, Algeria, 2019.
3. Ali Ibrahim Al-Mamouri, Cybersecurity and its impact on Iraqi national security after the year 2003, unpublished master's thesis, College of Political Science, University of Baghdad, Baghdad - Iraq, 2019.
4. Ali Abdel Aziz Marza, Democracy and National Security: An Analytical Theoretical Study, unpublished PhD thesis, College of Political Science, University of Baghdad, Baghdad - Iraq, 2014.
5. Mohamed Mehani, The Impact of Electronic Terrorism on Changing the Concept of Power in International Relations - Terrorist Organizations Employment of Social Networking Sites as a Model, Unpublished Master's Thesis, Department of Political Science and International Relations, University of Mohamed Boudiaf, Algeria, 2018.

Fifth: Research and articles

1. Ibrahim Musahib al-Dulaimi, Drugs and Arab National Security: A Study from a Sociological Perspective, Strategic Studies, Issue 84, 2003, Emirates Center for Strategic Studies and Research, Abu Dhabi - United Arab Emirates.
2. Jaafar Hassan Al-Taie, Information Terrorism and Mechanisms to Reducing it, Journal of Legal and Political Sciences, College of Law and Political Sciences, Diyala University, Diyala - Iraq, 2015.
3. Khaled Walid Mahmoud, Cyber Attacks - The New Electronic Conflict Arena, Series of Studies and Policy Studies, Arab Center for Research, Doha - Qatar, 2013.
4. Saif Nusrat Tawfiq, Actors of the Regime in the Twenty-First Century, Tikrit Journal of Political Science, Issue 11, Tikrit University, Salah al-Din - Iraq, 2017.
5. Salah Mahdi Hadi and Zaid Muhammad Ali Ismail, Cybersecurity as a new pivot in the Iraqi strategy, Journal of Political Issues, Issue 62, July-August-September 2020, College of Political Science, Al-Nahrain University, Baghdad - Iraq.
6. Abd al-Sattar Abd al-Jabbar and Raji Muhail, The Communications Sector in Iraq after 2003 and the Required Reforms to Achieve Economic Welfare, Wasit Journal of Human Sciences, University of Wasit, Wasit - Iraq, 2018.
7. Abd al-Hadi Muhammad al-Zaidi, Israeli electronic espionage on Arab countries, Journal of International Studies, Issue 58, Center for International and Strategic Studies, University of Baghdad, Baghdad - Iraq.
8. Kadir Ismail, Managing psychological warfare in cyberspace - the new American strategy in the Middle East, the international symposium tagged (the globalization of political media and the challenges of national security for developing countries), Department of Political Science, Faculty of Law and Political Science, Kasdi Merbah University, Algeria, 3/7/ 2007.
9. Lubna Khamis Mahdi and Taghreed Safaa, The Impact of Cyber on the Development of Power, Hammurabi Magazine, Issue 33-34, Year 8, Winter-Spring, 2020.

10. Muhammad Zuhair Abdul Karim, Cyberterrorism: A New Global Crisis, Journal of Political Issues, College of Political Science, Al-Nahrain University, Baghdad - Iraq.
11. Muhammad Wael al-Qaisi, The Future of Global Strategic Security in Light of Techno-Informatics Challenges and Cyberspace, Journal of Regional Studies, Year 14, Issue 44, April 2020, University of Mosul, Mosul - Iraq.
12. Marwan Salem Al-Ali, Strategic Challenges to Iraqi National Security in Light of International Changes, Tikrit Journal of Political Science, Issue 20, 2020, Tikrit University, Salah al-Din - Iraq.
13. Mustafa Ibrahim Salman Al-Shammari, Cybersecurity and its impact on Iraqi national security, Journal of Legal and Political Sciences, Volume X, Number One, 2021, College of Law and Political Science, Diyala University, Diyala - Iraq.
14. Munther Salman, Towards a Reformulation of the Concept of Arab National Security and its Foundations, Issue 1544, Year 8, Palestine, 2008.
15. Munim Sahi al-Ammar and Shaima Turkan Saleh, Iraqi National Security and Combating Terrorism (A Study on the Problematic Administration), Journal of International Studies, Issue 61, April 2015, Center for International Studies, University of Baghdad, Baghdad - Iraq.
16. Haitham Karim Siwan and Muhannad Jabbar Abbas, Cyberwar between Challenges and Confrontational Strategies, Iraq as a Model, Journal of Political Issues, Issue 70, 2022, College of Political Science, Al-Nahrain University, Baghdad - Iraq.

Sixth: Foreign sources

1. Khalid Walid Mohmoud, Cyber attacks: the electronic Battlefield, Series: Research Paper, Arab Center for research and Policy Studies, 2013.
2. New Webester's Dictionary and the Source of English long. Levicon Publishing inc, 1996.

Seventh: Internet sources

1. Amira Abd al-Azim Muhammad Abd al-Wad, Cyber risks and ways to confront them in public international law, Journal of Sharia and Law, Issue Thirty-five, Part Three, 2020, pdf, on the website: https://jlr.journal.ekb.eg

2. Amal Saqr, Realistic Risks: How (Social Media) Threatens National Security, on the website: http://futureuae.com

3. Muhammad Abdul Mohsen Saadoun, The Concept of Terrorism and its Criminalization in National Criminal Legislation, No. 7, 2008, pdf, on the website: www.iasj.net
4. Khaled Ali Muhammad Al-Amiri and Ahmed Falah Al-Amoush, National Security: Concept, Dimensions and Theories, Al-Adab Magazine, Supplement to Issue 133, June 2020, pdf, on the website: https://www.researchgate.net

5. Hayel Abd al-Mawla Tashtoush, National Security and Elements of State Power in Light of the New World Order, on the website: iefpedia.com
6. Ratiba Bard, American Security Policy in the Mediterranean, Journal of Policy and Law Notebooks, Issue 15, June 2016, pdf, on the website: www.dspace.univ-ouargla.dz
7. Muhammed Muhammed Saeed Shuaibi and Nadia Muhammed Saeed Al-Naqeeb, Humanizing Electronic War, Journal of Educational Sciences and Human Studies, Issue No. 1, September 2022, pdf, on the website: hesj.org
8. Soleimani Mubarak, Electronic terrorism and ways to combat it, Journal of Law and Political Science, University of Khenchela, Issue 8, Part 1, June 2017, pdf, on the website: www.asjp.cerist.dz
9. Al-Jazeera Channel, The Washington Post: The President of Iraq is on the list of targets for Israeli spyware, 7/21/2021, on the website: www.aljazeera.net
10. Karrar Abbas Meteb Faraj, Cyber War: A Study in the Strategy of Cyber Attacks between the United States of America and Iran, Hammurabi Journal for Studies, Issue 40, Year 10, Winter 2021,pdf, on the website: https://www.iasj.net
11. Yaqeen News Agency, Victims of Electronic Extortion in Iraq (file), July 5, 2022, on the website: yaqinnews.net
12. Ali Ziyad Al-Ali, Invisible Challenges to Iraqi National Security, Al-Bayan Center for Studies and Planning, on the website: https://www.bayancenter.org
13. Ali Hussein Hamid and Ali Ziyad Abdullah, Analyzing the Iraqi Strategic Environment from a Security Perspective, Hammurabi Magazine, Issue 33-34, Year 8, Winter-Spring 2020, pdf, on the website: https://wwwiasj.net
14. Ali Adham, Cybersecurity, Al-Nahrain Center for Strategic Studies, published on March 13, 2019, on the website: http://www.slnahrain.iq
15. Hanan Bint Shashou Al-Shehri, The Impact of Using Electronic Communication Networks on Social Relations (Facebook and Twitter as a Model), a research project submitted as part of the requirements for obtaining a master's degree in Sociology, Department of Sociology and Social Work, College of Arts and Humanities, King Abdulaziz University, Riyadh - Saudi Arabia, 1433-1434 AH, pdf, on the website: home.moe.gov.om
16. Khaled Zahir Abdullah Jaber Al-Suhail Al-Mutairi, The Role of Penal Legislation in Protecting Cybersecurity in the Gulf Cooperation Council Countries, Journal of Fiqh and Legal Research, Issue Thirty-Eighth, July 2022 issue, on the website: https://jlr.journal.ekb.eq
17. Samer Mohi Abdel-Hamza, Iraqi Legislative Policy to Protect Cybersecurity: A Study in Light of the Provisions of Public International Law, pdf, on the website: lark.uowasit.edu.iq
18. aafar Fahd Abd al-Ridha, The Reality of Wireless Communications in Modern Iraq, on the website:
19. http://law.uos-college.com/news-details/44/artical

20. Hussein Basem Abdel-Amir, Emerging Security Challenges, Center for Strategic Studies, Karbala University, January 28, 2021, on the website: http://kerbalacss.uokerbala.edu.iq
21. Majid Saddam Salem, Cybersecurity and its impact on the power of the state, Journal of Educational and Human Sciences, Issue 18, December 2022, pdf, on the website : www.jeahs.com
22. Hashim Shubar, Organizing the Joint Institutional and Ministerial Effort Concerning Cybersecurity in Iraq, Al-Bayan Center for Studies and Planning, on the website: bayancenter.org
23. Cyber Incident Response Team, Cyber Security Strategy 2022-2025 (Final Draft), pdf, on the website: cert.gov.iq
24. Hazem Hamad Musa, The Strategic Vision for Iraqi National Security in Cyberspace, Algerian Journal of Legal and Political Sciences, Volume 57, Issue 5, Year 2020, on the website: www.asjp.cerist.dz