مجلة فرسان الرد السريع للدراسات الأمنية
مجلة علميَّة مُحكمة نصف سنويَّة
تصدر عن وزارة الداخليَّة العراقيَّة/ قيّادة الردِّ السَّريع
العدد (2)/ المجلد (1)/ لسنـــة2024ـــة

ملف العدد
الأمن السيبراني
درع التحول الرقمي العراقي
(بين التحديات الراهنة وضرورات المستقبل)

- الافتتاحية: التهديدات الأمنية السيبرانية ومستقبل الأمن في العراق.
- الأمن السيبراني اوكسجين التحول الرقمي العراقي.
- رؤية استراتيجية تحليلية لواقع الحوكمة الرقمية في العراق.
- العراق بين ضرورات التحول الرقمي وتحديات المحافظة على امنه الوطني.
- تحليل التحول الرقمي في العراق.
- آليات تعزيز الوعي والتنشئة الرقمية في العراق.
- قراءة تحليلية لاستراتيجية الامن السيبراني العراقي.
- الأمن السيبراني وإدارة المخاطر.
- الذكاء الاصطناعي كآلية لتحقيق الامن السيبراني العراقي.
- دور الأمن السيبراني في تطور قوة الدولة العراقية.
- الأمن السيبراني والتهديدات الأمنية المستجدة.
- نحو استراتيجية للأمن السيبراني العراقي.

فرسان الرد السريع للدراسات الأمنية

مجلة علمية محكمة تعنى بالدراسات الامنية

تصدر عن وزارة الداخلية العراقية/ قيادة فرقة الرد السريع

العدد (2)/ المجلد (1)/ حزيران 2024

فرسان الرد السريع للدراسات الأمنية

"مجلة علمية محكمة تصدر عن وزارة الداخلية العراقية/ قيادة الرد السريع، وهي دورية نصف سنوية تصدر مرة واحدة كل ستة اشهر، وتستند إلى ميثاق أخلاقي لقواعد النشر فيها والعلاقة بينها وبين الباحثين، تعنى بالدراسات الأمنية المعاصرة، وتعالج المخاطر الأمنية بمختلف انماطها التي تمس الدولة العراقية محلياً واقليمياً ودولياً، وتستقبل المجلة (الأبحاث والمقالات الاكاديمية، والتحليلات الاستراتيجية والأمنية، والأوراق الإجرائية، وعروض الكتب، والأبحاث المترجمة) ذات العلاقة بتوجهات المجلة واهتماماتها، من التخصصات الآتية: (العلوم الأمنية والعسكرية، والقانون، والعلوم السياسية، وعلم الاجتماع، وعلم النفس، والإدارة، والاعلام)".

مرقم الايداع القانوني في دار الكتب والوثائق العراقية ببغداد (2698) لـ2023سنة

ترسل الأبحاث وجميع المراسلات باسم رئيس التحرير على العناوين التالية:

009647728778806

erdaliraq2023@gmail.com

بغداد، مطار بغداد الدولي، 8736+7CH

Fursan Alrad Alsaree' Journal for Security Studies

A peer-reviewed scientific journal specialized in security studies
Issued by the Ministry of Interior/ Iraq Special ops/E.R.D Forces Batting Command
Issue (2), Volume (1), 2024

"A peer-reviewed scientific journal issued by the Iraqi Ministry of Interior/ Iraq Special ops/E.R.D Forces Batting Command. It is a semi-annual periodical issued once every six months. It's based on an ethical charter for its publishing rules and the relationship between it and researchers. It's concerned with contemporary security studies and addresses security risks in their various forms that affect... The Iraqi state locally, regionally, and internationally, and the journal receives (academic research and articles, strategic and security analyses, procedural papers, book presentations, and translated research) related to the magazine's directions and interests, from the following specializations: (security and military sciences, law, political science, sociology, and Psychology, management, and media)".

التدقيق اللغوي

مدقق اللغة العربية
م.م. حسين محمد خلف
قيادة فرقة الرد السريع/ وزارة الداخلية العراقية

مدقق اللغة العربية
محمود محمد محمد
قيادة فرقة الرد السريع/ وزارة الداخلية العراقية

مدقق اللغة الإنكليزية
براء سعدون مطلك محمد
كلية الهادي الجامعة/ وزارة التعليم العالي والبحث العلمي

الدعم الاستشاري

اللواء مهدي عباس عبدالله سعدون الحيالي/ نائب قائد قيادة فرقة الرد السريع
اللواء الركن نعمان محمد نعمة غالي المالكي/ رئيس اركان قيادة فرقة الرد السريع
اللواء ضياء مزهر لفته حميد المنصوري/ مدير مكتب القائد
اللواء الركن عارف منسي صالح حسين الدليمي/ مدير مديرية العمليات
اللواء رافع سعيد حميد دفار العماري/ مدير مديرية الإدارة والميرة
العميد الركن رياض محمد جاسم/ مدير مديرية التدريب
العميد هيثم مهدي محمود محي الحيالي/ مدير مديرية الحسابات
العميد اثير إبراهيم خليل إبراهيم البكر/ امر مدرسة تدريب القوات الخاصة
العميد محمد علي محسن عبد سلمان السلماوي/ آمر لواء الرد السريع الأول
العميد الركن عمر عيسى كاظم جاسم الجبوري/ آمر لواء الرد السريع الثاني
العقيد سمير نعمة عبد الرضا عبيد الشبلاوي / آمر لواء الرد السريع الثالث
العقيد أسامة ناهض جبار جاسم الزبيدي / آمر لواء الرد السريع الرابع
العميد هشام عبد الكاظم خلباص طامي الخفاجي / آمر لواء الرد السريع الخامس
أ.م.د. أحمد رياض عباس/ كلية الهندسة/ جامعة النهرين

الإشراف الفني والطباعي

العميد عبد الأمير حمادي عطية المحمداوي
مدير قسم العلاقات والاعلام/ قيادة فرقة الرد السريع

التصميم الطباعي

المفوض رحيم زامل حمادي نعيم الكناني
قسم العلاقات والاعلام/ قيادة فرقة الرد السريع

اخلاقيات النشر

أولا: بيان اخلاقيات النشر

تستندُ السَّياسة الأخلاقيَّة لمجلّة فُرسان الرّد السريع للدّراسات الأمنيّة على المبادئ التّوجيهيّة للجنة أخلاقيّات النّشر (COPE) وتتوافق مع قواعد السُّلوك الصّادرة عن هيأة تحرير المجلّة، إذ يجب على القُراء والمؤلّفين والمراجعين والمحرّرين إتّباع هذه السّياسات الأخلاقيّة عند التّعامل مع المجلّة، وإنّ السّياسة الأخلاقيّة للمجلّة مسؤُولة عن تحديد أيّ من الأبحاث أو المقالات البحثيّة النّموذجيّة المقدّمة إلى المجلّة ليمكن نشرها في أعدادها، وللحصول على معلومات حول هذه المسألة في النّشر والمبادئ التّوجيهيّة الأخلاقية يُرجى زيارة المُوقع الإلكتروني: http://publicationethics.org .

ثانيًا: واجبات ومسؤوليات الناشرين

1. تلتزم المجلّة بضمان أنّ تكون القرارات التي تتّخذها هيأة التّحرير بشأن البُحوث العلميّة نهائيّة.
2. تعهّد المجلّة بضمان عدم اتّخاذ القرار بشأن تقديم البُحوث إلّا بناءً على تقدير مهني ولن يتأثّر بأيّ مصالحٍ.
3. تلتزم المجلّة بالحفاظ على سلامة السّجلّات الأكاديمية والبحثيّة.
4. تُراقب المجلّة الأخلاقيّات من قبل رئيس التّحرير والمحرّرين المُساعدين وأعضاء هيأة التّحرير والمراجعين والمؤلّفين والقرّاء.
5. تقوم المجلّة دائمًا بالتّحقُّق من مشّكلات الانتحال والبيانات الاحتياليّة التي تنطوي عليها البُحوث المقدّمة.
6. المجلّة مُستعدّة دائمًا لنشر التّصحيحات والإيضاحات وعمليّات التّراجع التي تتضمّنها منشوراتها عند الحاجة.

ثالثًا: واجبات ومسؤوليات المحررين

1. أن يتمتّع مُحررو المجلّة بالصّلاحيّة الكاملة لقبُول البحث أو رفضه.
2. الحفاظ على سرّية البحث المُقدم قيد المراجعة حتّى يتم نشرُه.
3. على رئيس التّحرير اتّخاذ القرار بشأن البحث المُقدم سواءً أنّ سيتم نشرُه أُمّ رفضه مع أعضاء هيأة التّحرير والمقيمين.
4. الحفاظ على سرّية المقيمين.
5. الكشفّ عن أيّ تضارُب في المصالح ومحاولة تجنبه.
6. الحفاظ على النّزاهة الأكاديمية والسّعي لتلبية احتياجات القُراء والمؤلّفين.
7. أن يكون مُحررو المجلّة على استعدادٍ للتّحقيق في قضايا الانتحال والبيانات الاحتياليّة وأن يكونوا على استعدادٍ لنشر التّصحيحات والإيضاحات والتّراجع والاعتذار عند الحاجة.
8. أن يكون لمحرّري المجلّة الحد الأقصى للمحتوى الفكري فقط.

9. يجب ألّا يكشفّ محررو المجلّة عن أيّ معلوماتٍ حول البحث المُقدم لأيّ شخصٍ آخر غير المُؤلف المسؤول والمقيمين المحتملين ومستشاري التّحرير الآخرين والنّاشر وحسب الاقتضاء.
10. عدم استخدام المواد غير المنشورة التي تمّ الكشفّ عنها في البحث المُقدم بواسطة المُحرر أو أعضاء هيأة التّحرير لأغراض البحث الخاصّة بهم.

رابعًا: واجبات ومسؤوليات المؤلفين

1. يتم تقديم البحث باللُّغة العربيّة أو الإنكليزيّة ويجب كتابته وفقًا للقواعد السّليمة والمصطلحات المناسبة.
2. يجب تقديم البحث على أساس أنّه لم ينشُر في أيّ مكانّ آخر، وهُو ليس قيد الدّراسة حاليًّا من قبل مجلّة أُخرى تنشُرها أو أيّ ناشر آخر.
3. الباحث هُو المسؤول عن ضمان الموافقة على نشر البحث من قبل جميع المؤلّفين الآخرين.
4. من أجل الحفاظ على نظام التّقييم، يلتزم المؤلّفون بالمشاركة في عمليّة مُراجعة المقيمين لتقييم بُحُوث مُرسلة من الآخرين.
5. تقع على عاتق المؤلّفين أيضًا مسؤوليّة ضمان تقديم البحث الصّادر من مُؤسسة مُعينة بموافقة المؤسّسة صاحبة الشأن.
6. يطلُب من المؤلّفين أن يُحدّدوا بوضوح من الذي قدّم الدّعم الماليُّ لإجراء البُحوث / أو إعداد البحث وأن يصف باختصار دور المؤسّسة / الرّاعية في أيّ جُزء من العمل.
7. يجب أن يُوقّع المُؤلف المسؤول نُسخة مُوافقة لجميع المؤلّفين في حالة البُحوث لأكثر من باحث، قبل قبُول البحث لنشره، ليكون مسؤُولا قانونًا تُجاه أخلاقيّات المجلّة وسياسة الخصوصيّة.
8. يحتفظ المؤلّفون بملكية حُقُوق الطّبع والنّشر لمحتواهم، ويسمح لأيّ شخص بتنزيل أو إعادة استخدام أو إعادة طبع أو تعديل أو توزيع / أو نُسخ المحتوى طالما تمّ ذكر المؤلّفين والمصدر الأصليّين بشّكل صحيح.
9. مُوافقة جميع المؤلّفين على السّماح للمؤلّف المسؤول بالعمل كمُراسل مع مكتبّ التّحرير، لمراجعة عمليّة تحرير البحث والإثبات.
10. عندما يكتشُف المُؤلف (المؤلّفون) خطأ كبيرًا أو عدم دقّةٍ في عمله المنشور، فمن واجب المُؤلف إخطار رئيس تحرير المجلّة أو النّاشر على الفور بسحب البحث أو تصحيحه.
11. يجب أن يعلم جميع المؤلّفين أنّ البُحوث المقدّمة قيد المراجعة أو المنشورة في مجلّة فُرسان الرّد السريع للدّراسات الأمنيّة تخضع للفحص باستخدام برنامج مكافحة الانتحال.
12. يجب على جميع المؤلّفين التّأكد من أنّ جميع المؤلّفين قد قرأ قائمة المراجعة النّهائيّة للتّقديم قبل إرسالها للمجلّة.

خامساً: واجبات ومسؤوليات المقيمين

1. مُساعدة أعضاء هيأة التّحرير في اتّخاذ قرار بشأن نشر البُحوث المقدّمة.
2. الحفاظ على سرّية البُحوث، التي أرسلت إليهم لغرض تقييمها.
3. تقديم التّعليقات في الوقت المناسب لتساعد أعضاء هيأة التّحرير على اتّخاذ قرار بشأن البُحوث المقدّمة التي سيتم نشرُها من عدمه.
4. التّعامل مع البُحوث التي تمّ استلامها للمراجعة على أنها سرّية، ويجب ألّا يستخدموا المعلومات التي تمّ الحُصول عليها من خلال مُراجعة هذه البُحوث لتحقيق ميزة شخصية.
5. تكون تعليقات المقيمين للبحث مدعُومة تقنيًّا ومهنياً وموضوعيّاً.
6. لا ينبغي للمقيمين مُراجعة البُحوث التي وجدُوا فيها تضاربًا في المصالح مع أيّ من المؤلّفين أو المؤسّسات.
7. يجب على المقيمين الإفصاح عن أيّ تضارُب في المصالح ومحاولة تجنبه.

سادساً: مبادئ الشفافية

1- آلية المراجعة المزدوجة: أن البُحوث في المجلّة تخضع لتقييم مُزدوج بشّكل سرّي ثُنائي والمقصود أنّ الباحث لا يعلم بالمقيم كما أنّ المقيمين ليس لهُم علم بالباحث.
2- تصدُر المجلّة بعددٍ نصف سنوي لستّة أشهُر بشّكل ورقي وإلكترونيّ تهتم بجميع جوانب المجلّة.
3- هيأة التّحرير: أن للمجلّة هيأة تحرير قويّة للغاية، أعضاؤها خُبراء مُعترف بهم في مجالات الموضوعات المدرجة في نطاق المجلّة.
4- معلومات الاتّصال: توفُّر المجلّة معلومات الاتّصال بهيأة تحرير المجلّة من خلال زيارة الموقع الإلكترونيّ للمجلّة.
5- رُسُوم نشر البحث: المجلّة تقع ضمن المجلّات المفتوحة بالكامل ويمكن الوُصول إلى النّص الكامل للبحوث المنشورة للجميع من خلال موقع المجلّة وبشكل مجاني، إلى جانب ذلك، يُلزم المؤلفين بدفع رُسُوم نشرهم للبحوث المقبولة، والمقدرة بـ (50.000) خمسون ألف دينار عراقيٍّ.
6- تحديد مزاعم سُوء السُّلوك البحثي والتّعامل معه: يتخذ رئيس التّحرير خُطوات معقُولة لتحديد ومنع نشر الأوراق التي وجد فيها سُوء سُلُوك الباحث، بما في ذلك الانتحال والتّلاعب في الاقتباس وتزوير / تلفيق البيانات، من بين أُمُور أُخرى.
7- موقع الويب: يحتوي موقع الويب الخاص بالمجلّة على معلومات كاملة للمجلّة لضمان المعايير الأخلاقيّة والمهنيّة العالية.
8- اسم المجلّة: اسم المجلّة " مجلّة فُرسان الرّد السريع للدّراسات الأمنيّة " ولا يمكن الخلط بينها وبين مجلّة أُخرى.
9- تضارُب المصالح: يطلُب من المؤلّفين توضيح ما إذا كانت التّعارضات الوشيكة موجُودة أو غير موجُودة أثناء تقديم مقالاتهم إلى مجلّة فُرسان الرّد السريع للدّراسات الأمنيّة من خلال نمُوذج الكشفّ عن تضارُب المصالح.
10-جدول النّشر: يُشار إلى الدّوريّة التي تُنشر فيها المجلّة بوضوح على الرّابط:

11-الأرشفة: يُشار بوضوح إلى خُطّة المجلّة الخاصّة بالنّسخ الاحتياطيّ الإلكتروني والحفاظ على الوُصول إلى مُحتوى المجلّة.

سابعًا: انتهاك أخلاقيات النشر

1- الانتحال:

- إن استخدام شخص عمدًا أفكار شخص آخر أو مواد أصلية أُخرى كما لو كانت أفكاره، حتّى لو كانت جُملة قد استخدمت لنفس الباحث قام بنشرها في مجلات أُخرى دُون اقتباس مُناسب تعتبره المجلّة انتحالا.
- تخضع جميع البُحوث قيد المراجعة أو المنشورة في المجلّة للفحص باستخدام برنامج الوقاية من الانتحال، وبالتّالي، الانتحال هُو انتهاك خطير لأخلاقيّات النّشر.
- تطوير CrossCheck وهي خدمة تُساعد المحرّرين على التّحقُّق من أصالة الأوراق، يتم تشغيل CrossCheck بواسطة برنامج Ithenticate من iParadigms، والمعروف في المجتمع الأكاديمي مُقدمي Turnitin للحصول على قائمة قابلة للبحث لجميع المجلّات في قاعدة بيانات CrossCheck.

2- تلفيق البيانات وتزويرها: يعني تلفيق البيانات وتزويرها أنّ الباحث لم يُنفّذ الدّراسة بالفعل، بل قام بتُكوين بيانات أو نتائج وقام بتسجيل أو تلفيق المعلومات المُفبركة، وتزييف البيانات يعني أنّ الباحث قام بالتّجربة، لكنه قام بمعالجة أو تغيير أو حذف بيانات أو نتائج من نتائج البحث.

3- التّقديم المتزامن: يحدُث التّقديم المتزامن عندما يتم إرسال بحث (أو أقسام كبيرة من البحث) إلى المجلّة عندما تكون قيد الدّراسة بالفعل من قبل مجلّة أخرى.

4- المنشور المكرر: يحدُث المنشور المكرر عندما تتشارك ورقتان أو أكثر، في نفس الفرضيّات والبيانات ونقاط المناقشة والاستنتاجات، ويعد هذا السلوك مرفوضاً ضمن سياسة النشر لمجلة فرسان الرد السريع للدراسات الأمنية.

5- مطبوعات زائدة عن الحاجة: تشمل المنشورات المكررة التّقسيم غير المناسب لنتائج الدّراسة إلى عدّة مقالات، وغالبًا ما يكون ذلك نتيجة للرّغبة في تضخيم السّيرة الاكاديمية.

6- مُساهمة أو إسناد غير لائق للمؤلّف: يجب أن يكون جميع المؤلّفين المدرجين قد قدمُوا مُساهمة علميّة مُهمّة في البحث ووافقوا على جميع مطالبها. ولا ننسى إدراج أيّ شخص قدّم مُساهمة علميّة كبيرة، بما في ذُلّك الطُّلّاب.

7- التّلاعب في الاقتباس: يشمل التّلاعب في الاقتباس الاقتباسات المفرطة، في البحث المُقدم، والتي لا تُسهم في المحتوى العلمي للمادّة والتي تمّ تضمينها فقط لغرض زيادة الاقتباسات من عمل مُؤلّف مُعيّن، أو في المقالات المنشورة بشّكل خاص للمجلّة. وهذا يُؤدّي إلى تحريف أهمية عمل المجلة، وبالتّالي فهُو شكل من إشكاليات سُوء السّلوك العلمي.

8- العقوبات: في حالة وُجُود انتهاكات مُوثقة لأيٍّ من السّياسات المُذكوُرّة أعلاه في أيّ مجلّة، بغضّ النّظر عمّا إذا كانت الانتهاكات قد وقعت في مجلّة أم لا، سيتم تطبيق العقوبات التّالية: (الرّفض الفوري للبحث المخالف، ولكل بحث آخر مُقدّم إلى أيّ مجلّة ينشُرها أيٌّ من مُؤلفي البحث المخالف، ويفرض الحظر لمدّة لا تقل عن 36 شهرًا على جميع المؤلّفين

لأيّ تقديمات جديدة إلى أيّ مجلّة، إمّا بشّكل مُنفرد أو بالاشتراك مع مُؤلّفين آخرين للبحوث المخالفة، ومنع جميع المؤلفين من العمل في هيأة تحرير أي مجلة).

Publishing ethics

1. Statement of publishing ethics

The ethical policy of the Journal of Rapid Response Knights for Security Studies is based on the guidelines of the Committee on Publication Ethics (COPE) and is consistent with the rules of conduct issued by the journal's editorial board. Readers, authors, reviewers, and editors must follow these ethical policies when dealing with the journal, and the ethical policy of the journal is responsible for To determine which research papers or sample research articles submitted to the journal can be published in its issue, and for information on this issue of publishing and ethical guidelines, please visit the website: http://publicationethics.org.

2. Duties and responsibilities of publishers

1. The journal is committed to ensuring that the decisions taken by the editorial board regarding scientific research are final.
2. The journal pledges to ensure that the decision to submit research will only be made based on professional judgment and will not be influenced by any interests.
3. The journal is committed to maintaining the integrity of academic and research records.
4. The journal's ethics are monitored by the editor-in-chief, assistant editors, members of the editorial board, reviewers, authors, and readers.
5. The journal always checks for problems of plagiarism and fraudulent data contained in the submitted research.
6. The magazine is always ready to publish corrections, clarifications, and retractions included in its publications when needed.

3. Duties and responsibilities of editors

1. The journal editors must have full authority to accept or reject the research.
2. Maintaining the confidentiality of the research submitted under review until it is published.
3. The editor-in-chief must decide whether to publish or reject the submitted research with the members of the editorial board and residents.
4. Maintaining resident confidentiality.
5. Detect any conflict of interest and try to avoid it.

6. Maintaining academic integrity and striving to meet the needs of readers and authors.
7. Journal editors should be prepared to investigate cases of plagiarism and fraudulent statements and be prepared to publish corrections, clarifications, retractions, and apologies when needed.
8. The magazine's editors should have a maximum limit for intellectual content only.
9. Journal editors must not disclose any information about the submitted manuscript to anyone other than the responsible author, potential reviewers, other editorial advisors, the publisher, and as applicable.
10. Do not use unpublished materials disclosed in the research submitted by the editor or members of the editorial staff for their own research purposes.

4. Duties and responsibilities of authors

1. The research must be submitted in Arabic or English and must be written in accordance with proper grammar and appropriate terminology.
2. The research must be submitted on the basis that it has not been published anywhere else, and is not currently under consideration by another journal or any other publisher.
3. The researcher is responsible for ensuring that all other authors approve the publication of the research.
4. In order to maintain the evaluation system, authors are obligated to participate in the rater review process to evaluate papers submitted by others.
5. It is also the responsibility of the authors to ensure that research originating from a specific institution is submitted with the approval of the relevant institution.
6. Authors are asked to clearly identify who provided financial support for the conduct of the research/or preparation of the manuscript and to briefly describe the role of the institution/sponsor in any part of the work.
7. The responsible author must sign an approval copy for all authors in the case of research by more than one researcher, before accepting the research for publication, to be legally responsible towards the journal's ethics and privacy policy.
8. Authors retain copyright ownership of their content, and anyone is permitted to download, reuse, reprint, modify, distribute and/or copy the content as long as the original authors and source are properly credited.

9. All authors agree to allow the responsible author to work as a correspondent with the editorial office, to review the research and proof editing process.
10. When the author(s) discover a major error or inaccuracy in his published work, it is the author's duty to immediately notify the editor-in-chief of the journal or publisher that the manuscript has been withdrawn or corrected.
11. All authors should be aware that research submitted under review or published in the Journal of the Knights of Rapid Response for Security Studies is subject to examination using anti-plagiarism software.
12. All authors must ensure that they have read the final submission checklist before submitting it to the journal.

5. Duties and responsibilities of residents

1. Assisting editorial board members in making a decision regarding publishing the submitted research.
2. Maintaining the confidentiality of the research that was sent to them for the purpose of evaluation.
3. Providing comments in a timely manner to help editorial board members make a decision regarding whether or not the submitted research will be published.
4. Treat the research received for review as confidential, and they must not use the information obtained through reviewing this research to achieve personal advantage.
5. Evaluators' comments on the research are technically, professionally, and objectively supported.
6. Reviewers should not review manuscripts in which they find a conflict of interest with any of the authors or institutions.
7. Residents must disclose and attempt to avoid any conflicts of interest.

6. Principles of transparency

1- The double review mechanism: Research in the journal is subject to a double evaluation in a confidential, bilateral manner. What is meant is that the researcher does not know the evaluator, just as the evaluators have no knowledge of the researcher.

2- The magazine is published in a semi-annual issue for six months in paper and electronic form, focusing on all aspects of the magazine.

3- Editorial staff: That of the magazine

دليل المؤلفين

أولا: تقديم البحث

1. متطلبات تقديم البحث لأول مرّة: يمكن للباحثين اختيار تقديم البحث في ملف واحد ليتم استخدامه في عمليّة التّقييم.
2. متطلبات تقديم البحث المُصحح: عندما يكون البحث المُقدم في مرحلة التّصحيح بعد التّقييم، سيطلب من الباحثين تعديل البحث بالصّيغة الصّحيحة المطلوبة من قبل المجلّة من أجل قبُول النّشر فضلًا عن تزويد المجلّة بأية عناصر إضافيّة من أجل نشر البحث.

ثانيًا: إرشادات أسماء الباحثين

ينبغي أن يسند أسماء الباحثين للبحث اعتمادًا على:

1. مُساهمات جوهرية في تصميم الدّراسة أو جمع على البيانات أو تحليلها وتفسيرها.
2. صياغة البحث أو مُراجعته بشّكلٍ جوهري للمحتوى الفكريٍّ.
3. الموافقة القطعية على النسخة النّهائية المرسلة للنشر.

جميع الشُّروط السّابقة يجب أن تتحقّق في جميع الباحثين المُذكور أسماؤهم في البحث، كما إنّ الحُصول على التّمويل أو جمع البيانات أو الإشراف العام على مجمُوعة البحث تُعتبر غير كافية وبالتالي لا يذكر اسم الباحث ضمن أسماء المشاركين في تأليف البحث؛ وعليه فإن المساهمين في البحث والذين لا يمثلون المعايير سّابقة الذكر يمكن إضافتهم في جُزء الشكر والتقدير كما يجب أن يُوافق جميع الباحثين على تسلسُل الباحثين المدرجين قبل إرسال البحث للنّشر، ويجب أيضًا أن يحصُل توافُق من قبل جميع الباحثين على تكليف باحث واحد ليكون الباحث المسؤول عن المراسلة، والذي سيقع على عاتقه مسؤوليّة ترتيب البحث بأكمله بناءً على مُتطلّبات المجلّة فضلًا عن الحوار مع الباحثين المُشاركين خلال مرحلة التّقييم والمراجعة اللُّغويّة والعمل بالنّيابة عنهُم.

ثالثًا: عملية تقييم البحث

من أجل الحفاظ على نظام تقييم البُحوث، يلتزم الباحثون بالمشاركة في عمليّة تقييم البحوث العلميّة المرسلة من قبل باحثين آخرين. وعند الحاجة قد يكون المؤلّفون مُلزمين بتقديم مُقيمٍ أو مجمُوعة مُقيمين لهيأة التّحرير. تقُوم مجلّة فُرسان الرّد السريع للدّراسات الأمنيّة بمراجعة جميع البُحوث المقدّمة للنّشر فيها إلى مُقيمين اثنين في الأقلّ. تتبنّى المجلّة سياسة مُراجعة مُزدوجة التّغطية إذ إنّ (الباحثون، والمقيمون) كلٌ منهم لا يعلم بالآخر، اذ تجري عملية التقييم بالسرية التامة، وتتم عمليّة تقييم البُحوث من خلال نظام تقديم البُحوث عبر الإنترنت.

رابعًا: تقييم البحوث قبل النشر

بالإضافة إلى عمليّة التّقييم الأوّليّة، تقُوم المجلّة بتقييم البُحوث قبل نشرها بشّكلها النّهائيٌّ من قبل مُدير تحرير المجلّة وأعضاء هيأة التّحرير، يعمل هذا التّقييم من أجل ضمان

جودة البُحوث المنشورة وأن تفي بمعايير النشر العلمية، وتتضمّن هذه المرحلة تعليقات واستشهادات عبر الموقع الإلكترونيّ وعلى الأوراق المنشورة، ويجب ان يستجيب الباحثون لتلك التعليقات والملاحظات الصادرة عن اللجنة العلمية المحكمة.

خامسًا: إعداد ورقة البحث

يجب تقديم البحث باللُّغة العربية أو الإنكليزية فضلاً عن كتابته وفقًا لقواعد الكتابة والإملاء المناسبة، وأن تكتبّ البُحوث مطبُوعة بنوعيّة خطّ Times New Roman بمقدار 14 نُقطة وفي برنامج MS - Word بصيغة عمُود واحد وعلى ورقة بحجم A 4 . كما يجب أن تكون المساحة المطبوعة 15 سُمٍّ × 24 سُمٍّ. وتقدّم البُحوث لمرة واحدة من أجل الحُصول على رقم مُعرّف للبحث في المجلّة . يمكن أن يُسبّب إرسال البحث لأكثر من مرّة رفض البحث بسبب إرسال أكثر من نُسخة واحدة من البحث، كما يجب أن تكون البُحوث مُرفقة بصفحة عُنوان البحث والتي تتضمّن اسم المؤلف / المؤلفين وجهة الانتساب.

سادسًا: إرسال البحوث الجديدة

يتم التّقديم من خلال موقع قيادة الرّد السريع وفي بوّابة المجلّة عبر الإنترنت وسيتم توجيه الباحثين خُطوة بخطوة خلال إنشاء وتحميل ملفّات البحث كجُزء من عمليّة التّقديم، قد يختار الباحثين تقديم البحث في ملف واحد ليتم استخدامه في عمليّة التّقييم، كما يجب أن يكون ملفُّ البحث . docx أو . doc لكي يمكن استخدام هذه الملفّات في عمليّة التّقييم، ويُفضّل أن يتم إضافة جميع الأشكال والجداول في ملفّ البحث الرّئيسيّ.

سابعًا: الاقتباس

يجب اعتماد طريقة (شيكاغو Chicago) في كتابة مصادر الاقتباسات في البحث.

ثامنًا: متطلبات التنسيق

لا تُوجد مُتطلّبات صارمة للتّنسيق، ولكن يجب أن تحتوي جميع البُحوث على العناصر الأساسيّة اللّازمة، على سبيل المثال المُلخص، الكلمات المفتاحيّة، المقدّمة، المواد وطرائق العمل، النّتائج، المناقشة، الاستنتاج، الشكر والتّقدير، تضارُب المصالح وقائمة المصادر، يُرجى التّأكد من تضمين جميع الأشكال والجداول في ملفّ البحث الرّئيسيّ .

تاسعًا: ارسال البحوث بعد التقييم

بصرف النظر عن تنسيق ملفّ التّقديم، وبالأخصّ بعد إجراء تصحيحات المقيمين، يطلُب من الباحثين تقديم ملفّ البحث وفقاً للتنسيق المتبع في مجلّة فُرسان الرّد السريع للدّراسات الأمنيّة في مُستند (MS-Word)، لتجنُّب الأخطاء غير الضّروريّة، ينصح الباحثون باستخدام " التّدقيق الإملائيّ " للملفّ المُقدم . في هذه المرحلة، يجب إدراج اسم الباحث (الباحثون) وُجهة الانتساب.

عاشرًا: تقديم وثيقة البحث

أثناء تقديم البحث لمجلّة فُرسان الرّد السريع للدّراسات الأمنيّة، يجب على جميع الباحثين المساهمين التّحقُّق من أنّ البحث يُمثّل عملا صحيحًا، فضلا عن كونه لم ينشُر كاملا في مجلّة أُخرى أو أنّه يحتوي على مُحتوى مُشابه إلى حدٍ كبيرٍ لبحوث مُؤلّفين آخرين، ويجب مُوافقة الباحثين الآخرين على اختيار احدهم ليكون مسؤولاً عن المراسلة مع هيأة تحرير المجلة وإجراء تصحيحات المقيمين وإثبات صحّتها.

أحد عشر: تقديم البحث والتحقق منه

يجب ألّا تكون البُحوث قد نشرت سابقًا بشّكل رقمي أو ورقي ولا تخضع في نفس وقت إرساله لمجلّة فُرسان الرّد السريع للدّراسات الأمنيّة للتّقييم في مجلّة أُخرى. يجب تقديم نُسخ من المراجع التي من المحتمل أنّ تكون مكررة في البحث الحاليّ (بما في ذلك تلّك التي تحتوي على مُحتوى مُشابه إلى حدّ كبير أو تستخدم نفس البيانات) والتي تمّ نشرُها مُسبقًا أو قيد النّظر في مجلّة أُخرى.

اثنا عشر: بيان الوصول المفتوح

تُعتبر مجلّة فُرسان الرّد السريع للدّراسات الأمنيّة من المجلّات ذات النّفاذ الحُر بالكامل، ممّا يعني أنّ جميع المقالات مُتاحة على الإنترنت لجميع المستخدمين فور نشرها. يجب أن يتم إدراج المُؤلف والمجلّة في البحث بشّكلٍ صحيح. تشمل مزايا الوُصول المفتوح للمؤلّفين ما يلي:

1. حرية الوصول لجميع المستخدمين فى جميع أنحاء العالم .
2. يحتفظ المؤلفون بحقوق النشر الخاصة بعملهم دون قيود .
3. زيادة وضوح الرؤية للقُراء .

ثلاثة عشر: ادعاءات سوء السلوك

مجلّة فُرسان الرّد السريع للدّراسات الأمنيّة حسّاسة للغاية لسوء سلوك البحث وتستخدم جميع الوسائل المتاحة لمنع نشر البُحوث الخاطئة . على الرّغم من عدم وُجُود تعريف مُوحّد لسوء السّلوك البحثي، فإن هيأة تحرير المجلّة تعرف سُوء السّلوك البحثي على نطاق واسع في ثلاث فئات من الإجراءات والسّلوكيات . تُستخدم المجلّة هذا التّعريف لسوء السّلوك في تعاملها مع هذه المسألة وتتبع بدقّة مُخطّط مُتابعة أخلاقيّات النّشر العلمي في التّعامل مع سُوء السّلوك البحثي . وعلى النّحو التالى:

1. سوء معاملة الموضوعات البحثية.
2. تزوير وتلفيق البيانات.
3. القرصنة والانتحال .
4. التزوير وتلفيق البيانات.

يتم تعريف التّصنيع على أنّه أخذ بيانات بُحُوث أُخرى من دُون جمع البيانات العلميّة . يعرف التّزوير بأنه التّلاعب في المواد البحثيّة للوصول إلى نتيجة مُواتية . يمكن أن يحدث تلفيق والتزوير في أيّ مرحلة من مراحل البحث (في الميدان) حتّى نشر البحث حيث يمكن أن يحدُث سُوء استخدام الاقتباس (الإشارة إلى الاقتباس عندما لا يدعم الاقتباس

الحُجة) . تُحاول المجلّة تحديد أيّ نوع من التّلفيق أو التّزييف في جميع مُستويات مُعالجة البُحوث، من الفحص الأولي إلى التّقييم الشّامل للبحث المنقّحة وحتّى بعد نشر البحث . أن تقرير أيّ تلفيق أو تزوير هُو واجب أخلاقيٌّ لمؤلّفينا، والمؤلّفين المُشاركين، والمراجعين، والمحرّرين، والقرّاء . في أيّ حالة من التّزييف أو التّلفيق، تحتفظ المجلّة بحقّها في سحب المادّة الملفّقة أو المزيّفة. تتبُّع المجلّة تعليمات لجنة أخلاقيّات النّشر بحذافيرها في التّعامل مع التّلفيق والتزوير.

Scientific Evaluator Guide

1. Initial instructions

Before you accept or decline the invitation to evaluate the current research, read these questions, as they will help you in this regard:

1. Does current research match your exact specialty? Accept the research evaluation if you believe that you can carry out a solid scientific evaluation process.
2. Do you have a potential conflict of interest with the subject matter or authors? Send these comments to the editor-in-chief when answering the evaluation request.
3. Do you have enough time to evaluate the research? Evaluating research in a solid, scientific manner requires a lot of time. Before you commit to doing so, make sure you know the deadline for submitting the research evaluation.

2. How to evaluate research in the Knights of Rapid Response Journal for Security Studies

The scientific evaluator's evaluation must be a comprehensive critique of the research submitted for publication, and must be in the form of a full report, rather than a few brief sentences. The journal does not require a specific model for the structure of the scientific evaluation report, but the following parts of the report can be used:

1. Conclusion
1. Important and big problems.

4. Minor and minor problems.

The journal encourages the scientific reviewer to help researchers improve the scientific component of their research papers. Therefore, the scientific evaluation report must provide a constructive analysis with clear evidence to the researcher, especially those parts of the research that require modifications. In cases where the scientific evaluator does not want the researcher to share his comments regarding the research, then those comments can be sent to the editor-in-chief of the journal in confidence. The evaluation process may differ from one scientific evaluator to another, but the scientific evaluator must pay attention to the following aspects as much as possible:

1. Has the topic of the current research been discussed previously?
2. Has a contemporary security problem been raised?

3. Is there a need for ethical approvals to conduct the research or does it need these approvals?
4. Is the study model sufficient to answer the study questions?
5. Are the statistical tests used sufficient and are their results reported correctly?
6. Are the figures and tables fully explained, and do they represent the results accurately?
7. Was the research that the researcher conducted previously and included in the current study adequately discussed, and were the results of studies related to the current research compared well?
8. Is there an incorrect inclusion of sources, is a source used on a topic that is different from where it was listed, or has the researcher made extensive use of his previous studies in the current study?
9. Are the results of the current study supported by the conclusions paragraph?
10. Were the limitations of conducting the research noted?
11. Is the conclusion an accurate summary of the current research and its results without repetition?
12. Is the current research language clear and understandable?
13. To help researchers make corrections quickly, the evaluator must send a copy of the evaluated research through the research tracking system sent for publication in the journal. The scientific evaluator must contact the journal if he is unable to evaluate the research at the specified time, in order to make an amendment to the final time for submitting the evaluated research. We encourage the scientific evaluator to constructively criticize the research under examination and to focus his report on objectivity in criticizing the scientific aspects of the research, which includes, for example, the integrity of the research methods and methodology. At the end of the research evaluation process, the following question will be asked to the evaluator: Which of these options do you recommend regarding the current research:

- acceptable.
- It needs major corrections.
- It needs moderate corrections.
- unacceptable.

- Unable to evaluate the research.

3. Confidentiality in the research evaluation process

Research sent for the purpose of evaluation must be kept strictly confidential throughout the evaluation process. The scientific evaluator must not share information about the research being evaluated or discuss its content with anyone outside the research evaluation process. The scientific evaluator may, upon his request, consult one of his colleagues who is related to the subject of the research and who is trusted with the confidentiality and secrecy of the subject of the research being evaluated. In these cases, the researcher must first contact the journal or its editor-in-chief and be informed of the name of the colleague he wishes to contact in this regard, with his information included in the "Comment to the Editor" field in the evaluation report.

4. Conflict of interest

The scientific evaluator must refuse to evaluate the research in one of the following cases:

1. He has a special commercial interest in the research topic.
2. He previously discussed or expressed opinion and advice on the research topic with the researcher.
3. When he feels unable to be objective in evaluating the research for any reason.
4. Applications to be a scientific evaluator

The Knights of Rapid Response Journal for Security Studies appreciates those who have applied for membership in the journal's committees. The journal's editorial board is responsible for selecting research evaluators based on the research itself. In each case, the appropriate evaluators are invited depending on their specialization or the research they have previously published. In order to ensure the possibility of choosing a scientific evaluator, please update your contact information periodically. As for those who are not registered on the journal's website and wish to be chosen as a scientific evaluator in the journal, they must register on the site as a researcher.

دليل المقيم العلمي

أولا: إرشادات اوليّة

قبل أن تقبل أو ترفُض الدّعوة لتقييم البحث الحاليّ ، اقرأ هذه الأسئلة فإنها سوف تُساعدك بهذا الشّأن :

1. هل يُطابق البحث الحاليُّ اختصاصك الدقيق؟ اقبل تقييم البحث أنّ كنت تعتقد بإمكانية قيامك بعمليّة تقييم علميّة رصينة .
2. هل لديك تضارُب مُحتمل في المصالح مع موضُوع البحث أو المؤلّفين؟ أرسل هذه المتعلّقات إلى رئيس التّحرير عند الإجابة على طلب التّقييم .
3. هل لديّك الوقتُ الكافي لتقيم البحث؟ إنّ تقييم البُحوث بشّكل علمي رصين يحتاج إلى وقت كبير فقبل أن تلتزم بذلك تأكد من مُعرفتك للموعد النّهائيّ لإرسال تقييم البحث.

ثانيًا: كيف تقيم بحثًا في مجلّة فُرسان الرّد السريع للدّراسات الأمنيّة

يجب أنّ يكون تقيم المُقيم العلمي ناقدًا شاملا للبحث المُقدم للنّشر ، وان يكون بشّكل تقرير كامل الجوانب ، أكثر من أنّ يكون عبارة عن بضع جمل مُختصرة. إنّ المجلّة لا تطلُب نمُوذج مُحدّد لهيكليّه تقرير التّقييم العلمي، إلّا أنّه يمكن الاستعانة بأجزاء التّقرير الآتية:

1. الخلاصة
3. المشاكل المهمة والكبيرة.
4. المشاكل الثانوية والصغيرة .

إنّ المجلّة تُشجّع المقيم العلمي على مُساعدة الباحثين في تحسين المكنُون العلمي لأوراقهم البحثيّة . لذا يجب أن يُعطي تقرير التّقييم العلمي تحليل بناء بدلائل واضحة إلى الباحث ، وبالأخصّ تلّك الأجزاء من البحث التي تتطلّب إجراء تعديلات عليها . وفي الحالات التي لا يرغب المقيم العلمي أن يُطلع الباحث على تعليقه بخصوص البحث، فيمكن عندها أن يتم إرسال تلّك التّعليقات إلى رئيس تحرير المجلّة وبشكل سرّيّ . إنّ عمليّة التّقييم يمكن أن تختلف من مُقيمٍ علمي لآخر ، إلّا أنّه يتوجّب على المقيم العلمي الانتباه إلى الجوانب الآتية قدر الإمكان :

1. هل موضُوع البحث الحاليّ مطرُوق سابقًا؟
2. هل تمّ طرح إشكاليّة أمنية مُعاصرة ؟
3. هل هنالك حاجة لوجود مُوافقات أخلاقيّة عن إجراء البحث أو هل يحتاج إلى تلّك الموافقات ؟
4. هل نمُوذج الدّراسة كافي للإجابة على أسئلة الدّراسة ؟
5. هل الاختبارات الإحصائيّة المستخدمة كافيه وهل تمّ إدراج نتائجها بشّكل صحيح؟
6. هل الأشكال والجداول وافية الشّرح ، وهل تُمثّل النّتائج بشّكل دقيق ؟
7. هل تمت مُناقشة البُحوث التي قام الباحث بها سابقًا والتي أُدرجت في الدّراسة الحاليّة بشّكل كاف ، وهل تمّ مُقارنة نتائج الدّراسات التي لها علاقة بالبحث الحاليّ بشّكل جيّد ؟

8. هل يُوجد إدراج غير صحيح للمصادر ، أن يستخدم مصدر في موضُوع مُخالف للمّكانّ الذي أدراج فيه ، أو هل قام الباحث باستخدام دراساته السّابقة بشّكل كبير في الدّراسة الحاليّة؟
9. هل تدعم نتائج الدّراسة الحاليّة بفقرة الاستنتاجات ؟
10. هل تمّ التّنويه إلى قُيُود إجراء البحث ؟
11. هل إنّ الخلاصة هي تلخيص دقيق للبحث الحاليّ ونتائجه من دُون تكرار ؟
12. هل لُغة البحث الحاليّة واضحة ومفهومة ؟

لمساعدة الباحثين من أجل إجراء التّصحيحات بشّكل سريع ، يجب على المقيم إرسال نُسخة من البحث الذي تمّ تقييمه عبر نظام تتبُّع البُحوث المرسلة للنّشر في المجلّة . على المقيم العلمي الاتّصال بالمجلة إذ لم يكن بمقدوره إجراء تقييم البحث في الوقت المُحدد لذلِّك ، من أجل إجراء تعديل على الوقت النّهائيّ لتسليم البحث الذي تمّ تقييمه . إنّنا نُشجّع المقيم العلمي على النّقد البنّاء للبحث قيد الفحص والتّدقيق وان يركز في تقريره على الموضوعيّة في النّقد للجوانب العلميّة للبحث ، والتي تتضمّن مثلا سلامة طرائق البحث ومنهجيّته. في نهاية عمليّة تقييم البحث سيتم طرح السُّؤال الآتي على المقيم ، أي من هذه الخيارات تُوصي بها بخصوص البحث الحاليّ :

- مقبول.
- يحتاج الى تصحيحات كبيرة.
- يحتاج الى تصحيحات معتدلة.
- مرفوض.
- غير قادر على تقييم البحث.

ثالثًا: السرية في عمليَة تقييم البحث

إنّ البُحوث التي تُرسل لغرض التّقييم يجب أن تُحاط بسرّيّة تامّة طوال عملية التّقييم. على المقيم العلمي عدم مُشاركة معلومات عن البحث قيد التّقييم أو يُناقش مُحتواه مع أيّ شخص آخر خارج عمليّة تقييم البحث. يمكن للمقيم العلمي ، وبناء على طلبه ، من أن يتم استشارة أحد زُملائه ممّن له علاقة بموضوع البحث ومن الموثوق بهم بسرّيّة وُكتمان موضُوع البحث قيد التّقييم . على الباحث في هذا حالات أوّلا الاتّصال بالمجلّة أو رئيس تحريرها ويتم إعلامه باسم الزميل الذي يرغب في التّواصل معه بهذا الخُصوص، مع إدراج معلوماته في حقل " تعليق إلى المُحرر " في تقرير التقييم.

رابعًا: تضارب المصالح

على المقيم العلمي رفض تقييم البحث فى أحد الحالات الآتية:

1. له اهتمام تجاري خاص بموضوع البحث.
2. قام سابقاً بمناقشة أو إبداء الرأي والمشورة بموضوع البحث مع الباحث.
3. عند إحساسه بعدم قدرته على أن يكون موضوعياً فى تقييم البحث لأي سبب كان.

خامسًا: الطلبات المقدمة لكي تكون مقيمًا علميًا

إنّ مجلّة فُرسان الرّد السريع للدّراسات الأمنيّة تثمن اصحاب الطّلبات المقدّمة لعضوية اللجان الخاصة بالمجلة. إنّ هيأة تحرير المجلّة هي المسؤولة عن اختيار مُقيمي البُحوث واعتمادًا على البُحوث نفسها ، ففي كل حالة يتم دعوة المقيمين المناسبين اعتمادًا على تخصصهم أو ما قد قامُوا بنشره سابقًا من بُحُوث . من أجل التّأكد من إمّكانيّة اختيار مُقيمٍ علمي ، الرّجاء قُم بتحديث معلومات الاتّصال الخاصّة بشّكل دوري، أمّا بالنّسبة لغير المسجّلين في موقع المجلّة الإلكتروني والرّاغبين بأنّ يتم اختيارهم مُقيم علمي في المجلّة فعليهم التّسجيل في الموقع بصفة باحث .

Scientific Evaluator Guide

1. Initial instructions

Before you accept or decline the invitation to evaluate the current research, read these questions, as they will help you in this regard:

1. Does current research match your exact specialty? Accept the research evaluation if you believe that you can carry out a solid scientific evaluation process.
2. Do you have a potential conflict of interest with the subject matter or authors? Send these comments to the editor-in-chief when answering the evaluation request.
3. Do you have enough time to evaluate the research? Evaluating research in a solid, scientific manner requires a lot of time. Before you commit to doing so, make sure you know the deadline for submitting the research evaluation.

2. How do you evaluate a research in the Journal of the Knights of Rapid Response for Security Studies?

The scientific evaluator's evaluation must be a comprehensive critique of the research submitted for publication, and must be in the form of a full report, rather than a few brief sentences. The journal does not require a specific model for the structure of the scientific evaluation report, but the following parts of the report can be used:

1. Conclusion
2. Important and big problems.
3. Minor and minor problems.

The journal encourages the scientific reviewer to help researchers improve the scientific component of their research papers. Therefore, the scientific evaluation report must provide a constructive analysis with clear evidence to the researcher, especially those parts of the research that require modifications. In cases where the scientific evaluator does not want the researcher to share his comments regarding the research, then those comments can be sent to the editor-in-chief of the journal in confidence. The evaluation process may differ from one scientific evaluator to another, but the scientific evaluator must pay attention to the following aspects as much as possible:

1. Has the topic of the current research been discussed previously?
2. Has a contemporary security problem been raised?

3. Is there a need for ethical approvals to conduct the research or does it need these approvals?
4. Is the study model sufficient to answer the study questions?
5. Are the statistical tests used sufficient and are their results reported correctly?
6. Are the figures and tables fully explained, and do they represent the results accurately?
7. Was the research that the researcher conducted previously and included in the current study adequately discussed, and were the results of studies related to the current research compared well?
8. Is there an incorrect inclusion of sources, is a source used on a topic that is different from where it was listed, or has the researcher made extensive use of his previous studies in the current study?
9. Are the results of the current study supported by the conclusions paragraph?
10. Were the limitations of conducting the research noted?
11. Is the conclusion an accurate summary of the current research and its results without repetition?
12. Is the current research language clear and understandable?

To help researchers make corrections quickly, the evaluator must send a copy of the evaluated research through the research tracking system sent for publication in the journal. The scientific evaluator must contact the journal if he is unable to evaluate the research at the specified time, in order to make an amendment to the final time for submitting the evaluated research. We encourage the scientific evaluator to constructively criticize the research under examination and to focus his report on objectivity in criticizing the scientific aspects of the research, which includes, for example, the integrity of the research methods and methodology. At the end of the research evaluation process, the following question will be asked to the evaluator: Which of these options do you recommend regarding the current research:

- acceptable.
- It needs major corrections.
- It needs moderate corrections.
- unacceptable.
- Unable to evaluate the research.

3. Confidentiality in the research evaluation process

Research sent for the purpose of evaluation must be kept strictly confidential throughout the evaluation process. The scientific evaluator must not share information about the research being evaluated or discuss its content with anyone outside the research evaluation process. The scientific evaluator may, upon his request, consult one of his colleagues who is related to the subject of the research and who is trusted with the confidentiality and secrecy of the subject of the research being evaluated. In these cases, the researcher must first contact the journal or its editor-in-chief and be informed of the name of the colleague he wishes to contact in this regard, with his information included in the "Comment to the Editor" field in the evaluation report.

4. Conflict of interest

The scientific evaluator must refuse to evaluate the research in one of the following cases:

1. He has a special commercial interest in the research topic.
2. He previously discussed or expressed opinion and advice on the research topic with the researcher.
3. When he feels unable to be objective in evaluating the research for any reason.

5. Applications submitted to be a scientific resident

The Knights of Rapid Response Journal for Security Studies appreciates those who have applied for membership in the journal's committees. The journal's editorial board is responsible for selecting research evaluators based on the research itself. In each case, the appropriate evaluators are invited depending on their specialization or the research they have previously published. In order to ensure the possibility of choosing a scientific evaluator, please update your contact information periodically. As for those who are not registered on the journal's website and wish to be chosen as a scientific evaluator in the journal, they must register on the site as a researcher.

محتويات العدد

البحوث والدراسات الأمنية

عروض الكتب والدراسات

أَضحى الأمن السّيبرانيَّ واحدًا من مُستحدثات التَّطوُّر التكنولوجي والرَّقمي الذي نعيشهُ في العالم مُؤخرًا، إذ يشهد العالم المتقدّم بكافَّة أرجائه تطورًا كبيرًا لا يُمكننا بأيّ حالٍ الإغفال عنه، لذا؛ أَصبحت الدّراسات الأمنيَّة – التّكنولوجيَّة في العالم الرقمي مقصد الكثيرين من صُنَّاع القرار والمشرّعين والدَّارسين، فمع التَّقدُم التّكنولوجيّ والثَّورة المعلوماتيَّة ودخُول العراق للعالم الرقمي، انبلج صبحُ تداعياتٍ عديدة كان سببها ظُهُور تهديدات وجرائم سيبرانيَّة باتت تُشكل تحدّيًا كبيرًا للأمن القومي العراقي، لدرجة أنَّ الكثير من الدراسات برهنت بأنَّ الفضاء السّيبراني يأتي بالمرتبة الخامسة ضمن تصنيف مسميات الحُروب، تاليًا بذلك حرب البر والبحر والجوّ والفضاء، وهُو ما يستدعي ضرورة وجُود ضمانات أَمنية لا تنفك عن هذه البيئة الرَّقميَّة.

صبت الحكومة العراقيَّة اهتمامها على التَّطوير الشَّامل للوطن وأمنه واقتصاده ورفاهية مُواطنيه وضمان العيش الكريم لقاطنيه، ولقد كان من المسلمات، والمُسلّم به لا يحتاج إلى دليل أن يكُون أحد مُستهدفاتها التَّحوُّل نَحو العالم الرقمي وتنمية البنى التَّحتيَّة الرَّقميَّة، لما له من مزايا اقتصاديَّة وسُرعة في الإنجاز وتقليص للنَّفقات، بما يُعبّر عن مُواكبة التَّقدُّم العالميّ المتسارع في الخدمات الرَّقميَّة وفي الشَّبكات العالميَّة المتجدّدة، وهُو ما يُمكن مُلاحظته ومتابعة سيره في لجنة (22) المشكلة في الأمانة العامَّة لمجلس الوزراء، بما تُقدمه من مشاريع استراتيجيَّة خدميَّة وأُخرى حكوميَّة في المجال الرقمي، سعيًا منها لإلغاء التَّعاملات الورقيَّة في مُؤسسات الدَّولة، وحوكمة تلك المؤسَّسات رقميًّا بما يضمن الشَّفافيَّة والنَّزاهة والحد من استنزاف الوقت واستثمارًا أَمثل ومستدام للطَّاقات والموارد... ومزايا أُخرى، لسنا بصدد ذكر مناقبها لكثرتها.

إِنَّ هذا التَّحوُّل يتطلَّب انسيابيَّة المعلومات وأمانها وتكامل أنظمتها، ويستوجب المحافظة على الأمن السّيبراني ورسم ملامحه ووضُوح اِستراتيجيَّته وتحديد أهدافه في منظُومة أَمن العراق القومي، ابتغاء حماية المصالح الحيويَّة العُليا للدَّولة، والبنى التَّحتيَّة الحسَّاسة والقطاعات ذات الأولويَّة والخدمات والأنشطة الحكوميَّة، وذلك لأسبابٍ مُتعددة أَدركت قيادة فرقة الرَّد السريع أنَّ تُخصُّص ملفّ عدد مُتخصصٍ في العدد الثَّاني لمجلَّة فُرسان الرَّد السريع، رجاء تحليل الواقع الرقمي العراقيّ، وتشخيص أهمّ المعاضل والتَّحدّيات التي تعتري مسيرة أَمن العراق السّيبراني، سعيًا للتَّكامل مع بقيَّة مُؤسسات الدَّولة العراقيَّة في حماية المصالح الحيويَّة العراقيَّة، وللارتقاء بالواقع الأمني وتنميته.

إِذ تُدرك قيادة فرقة الرَّد السريع التَّطوُّر الذي يشهدهُ العالم في هذه السَّنوات، فالتّكنولوجيا الرَّقميَّة لم تُعد تقتصر على الاستخدامات الفرديَّة للهواتف الذكية أو أَجهزة الكومبيوتر، ولا تعتمد عليها المؤسَّسات والشَّركات في إِدارة أعمالها وتخزين بياناتها فحسب، بل أصبحت عامل ربط أساس في معظم نواحي الحياة الشخصية والمعاملات المالية والرسمية، وأنَّ هجمات القراصنة الإلكترونيّين على الشَّركات والحسابات الشَّخصيَّة لسرقة بعض البيانات باتت فكرة بالية ومهترئة بعد الذي شهدته السَّنوات القليلة الماضية من تطوُّرات لِتقنيَّات وخطط المخترقين وأهدافهم من وراء الهُجوم، فتسعى دائرة المخاطر وخسائر هذه الحرب لتصل إِلى تعطيل أَنظمة كبيرة والإضرار بمصالح مُؤسسات أو التَّدخُّل في الشُّؤون الدَّاخليَّة للدُّول، الأمر الذي جعل الأمن السّيبراني هاجسًا عالميا، إذ أَعلنت أَكثر من (130) دولة في العالم عن تخصيص أَقسام وفرق خاصَّة بالحرب الإلكترونيَّة ضمن فرق أَمن الدَّولة الوطني .

واستدلالًا مما تقدم، انَّ إِيجاد أَمنًا سيبرانيًا وطنيًّا عراقيًّا هُو تحدّ وطني ضخم، علاوةً على أن المنظومة الأمنيَّة للدَّولة العراقيَّة بأمس الحاجة إِلى إِطارٍ مُتماسكٍ للأمن السّيبراني، بهدف إيجاد نهج شامل إِزاء المشهد الحاليّ والمستقبلي؛ لأنَّ أَمن الدَّولة والاقتصاد يسيرا بخطىً سريعة ويتَّجهان نحو تضاريسٍ مُتحركة ومتنقّلة رقميًّا، فالجهات

الفاعلة المتورطة في الجرائم السّيبرانيَّة مُجهزة تجهيزًا كافيًا وبأدواتٍ إلكترونيَّةٍ مُتطورة، مسببةً أَضرار ذات بُعد لم يسبق له مثيل، ومن شأن إدراج الأمن السّيبراني في مجال الفضاء الإلكتروني أن يُساعد البلد على الاستعداد والاستجابة لهذه التَّهديدات الأمنيَّة غير التَّقليديَّة، والمساعدة على مُعالجة ضعف البلد في المجال السّيبراني، فضلاً عن ضرُورة تعزيز قُدراتنا على توفير تدابير مُضادَّة بالاشتراك مع جهات فاعلة شرعية وأُخرى غير حكوميَّة، وهذا هُو الأساس المنطقيُّ الذِي يُبنى عليه أَمن العراق السّيبراني، والسّياق الذي يتم من خلاله حماية التَّحوُّل الرقمي في العراق واستدامته .

هذا وأكثر ما استدعى قيادة فرقة الرَّد السريع للبحث في هذا المجال وتحليل الواقع وطرح المعالجات في ملفّ عدد مُتخصص، لرفد صُنَّاع القرار في الدَّولة العراقيَّة بأَهم الأبحاث والدّراسات التي تُساعد في صناعة القرار الأمني والسّياسي.

الفريق الدكتور

ثامر محمد إسماعيل الحسيني

قائد قيادة فرقة الرد السريع

ملف العدد: الأمن السيبراني درع التحول الرقمي العراقي
(بين التحديات الراهنة وضرورات المستقبل)

- هواجس المخاطر السيبرانية على منظومة التحول الرقمي العراقية.

م.د. علي احمد عبد مرزوك

- الأمن السيبراني اوكسجين التحول الرقمي العراقي.

المهندس/ قاسم عبد الرضا شنغيت

- رؤية استراتيجية تحليلية لواقع الحوكمة الرقمية في العراق .

أ.م.د. مروان سالم العلي

- العراق بين ضرورات التحول الرقمي وتحديات الحفاظ على امنه الوطني.

د. يونس مؤيد يونس مصطفى

- تحليل التحول الرقمي في العراق بين التحديات والفرص.

م.د. تمارا كاظم الأسدي

- آليات تعزيز الوعي والتنشئة الرقمية في العراق بعد العام 2003.

م.د. هند محمد عبد الجبار

- الأمن السيبراني العراقي مسار التطور بين المتطلبات والتحديات

أ.د. مثنى فائق مرعي

- قراءة تحليلية لاستراتيجية الامن السيبراني العراقي .

أ.د. حازم حمد موسى

- الأمن السيبراني وإدارة المخاطر .

م.د. زمن ماجد عودة

- الذكاء الاصطناعي كآلية لتحقيق الامن السيبراني العراقي.

م.د. زيد احمد بيدر

- دور الأمن السيبراني في تطور قوة الدولة العراقية .

م.د. سالي سعد محمد

- الأمن السيبراني والتهديدات الأمنية المستجدة .

د. خديجة عرفة

- نحو استراتيجية للأمن السيبراني العراقي .

أ.م.د. محمد ميسر فتحي

هواجس المخاطر السيبرانية على منظومة التحول الرقمي العراقية

م.د. علي احمد عبد مرزوك
مدير تحرير مجلة فرسان الرد السريع للدراسات الأمنية
aliahmed2022iq@gmail.com

يركز ملفُّ العدد الحاليّ لمجلَّة فُرسان اَلرَّد اَلسريع على مَبادئ وَأُسس في حَقل الدّراسات الأمنيَّة المعاصرة، إذ يَتَناوَل الملفُّ عُنصُراً مُهمًّا في التَّحديث السّياسيّ والأمنيّ المعاصر، وَمِمَّا لَا شكَّ فيه بدونه لَا يمكن إتمام التَّحديث، وعلى كَافَّة الأصعدة السياسيَّة منها والاجتماعيَّة علاوةً على القانونيَّة والاقتصاديَّة، إذ إنَّ للأمن السّيبراني العراقيَّ ضَرُورَة وَطَنيَّة آنيَّة وَضَمان تنميَته حَاجَة مُستقبليَّة مُلحَّة لحوكَمة التَّحَوُّل اَلرقمي العراقيَّة اَلتي يَضطَلع بهَا العرَاق مُنذ اَلعام 2020 وَإِلَى يَوم النَّاس هذَا .

فالمبدأ الأوَّل: يَنطَلق من الفكرة القائلة "لَم تعُد الحكومات تَملك خيار الانتظار أو التَّأخُّر في مُوَاكبَة التَّحوُّلات العالميَّة نَحو الرَّقمنة، في ظلّ الإمكانات الهائلة للتّكنولوجيَا الرَّقميَّة في تَطوير أَدَاء الجهَاز الحكوميّ"، وبالتَّوازي مع الفكرة آنفة الذكر، يَزداد الطَّلب وَعلَى نَحوٍ مُطرد في العرَاق، وذلك لضَرُورَة تَحوُّل الحكومة العراقيَّة من وظيفتهَا التَّقليديَّة في كونهَا نموذَجًا مُرتكزًا على القيَام بمهامَّ إداريَّة مُحَدَدَة، إلى نَمُوذَج مُرتَكز على مُتطلَّبات الجمهور وَالذي يُمكن اَلوُصول إلى الخدمات الحكوميَّة والتَّواصل مع وحداته وإداراته من أيّ مَكَان وأي وَقت، وَهذَا لَيس بكَافٍ من وُجهَة نظرنَا المستكينة، فالحكومات الرَّقميَّة لَيسَت مَعنية بتقديم خدمَات مُعَينَة للمواطنين فحسب، بل تَقُوم بخطوَات وَاسعة لتحقيق التَّنمية المستدامة من خلَال تَطوير وَتمكين نَماذج عمل جَديدَة في كَافَّة القطاعات

(التَّعليميَّة، والصّحّيَّة ، وَالبنى التَّحتيَّة.. إلخ) ، فضلاً عن الهدف الأسمى لدَعم الدّيمقراطيَّة، المتمثل بدَعم المشاركة الرَّقميَّة في المناسبات السّياسيَّة كالانتخابات والاستفتاءات الشَّعبيَّة.

وَإن هذَا المبدأ المتُمثّل بالشّقّ الأوَّل من ملفّ العدد والذيَ هو (التَّحَوُّل اَلرقمي العراقيُّ)، إذ وحسبما نعتقد أنه تَمَّت دراسَته من جَوانب مُتَعددَة من قَبل بَاحثين مُتخصّصين في الدَّولة العراقيَّة، وقد عَالَج هذا الملفُّ اَلعديد من الموضوعات، ولعلَّ من أهم ما جاء فيها الآتي:

1. لَن تَتَمَكَّن الحكومة العراقيَّة من مُوَاجهَة تحدّي الفجوة الرَّقميَّة دُون مُعَالجَة الانقسام والتَّباين بَين الطَّبقات المجتمعيَّة وارتفاع مُستويات الفقر والتَّعليم والظُّروف الاجتماعيَّة والاقتصاديَّة كَكُل، زيادةً على ذَلك ثَمَّة حَاجَة مُلحَّة إلى تَطوير المهارات الرَّقميَّة وَتعزيز الثَّقافة والوَعي الرَّقميَّين، بُغيَة استدامة العمل الحكوميّ في تَقديم الخدمات الرَّقميَّة ، وَهذَا لَا يَتأتى بالتَّمَنّي ولَا بالشّعارات الرَّنَّانة، بل بسياسات حُكوميَّة تَوزَّع على كَافَّة القطاعات ذات اَلصلَة بالتَّنشئة الاجتماعيَّة السّياسيَّة العراقيَّة.
2. نرى بأنَّ أفضل مشروع يُمكن أن يُعزّز أَدَاء الحكومة العراقيَّة في مَجَال الحوكمة هُو (اَلهوية الرَّقميَّة العراقيَّة)، وتفعيلهَا في كَافَّة التَّعاملات (الماليَّة، الصّحّيَّة، التَّعليميَّة، الخدميَّة.. إلخ) لتيسير السّياسات وإنجَاز كُلّ مَا يَتعلَّق بمعاملات المواطنين مع الحكومة، وذلك ضمن أُطُر تقنيَّة عَالية المستوى، وَهذَا وفقًا للتَّجارب الدَّوليَّة كَتجربة (أستونيَا) اَلتي أَبدَعت في هذَا المجَال، حَيث تُمثّل مثالا للتَّجربة اَلسلسة اَلتي يُمكن مَعهَا تَطوير الأنشطة الاقتصاديَّة، لَا سيَّما وان وُجُود ملفّ تعريفيّ رَقمي للمواطن (اَلهوية الرَّقميَّة) سيشكّل أَدَاة تَعريف مُشتركَة يُمكن استخدَامهَا للوصول إلى جميع خدمَات الإدارة الحكوميَّة وَحتَّى القطَاع اَلخاص.

3. ثَمَّة قُصُور وَاضح في الجانب التَّشريعيّ العراقيّ، يتجسد بقلَّة التَّشريعات اَلتي تَدعَم عَمَليَّة التَّحوُّل اَلرقمي العراقيَّة، فضلا عن أنَّ هُنَالك اَلعديد من التَّشريعات القائمة تَحتاج إلى تَحديث بمَا يَتَلاءَم مع التَّحَوُّل اَلرقمي المنشود، وَفي هذَا السّيَاق نرى بضرورة تَفعيل التَّوقيع اَلرقمي، لأنَّ جميع الخدمات الحكوميَّة المقدَّمة، وَالتي تُلجَأ المواطن إلى اَلخُروج من الدَّائرة الرَّقميَّة في المعاملات الحكوميَّة إلى التَّوقيع التَّقليديّ، وَهذَا التَّحَدّي اَلذي يَتسم بعرقَلة عمل المؤسَّسات وَفي اَلبُطء الملاحظ في تَكيُّف الحكومة العراقيَّة مع التّكنولوجيَا الجديدة.
4. ومَا يَتصل بالنُّقطة أَعلَاه، نرى بأنَّ الممارسات الحكوميَّة العراقيَّة في الجانب اَلرقمي، قد انتهَجت سبيل التَّعامل مع تكنولوجيَا المعلومات والاتّصالات كاستراتيجيَّة أَقرَب لأن تَكُون " فَنيَّة " الأبعاد وَعلَى مُستوَى خاصٍّ بالمؤسَّسة، أَكثَر من كونهَا استراتيجيَّة عَامَّة تُحَاول تَحقيق الأجندات الوطنيَّة والغاية الرَّئيسة لمثل هَذه المشاريع التَّنمويَّة.
5. إنَّ لمشروع الحوكمة الرَّقميَّة العراقية أبعادًا مُختلفَة ومعقَّدة للغاية، يَستلزم خُرُوج الإشراف على المشروعات (الوزاريَّة، والخدميَّة)، من دَائرة لَجنَة (22) وَتأسيس هَيئَة حُكوميَّة مُتَخصصَة بالتَّحوُّل اَلرقمي، لقياس وَتقييم المخرجات والنَّتائج والتَّأثير النَّاتج عن التحول الرقمي العراقِيّ، وَبمَا يَدعَم اتّخاذ القرارات المستنيرة.

الخُلَاصَة مما تَقدَّم، أنَّ تَعزيز الحوكمة الرَّقميَّة العراقيَّة وبلوغ مُمارسات الحوكمة العراقيَّة لكامل طاقاتهَا لَا يَزَال أمرًا بعيدًا عن الاكتمال والتَّحقق، وَهذَا من البديهيات في ظلّ التَّطوُّرات العالميَّة في المجَال اَلعلمي والتّقنيّ، وَهذَا مَا يَتطلَّب منا إيجَاد ، استراتيجيَّة حُكوميَّة رَقمية وَاضحة المعالم وَلهَا صفة مُستمرَّة وَقابلة للتَّحديث مع آخر التَّطوُّرات اَلتي يُمكن الاستفادة منهَا للدَّولة العراقيَّة في المجَال اَلرقمي، فضلا عن ذَلك لَا يُمكن الحفَاظ على التَّحَوُّل اَلرقمي العراقيّ من دُون وَضع استراتيجيَّة وَاضحة المعالم للأمن السّيبراني العراقيَّ، وَهذَا مَا سَيجري اَلحديث عَنه تباعًا في الفقرات المقبلة.

فالمبدأ الثَّاني: وَالذي يَتَمَثَّل بالشّقّ أو المتغيّر الآخر محلَّ الدّراسة في ملفّ العدد، هو (الأمن السّيبراني العراقيَّ)، وَالذي انطلَقت فكرَة الكتابة فيه برأينَا، وبتوجيهٍ ودعم دؤوب من قبل رئيس تَحرير المجلَّة على ضوء اجتماعات مُتَعددَة ، كَانَت تَنظُر بعَين فَاحصة إلى مَا تُقَدمه الدّنمارك وكوريَا الجنوبيَّة وأستونيَا وفنلندَا والعديد من دُوَل العالم من خدمَات رَقمية (آمنة) ومجهَّزة بكافَّة التَّجهيزات من بنًى تَحتية رَقمية وموارد بَشَريَّة مُحترفَة، لتأمين مشاريعهَا الرَّقميَّة في الفضَاء السّيبراني.

فالعالم اليوم يَشهَد سباقًا جديدًا في التَّسَلُّح، لَا على غرَار المعروفة منهَا في حَقل الأسلحة التَّقليديَّة وَحتَّى غَير التَّقليديَّة، وَهذَا السّبَاق على استحداث أو تَطوير منظومات إلكترونيَّة مُعدَّة لأغرَاض عَسكرية تَعرف اختصارًا بـ (السايبر)؛ على ذَلك احتلَّت الهجمات السّيبرانيَّة مَرتَبة مُتَقدمَة في اَلجُهد القانونيّ وبالذَّات عند المؤسَّسات الدَّوليَّة المتخصّصة هذَا من جَانب، وَمن جَانب آخر فقد تَطوَّر مَسرَح الصّراعات، ومع دُخُول العرَاق إلى الجانب اَلرقمي في تَيسير السّياسات وَتقديم الخدمات للمواطنين، فقد يَدخُل العرَاق وبالتَّأكيد في دَائرة اَلحرُوب السّيبرانيَّة وَيقَد يَتَعرَّض وَبلَا شكّ إلى هَجَمات سيبرانيَّة قد تُشل حَركَة الحكومة العراقيَّة، أو تَنتَهك السّيادة العراقيَّة بمفهومهَا المعاصر، فالعراق وَهُو ضمن مَنظُومة المجتمع اَلدولي عُرضَة للانتهاكات والتَّهديد لمنظومته الإلكترونيَّة، إذ لَا يُمكن للحكومة العراقيَّة أن تَنأَى بنفسهَا عن اَلهَم اَلذي يُمثّل اختراق الشَّبكات وَتهديد أَمنها اَلقومي ومصالحهَا الحيويَّة، لذا نرى وَبكُل تَواضُع أن أهمَّ مَا يُمكن تحليله في هذَا السّيَاق يتمّثل بالآتي:

1. إنَّ التَّقرير الصَّادر عن الاتّحاد اَلدولي للاتّصالات / اَلأُمم المتَّحدة، قد مَنح العرَاق مَراتب مُتَأخرَة عَالميا فقد احتلَّ العرَاق المرتبة (107) عَالميا في الأمن السّيبراني، والمرتبة (13) عربيًّا، إذ تَفوقَت عليه في المستوى عدَّة دُوَل عَرَبيَّة لَا يُمكن مُقارنتهَا بموازناتهَا الماليَّة بالعراق، كالسُّودان وفلسطين والأردنّ وَهذَا مَا يُنذر تَطوير

استراتيجيَّة العراَق في هذَا المجَال، عَبر الأخذ بتدابير مُعَمقَة لمعالجة هذَا الملفّ اَلأمني اَلهام.

2. البنى التَّحتيَّة العراقيَّة في مَجَال الأمن السّيبراني لَا يمكن أن نَقول بأَنَّهَا مَعدُومة، بل تَعمَل وفقًا لأدوَات وبرامج تكنولوجيَّة قد تَكُون تقليديَّة ولَا تُوَاكب التَّطَوُّر الحاصل في العالم السّيبراني اَلآمن، لذَا، من الضَّروريّ على صانع القرَار العراقيّين تَقييم جَاهزية البنى التَّحتيَّة السّيبرانيَّة في العراَق، ووضع اَلخُطط الملائمة لتطويرهَا في مشروعات رَقمية مُستقبليَّة.
3. مَا يُمكن مُلاحظته في العراَق قلَّة الكوادر المتخصّصة في الأمن السّيبراني وَهذَا يُمثّل تحدٍ أساس أَمَام القدرات البشريَّة في تَسخير التّكنولوجيَا الحكوميَّة وَأمنها، مَا يَتطلَّب على المؤسَّسات والأفراد، تَشجيع البحث اَلعلمي المتعلّق بهَذا المجَال، عَبر طُرُق مُختلفَة، كطريق تَأسيس أَقسَام للأمن السّيبراني في الجامعات العراقيَّة، وفتح اَلباب لبرامج دراسيَّة سيبرانيَّة (دبلوم، عُلُوم) تَستهدف العاملين في المؤسَّسات الأمنيَّة، وَبهذَا المجَال يُمكن الاستفادة من التَّجارب الدَّوليَّة والجامعات العالميَّة في كتَابة المناهج الدّراسيَّة والبرامج التَّعليميَّة وبمستويات مُتَقدمَة تَضمَّن النَّتائج الإيجابيَّة دُون الاستعانة بشركَات أَمنية سيبرانيَّة قد تَكُون عَامل تَهديد للأمن الوطَنيّ العراقيّ ومصالحه الحيويَّة.
4. إنَّ تَأسيس فريق الاستجابة للطَّوارئ السّيبرانيَّة غَير كاف، نظرًا لتفاقم التَّهديدات في المستقبل، لذَا، نرى من أن تُؤسّس الحكومة العراقيَّة هَيأة وَطَنيَّة مُوَحدَة لجميع الفرق الإلكترونيَّة للأجهزة العراقيَّة، وَضَرورَة العمل بجدّيَّة على تَحديث الاستراتيجيَّة الوطنيَّة للأمن السّيبراني، وأن تَتَضمَّن تَدابير وسياسات مُوَسعَة لمكافحة الجريمة السّيبرانيَّة، والتَّجسُّس السّيبراني، عَبر تَفعيل الاستخبارات الإلكترونيَّة والشُّرطة السّيبرانيَّة، وبناء اَلجُيوش السّيبرانيَّة المتخصّصة، بُغيَة تَحصين المنظومة الرَّقميَّة العراقيَّة من أيّ خَرق أَمني سيبراني.

ختامًا، إنَّ الأمن السّيبراني العراقيَّ وَكَما أسميناه في ملفّ العدد هُو درع التَّحَوُّل اَلرقمي العراقيّ، وَهُو فُرصَة حَقيقية رَغم مُخَاطرَه، في إعادة النَّظر للبنى التَّحتيَّة للمؤسَّسات الأمنيَّة العراقيَّة، وَفي تَطوير العقيدة الأمنيَّة العراقيَّة، وَمَنحهَا اختصاصات أَمنية أَكثَر دقَّة و (غَيَّر تقليديَّة)، لتعزيز اَلمكنة الأدائيَّة العراقيَّة في مُوَاجهَة التَّحدّيات المستقبليَّة والأخذة في التَّطَوُّر، ونترك القارئ الآن إلى تَصفَح الأبحاث المعمَّقة في هذَا الملفّ، وَعسَى أن نَكُون قد وفَّقنَا في خدمَة بلدنَا العرَاق، اَلذي نُدين لَه بالولاء ونُضمر ونُظهر لكائديهِ البراء.

ملف العدد
الأمن السيبراني
درع التحول الرقمي العراقي
(بين التحديات الراهنة وضرورات المستقبل)

الأمن السيبراني اوكسجين التحول الرقمي العراقي
(دراسة في ضرورات التخطيط المسبق لضمان الاستدامة)

المهندس/ قاسم عبد الرضا شنغيت
مدير عام دائرة البحوث والدراسات الإدارية/
مجلس الخدمة العامة الاتحادي

انطلاقاً من أهمية التحول نحو الحوكمة الإلكترونية والأمن السيبراني في العراق، يتخصص البحث في بيان مراحل تطور الحوكمة الالكترونيَّة والأمن السيبرانيّ، وتحليل وأهم الإمكانات العراقية وما تم تحقيقه على مستوى المشاريع الاستراتيجية الرقمية سواءً ما يتعلق بتقديم الخدمات أو بتيسير الإجراءات الحكومية داخل الوزارات أو بينها، فضلاً عن الأمن السيبراني وبيان استراتيجية العراق السيبرانية، ومرتبة العراق في مؤشرات الحكومة الإلكترونية والأمن السيبرانية، وصولاً الى تحليل التحديات التي تواجه حوكمة التحول الرقمي والأمن السيبراني في العراق وطرح أهم السبل والفرص التي من الممكن واتباعها لمواجهة التحديات وتعزيز السياسات العراقية ذات العلاقة.

الكلمات المفتاحية: الأمن السيبراني، التحول الرقمي، التخطيط المسبق، ضمان الاستدامة.

Cybersecurity is the oxygen of Iraqi digital transformation
(A study into the necessities of advance planning to ensure sustainability)

Engineer/ Qasim Abdel Reda Shagit
Director General of the Department of Administrative
Research and Studies/ Federal Public Service Council

Based on the importance of the shift towards electronic governance and cybersecurity in Iraq, the research specializes in explaining the stages of development of electronic governance and cybersecurity, and analyzing the most important Iraqi capabilities and what has been achieved at the level of digital strategic projects, whether related to providing services or facilitating government procedures within or between ministries, as well as About cybersecurity and a statement of Iraq's cyber strategy, and Iraq's rank in e-government and cybersecurity indicators, leading to an analysis of the challenges facing the governance of digital transformation and cybersecurity

الاستلام	الارجاع	القبول
2024/01/04	2024/4/12	2024/5/3

in Iraq and presenting the most important ways and opportunities that can be followed to confront the challenges and strengthen the relevant Iraqi policies.

Keywords: cybersecurity, digital transformation, advance planning, ensuring sustainability.

المُقدمة

منذ أحداث عام 2003 والعراق يمر بتغييرات سياسية واقتصادية واجتماعية كبيرة وإن أحد الجوانب الحاسمة لهذا التحول هو اعتماد التقنيات الرقمية لتحسين الخدمات العامة وتعزيز الحوكمة وتحفيز النمو الاقتصادي، ومع ذلك عندما تصبح البلاد أكثر اعتماداً على البنية التحتية الرقمية تصبح الحاجة إلى تدابير قوية للأمن السيبراني ذات أهميّة قصوى لحماية المعلومات الحساسّة والبنيّة التحتيّة الحيويّة والحفاظ على ثقة الجماهير في الحكومة وأحد أهم هذه الأسس هي اعتماد أُطر حوكمة متينة وفق حماية سيبرانية معتدٌ بها على مستوى البُنى التحتيّة والبرمجيات والحفاظ على البيانات الحساسة.

إذ أصبح الأمن السيبراني في عالمنا المعاصر أكثر من كونه مسألة مرتبطة بأمن المعلومات والتقنيات وشبكات الحاسوب وغيرها، بحكم علاقته المباشرة بالمجال السياسي والأمني والاقتصادي والاجتماعي والثقافي، إذ تعتمد معظم أن لم تكن جميع المؤسسات الحيوية لأية دولة على تقنيات المعلومات وفي عملياتها اليومية التي تعتمد بدورها على أنظمة الاتصالات والمعلومات وهذا يعني بالنتيجة أنها تعتمد على الأمن السيبراني، ومنذ العام 2003 شهد العراق انفتاحًا وتطورًا ملحوظاً في المجال التقني والمعلوماتي، مما جعل مؤسساته الرسمية والخاصة أكثر عرضة للهجمات السيبرانية، إذ نشطت عبره التجارة والوسائل غير المشروعة مما فرض تحديات جديدة أثرت بشكلٍ مباشرٍ في منظومة أمنه الوطني وتستلزم معالجتها.

اولاً: أهداف البحث

1- استكشاف الحالة الراهنة للأمن السيبراني في العراق ودور الحوكمة وفق الإجراءات الحكومية في تشكيل المشهد الرقمي.
2- تحقيق سياسات واستراتيجيات وأطر الأمن السيبراني التي اعتمدتها البلدان الأخرى التي خضعت بنجاح للتحول الرقمي.
3- تقديم توصيات سياسية لتعزيز وضع الأمن السيبراني في العراق وتعزيز بيئة رقمية أكثر أمانًا.

ثانيا: إشكالية البحث

تسعى الدول من خلال سياساتها العامة الى اعتماد حوكمة التحول الرقمي في تسيير إجراءاتها وتبسيط خدماتها في المؤسسات الحكوميّة والقطاع الخاص، وأصبحت العديد من الدول تحتل الصدارة والريادة في مجال حوكمة التحول الرقمي، وأمام هذا التطور في مجال الحوكمة الرقمية تصاعدت وتيرة التهديدات السيبرانية في الفضاء السيبراني، والتي وضعت الحكومات ونهجها الالكتروني أمام تحدي البقاء والاستمرار في هذه السياسات، وبالتالي وضعت الدول العديد من التدابير والسياسات والاستراتيجيات منه على المستوى المحلي والأخرى على مستوى التعاون الدولي لمواجهة تلك التهديدات، ومواكبة عجلة التقدم في مجال تطور الإدارة والحكم.

وعلى أساس ما تقدم، تتمثل إشكالية الدراسة في التساؤل الرئيس الآتي: ما هو الأمن السيبراني والحوكمة للتحول الرقمي في العراق؟ وعلى أثر هذا التساؤل تندرج لدينا العديد من التساؤلات، نذكر منها ما يلي:

- ما أهم طبيّعة التحول الرقمي في العراق؟ وما أهم محدداته ومهدداته؟
- ما السياسات والتدابير الحكومية العراقية لتعزيز حوكمة التحول الرقمي والأمن السيبراني؟

ثالثا: فرضية البحث

توصلت الدراسة الى فرضية مفادها: (أن عملية تطور الحوكّمة الرقمية ليست عبارة عن رقمنة البيروقراطيات وبينت العديد من الدول وعلى رأسها (استونيا، والأمارات العربية المتحدة) أنها سعت جاهدة الى إزالة نقاط الاحتكاك بين الحكومة والمواطن التي تخدمه، وسعى العراق الى إزالة هذا الاحتكاك وبالرغم من التقدم الذي يشهده العراق؛ تبقى التكنولوجيا ليست خالية من المخاطر ويجب أن تكون معالجة مخاوف الخصوصية والأمن السيبراني والحوكمة الالكترونية أولوية في التحول الرقمي وديمومة المشاريع الرقمية في العراق وإدارتها للحفاظ على رقمنة الخدمات الحكومية).

رابعا: مناهج الدراسة

لكي تكون الدراسة متكاملة من خلال تقديم تحليلات علميّة موضوعيّة إيجابيّة حول موضوع الدراسة، فمن المهمّ صياغة هذه الدراسة ضمن سياقات علميّة منطقيّة منهجية إذ وجدنا من الضّروريّ أن نسير على خطّى المناهج الآتية:

- **المنهج التحليلي الوصفيّ:** والّذي سنحاول من خلالهِ استنباط الحقائق والتّأكّد من مصداقيتها، وعدم إغفال كافّة التأثيرات المتعلقة بهذا البحث.
- **منهج دراسة الحالة:** يتيح هذا المنهج الإحاطة والتّعمّق في جوانب الحالة موضع البحث كما أنّه يتلاءم مع طبيعة الدّراسة من حيث كونها لا تهدف الى التّعميم وإنّما هي دراسة التّجربة العراقيّة.
- **المنهج التاريخي:** فهو يجيبُ على السّؤال كيف؟ بمعنى أنّه يسمح بتتبّع التّطوّرات المختلفة، ويسمح بدراسةِ الأحداث والوقائع، ويدخل عامل الزّمن في مقوّمات التّحليل جميعًا، وتقديم الأدلّة في التّحليل السّياسيّ.

المبحث الأول: حوكمة التحول الرقمي في العراق (الواقع، التحديات، الفرص)

ترتبط فلسفة حوكمة التحول الرقمي بالحكومة كمصدر للمعلومات والخدمات كما أن المواطنين ومنشآت الأعمال والمنظمات المختلفة المتواجدة في المجتمع تعامل كمستفيدين يرغبون الاستفادة من هذه المعلومات والخدمات الحكومية ويمثل ذلك تغييرا جوهريًّا في ثقافة تنفيذ الخدمات والمعاملات الحكومية ونظرة المواطنين والأعمال اتجاهها، والهدف الإستراتيجي للحكومة الالكترونية يتمثل في دعم وتبسيط الخدمات الحكومية لكل الأطراف المعنية، واستخدام تكنولوجيا المعلومات يُساعد على ربطِ كل الأطراف معًّا وتدعيم الأنشطة والعمليات أي أنه في الحكومة الالكترونية تساند الوسائل الالكترونية وتسهم في تدعيم جودة الأعمال التي تقدمها الأطراف الثلاثة المعنية (الحكومة، والمواطنون، والقطاع الخاص)، إذ أن الحكومة الالكترونية تمثل تحولًا اساسياً في مفهوم الوظيفة العامة بحيث ترسخ قيم الخدمة العامة ويصبح جمهور المستفيدين من الخدمة محور أهتمام مؤسسات الدولة[1]، وبذلك يعد برنامج الحكومة الالكترونية عنصراً حيوياً لإصلاح وتحديث القطاع العام في العراق حيث اعتمدت الحكومة العراقية نهجاً متكاملاً للحكومة الإلكترونية لتنميته على المستوى الوطني والمحلي بالتماشي مع استراتيجية التنمية الوطنية، والأهداف الإنمائية العراقية، والخطة الوطنية للتنميّة، ويواجه العراق العديد من التحديات في مجال حوكمة التحول الرقميّ على المستويات البشريّة والتشريعيَّة والفنيَّة.. وغيرها ما أدى الى تموضع العراق في مراكز متأخرة في مؤشرات الحكومة الالكترونية الصادرة عن الأمّم المتحدة، وعلى هذا الأساس سيتناول هذا المبحث واقع الحكومة الالكترونية في العراق وتحدياتها وأهم الفرص والتدابير لتعزيزها وتطبيقها على

مستويات تنموية عالية المستوى، فضلاً عن مقارنة الانموذج العراقي مع نماذج الدراسة المختارة (استونيا، والامارات العربية المتحدة)، بُغية إيجاد أبرز السبل والتدابير للاستفادة من التجارب المختارة.

المطلب الأول: حوكمة التحول الرقمي في العراق (البادرة التاريخية، الإمكانيات)

اولاً: البادرة التاريخية لحوكمة التحول الرقمي في العراق

ادرك صُانع القرار العراقي أهمية اعتماد حوكمة التحول الرقمي في مؤسسّات الدولة، وكانت بدايات هذا الإدراك في عام 2003 حينما وقعت وزارة العلوم والتكنولوجيا عقداً بمبلغ 20 مليون دولار مع إحدى الشركات الإيطالية لتنفيذ مشروع الحكومة الالكترونيّة، وكانت خطة الوزارة تتكون من ثلاثة مراحل[2]:

1. المرحلة الأولى: قصيرة المدى وعمرها (سنتان)، وتتضمن تأسيس البنيّة التحتيّة لتكنولوجيًّا المعلومات وتقديم الخدمة إلى موظفي وزارة العلوم والتكنولوجيا.
2. المرحلة الثانية: ومدتها خمسة سنوات وتضمنت تقديم الخدمة إلى موظفي الوزارات والى القطاع التجاري.
3. المرحلة الثالثة: بعيدة المدى وتهدف إلى تقديم الخدمة إلى الموظفين.

كان الهدف من تأسيس دائرة تكنولوجيا المعلومات في وزارة العلوم والتكنولوجيا أن تتولى إنشاء الحكومة الالكترونية في العراق، وأن تكون مهمتها الإستراتيجية هي ردم الهُوة الرقمية التي تفصل العراق عن مصاف الدول المتقدمة[3]، وقد باشرت الدائرة عملها في تشرين الأول من العام 2003 وذلك وقت تأسيس وزارة العلوم والتكنولوجيا، وتم تشكيل هيئة تنسيقية مشرفة على النشاط تتكون من ممثلين من الوزارات العراقية التي تمارس العمل في القطاع المعلوماتي، وتجتمع هذه الهيئة بشكل دوري وتستضيف ذوي الخبرة والاختصاص في القطاع الخاص والقوى متعددة الجنسية لضمّان النموذج الذي تتبعه الحكومة العراقية في تنفيذ الحكومة الالكترونية، وكان أهم ما تحقق خلال الاجتماعات التي أستمرت في تلكَّ المدة هو نشر الوعي وتطوير القابليات وسعة الأفق واطلاع الملاكات في الوزارات العراقية على المهمات والواجبات وتطور المفاهيم والرؤى المتجددة للهدف المشترك والنتائج المستقرة

ميدانياً، ووضعت خارطة طريق وإستراتيجية تطوير قطاع تقنية المعلومات والاتصالات في عموم دوائر الدولة والقطاع الخاص[4].

وقام العراق بالبدء في تنفيذ برنامج الحكومة الالكترونية عام 2009[5]، وخلال 10 سنوات على عدة مراحل وكالآتي:

1. صدر الأمر الديواني (46) لسنة 2009 المتضمن تشكيل لجنة أوكلت مهمّة إنشاء المشروع الى وزارة العلوم والتكنلوجيا العراقية وعضوية ممثلين من أغلب الوزارات.
2. بعد مرور أكثر من عام قدمت وزارة العلوم والتكنلوجيا مشروعها واعتمدتهُ الأمانة العامة لمجلس الوزراء، وعُرِض بمجلس الوزراء بجلسته (11) في 2010/7/20 من قبل وزير العلوم والتكنولوجيا، وأُقر من قبل مجلس الوزراء.
3. في نهاية عام 2011 أرسل المشروع الى مجلس النواب، وعقد مجلس النواب حلقات نقاشية وآخرها في 2011/10/4، وذكرت توصيات لا مجال لسردها دارت بين لجان المجلس استمرت لغاية 2012، ولم يتم تشريع القانون.
4. عقدت الامانة العامة لمجلس الوزراء عام 2014 ندوة حضرتها اغلب القيادات الادارية تشير باقتراب إطلاق خدمات الحكومة الالكترونية.
5. محصلة عمل اللجان المشكلة خلال السنوات من 2012 لغاية 2015 قانون التوقيع الالكتروني والمعاملات الالكترونية رقم (78) لسنة 2012 معطل لم يعمل به، وعقدت الجامعة المستنصرية ورشة علمية عن معوقات تنفيذ هذا القانون[6].
6. في عام 2016 تشكلت لجنة تنسيق وإدارة النشاط الحكومي باتجاه الحكومة الالكترونية بموجب الأمر الديواني (45) لسنة 2016 برئاسة الأمين العام لمجلس الوزراء السيد علي العلاق.
7. بتاريخ 2017/3/22 أعلن الأمين العام لمجلس الوزراء في مؤتمر صحافي حضرته كافة وسائل الاعلام الوطنية على هامش الاجتماع الذي عقدته لجنة الحوكمة الالكترونية أن الامانة ستبدأ بتنفيذ التحول نحو الحكومة الالكتروني سواءً بين دوائرها أو الوزارات الرئيسية ليتم التواصل بينها الكترونيًّا، معربًّا عن أملهِ في تحقيق 80% من هذه الخطوات خلال العام الحالي.

8. بتاريخ 2018/10/17 تم التصويت على إقرار توصيّات لجنة الأمر الديواني رقم 45 لسنة 2016 لجنة تنسيق وإدارة النشاط الحكومي باتجاه الحوكمة الالكترونية بشأن الشبكة الحكومية المؤمنة.
9. في عام 2020 تشكلت لجنة جديدة سميت (لجنة تنسيق وإدارة النشاط الحكومي باتجاه الحكومة الالكترونية) بموجب الأمر الديواني (22) لسنة 2020 برئاسة الأمين العام لمجلس الوزراء وحلت هذهِ اللجنة محل اللجنة (45) السابقة، وتضم ممثلين في عضويتها من مُختلف الوزارات والمؤسسات لإعادة تقييم المشروع والبدء بإنشاء بُنى تحتية تتعلق في بناء مركز بيانات وطني ليستضيف مختلف الخدمات الالكترونية للمواطنين والمؤسسات المختلفة.

تشمل الجهات الفاعلة الرئيسية الأمانة العامة لمجلس الوزراء و لجنتها الفرعية المتعلقة بقضايا الحكومة الإلكترونية لجنة (22) لسنة 2020، وكذلك المركز الوطني للبيانات كوحدة تنفيذ رئيسية، وتمثل اللجنة 22 بمثابة هيئة استشارية وكذلك كوحدة تنسيق، لأن لديها دور استشاري وتنسيقي على حدٍ سواء، لكنها تفتقر إلى الموظفين الدائمين ليعتبروا وحدة تنسيق فعلية[7].

تتمثل مهام اللجنة 22 الرئيسية في العمل على متابعة مشروع التحول نحو الحوكمة الالكترونية وإدارة مهامه، وتنسيق عملياته، بالتعاون مع الوزارات والجهات غير المرتبطة بوزارة والمحافظات، عن طريق (تطوير عمل المؤسسات الحكومية من خلال استخدام الأنظمة والتقنيات الحديثة وتبادل المعلومات بما يخدم تطوير الخدمات المقدمة للمواطنين، وتبسيط إجراءات العمل، وزيادة الموارد المالية للدولة، والمساهمة في وضع الخطط والقرارات بناءً على بيانات ومؤشرات دقيقة)، وقد عقدت اللجنة وفرقها خلال مدة عملها عددًا من الاجتماعات نتج عنها أكثر من (210) توصية الى المؤسسات الحكومية لمساعدتهم في عملية التحول الرقمي وتنفيذ مشروع الحوكمة الالكترونية، وتتألف اللجنة 22 من رئيس اللجنة، الأمين العام لمجلس الوزراء الدكتور حميد نعيم الغزّي و 20 عضوا من مختلف الوزارات والهيئات والوكالات ذات الصلة ومساعدان (منظمان) لاجتماعات اللجنة[8].

وهناك (10) فرق عمل رئيسية تعمل بصورة متوازية ومشتركة، وتساندها العديد من اللجان والفرق الفرعية، التي تشكل مؤقتاً لإنجاز مهام معينة تحدد من خلالها توصيات اجتماعات اللجنة، وينتهي عملها بانتهاء المهمة المكلفين بها[9].

وتتمتع اللجنة 22 بصلاحية وسلطة اتخاذ القرارات، وتُعتبَر المقترحات التي تقدمها اللجنة مُلزِمة للوزارات على الأقل بقدر ما يتعين على الوزارات النظر فيها، وتشمل الملاحظات الأولية أن هناك مجالًا للتحسين من أجل تنسيق استراتيجية الإدارة الإلكترونية على مستوى الوزارة وتنفيذها، فضلاً عن تخطيط ميزانية تكلوجيا المعلومات وتنفيذها والإشراف عليها، و فيما يتعلق بالتنفيذ، تم التركيز على تطوير البنية التحتية، ولكن لم يحرز سوى تقدماً محدوداً في التطوير المنسق للأنظمة الحديثة، وإدارة قابلية التشغيل البيني، وتبادل البيانات[10].

وقد أجرى الباحث مقابلات معمقة مع رئيس لجنة (22)، وتسنى الاستفسار عن تنظيم اللجنة وفرقها الفرعية مع التركيز على أعضاء الفريق القانوني وخطتهم والعمل المنجز حتى الآن ورؤيتهم وتوجيهاتهم الإضافية، حيث تقرر في تشرين الثاني 2021 ، أن هناك حاجة إلى فريق فرعي معني بالمسائل القانونية للنظر في الإطار القانوني والاستراتيجيات الحكومية ذات الصلة، و تشمل المهام الرئيسية للجنة الفرعية القانونية صياغة القوانين، ومراجعة القوانين التشريعية القائمة والمتداولة، بالإضافة إلى وضع الاستراتيجيات، والوثائق المتعلقة بالسياسات، ويتألف الفريق القانوني الفرعي من 5 أعضاء (احد أعضاء الفريق يحمل شهادة القانون، وبقية الأعضاء من اختصاصات تقنية) وهذا مؤشر على بعد الاختصاص ضمن مهام ومسؤوليات الفريق، وقد أبرزت نتائج مقابلات الباحث بأن هناك عددًا من المقترحات التشريعية قيد الاعتماد، ولكن هناك مشاكل تتعلق بالاعتماد الفعلي للقوانين، فعلى سبيل المثال وبسبب الاختلافات في الرأي، لم يدخل قانون الجرائم الإلكترونية الذي تمت صياغته في عام 2008 حيز التنفيذ بعد، ولم يتم تنفيذ التشريع المتعلق بالتوقيعات الإلكترونية تنفيذًا كاملاً، كما أن عمليات اعتماد أو مراجعة قانون التوقيع الإلكتروني، وقانون الحق في الحصول على المعلومات، ومشروع قانون حماية المعلومات الشخصية، والقانون التجاري، واستراتيجية أمن المعلومات مازالت متوقفة[11].

تم إعداد مسودة خارطة الطريق الاستراتيجي للتحول الالكترونيّ من خلال تظافر جهود لجنة الحوكمة الالكترونية والفريق الاستشاري للجنة الأمر الديواني (22) لسنة 2020

وقسم إدارة الجودة الشاملة والتطوير المؤسسي بعد الاطلاع على عددٍ من استراتيجيات الدول المقارنّة ودراسّة تقارير المنظمات الدوليّة المشار لها آنفاً والتنسيق مع الجهات ذات العلاقة، تم تأليف فرق عمل في الوزارات والجهات غير المرتبطة بوزارة والمحافظات من الموظفين المعنيين في تشكيلات الجودة، وتقنية المعلومات التخطيط الاستراتيجي، والقانونية والإدارية والمالية وحسب الإعمامات المرقمة بالعدد /49922 و 18256 و 32266 والمؤرخة في 2022/2/7 و 2022/5/19 و 2022/9/14 على التوالي، يتولى الفريق المشاركة في صياغة الخطة الاستراتيجيّة للحكومة الالكترونيّة، وتم الطلب من الوكالة الدولية للتعاون الإنمائي (UNDP) وبعض الجهات الدوليّة لغرض تقديم الدعم الاستشاري اللوجستي للخطة الاستراتيجية، فضلاً عن تبني مؤتمر دولي لغرضِ تسليط الضوء على الجهود الوطنية للتحول الرقمي وفتح آفاق التعاون مع الجهات الدولية والقطاع الخاص تنفيذاً للتوصية رقم 2 من الاجتماع (17) للجنة الأمر الديواني (22) لسنة (2020) حول عقد مؤتمر دولي للتحول الرقمي لتقديم رؤية متكاملة، وما زال الفريق المكلف بإعداد وثيقة الخطة الإستراتيجية مستمراً بالعمل خاصة بعد صدور قانون الموازنة العامة وتوجيهات دولة رئيس الوزراء آنفة الذكر[12].

وقد تم إقرار توصية اعتماد إستراتيجية تحول رقمي شاملة عالية المستوى تتوخى العناصر والهياكل الأساس لنظام الحوكمة الرقمية وتكليف اللجنة بإعدادها بالتنسيق بينها والجهات ذات العلاقة، وتم تأليف فريق من المخططين الإستراتيجيين وصانعي السياسات لإعداد وصياغة الخطة الإستراتيجية الوطنية الخاصة بالتحول الرقمي بالتنسيق مع الوزارات والجهات غير المرتبطة بوزارة والمحافظات كافة بموجب الأمر الإداري المرقم بالعدد 9670 والمؤرخ في 2023/2/28، ليتولى مهمة إعداد الاستراتيجية آنفاً بعد الاستعانة بالخبرات المحلية والدولية التي تعمل في هذا المجال، وله عقد الاجتماعات والورش اللازمة مع الوزارات والجهات ذات العلاقة[13]، وتمثلت الرؤية والرسالة والأهداف الاستراتيجية للخطة الحكومة الإلكترونية بالآتي[14]:

1. **الرؤية:** خدمات إلكترونية متكاملة لتعزيز الاقتصاد الرقمي وتسهيل حياة المواطن.
2. **الرسالة:** إدارة التحول الرقمي لبناء مجتمع معرفي مستدام يلبي احتياجات وطموحات المواطن ويسهم في ردم الفجوة الرقمية من خلال تهيئة البُنى التحتية،

وتبني القوانين والتشريعات والسياسات والمعايير الدولية اللازمة للحكومة الالكترونية بشراكات مختلفة للحاق بالركب العالمي.

3. **الأهداف الاستراتيجية:** وتتمثل بالآتي:

أ. توفير البُنى التحتية اللازمة لبناءِ الجاهزية الالكترونية.

ب. خلق حكومة ممكنة وذات أداء عالٍ.

ج. رفع مستوى الشفافية والمشاركة المجتمعية.

د. رفع مساهمة قطاع تقنيّة المعلومات والاتصالات في الناتج المحلي الإجمالي (GDP) وصولاً للاقتصاد الرقمي.

ثانيا: إمكانيات الحكومة الالكترونية العراقية

كانت من أبرز مخرجات لجنة (22) تأسيس مركز البيانات الوطني، وهو مركز متخصص لحفظ بيانات المؤسسات الحكومية، ويجري الى حد هذه اللحظة تجهيزهُ وفق أحدث المواصفات ومن الجوانب الفنية جميعها[15]، وتمثلت أهم إنجازات لجنة (22) لسنة (2020) بنوعين من المشاريع، تمثلت بالمشاريع المركزية، التي سيجري التفصيل فيها من ناحية تشكيلاتها وأدائها ومخرجاتها وآلية عملها والبالغة (12) مشروعاً مكتمل التنفيذ، فضلاً عن المشاريع التخصصية وهي المشاريع المختصة بعمل المؤسسات الحكومية التي يقوم مركز البيانات الوطني بالمساعدة في إنجازها من خلال تقديم الاستشارات وتوفير البنى التحتية وتوفير الأدوات اللازمة، ودراسة المواصفات الفنية ووضع المعايير والكلف التخمينية وغيرها من المتطلبات الضرورية لإتمام عملية التحول الرقمي في الوزارات، وبلغت عدد المشروعات المنجزة أكثر من (350) مشروعاً، موزعة على (22) وزارة، و(18) هيئة وجهات غير مرتبطة بوزارة، و(2) ديوان محافظة[16]، وفيما يلي المشاريع التكاملية (المركزية) لمركز البيانات الوطني:

1. النافذة الموحدة (بوابة أور الإلكترونية للخدمات الحكومية)

تعد بوابة أور الإلكترونية منصة الخدمات الحكومية الرقمية الرسمية لجمهورية العراق، وهي نقطة وصول لكافة الخدمات الحكومية التي تقدمها المؤسسات الرسمية، وتمثل نواة انطلاق مشروع الحكومة الالكترونية بتاريخ 2021/9/5، وهي حاليًا مصنفة ضمن مواقع

الإحصائيات العالمية، حيث تصدرت البوابة كأول موقع حكومي عراقي من ناحية التصنيف، والعمل مستمر لتطويرها بالشكل الذي يجعلها تضاهي مثيلاتها في الدول المتقدمة[17].

2. المشروع الوطني لإلغاء معاملات صحة الصدور نظام الوثائق المؤمنة الإلكتروني:

هو نظام الكتروني لإلغاء ترويج معاملات صحة الصدور للوثائق، منجز من قبل ملاكات الأمانة العامة لمجلس الوزراء / دائرة مركز البيانات الوطني، وصدر بتاريخ 2022/5/24 توجيه رئيس مجلس الوزراء بإعمام النظام ليشمل كافة القطاعات الحكومية والغاء ترويج معاملات صحة الصدور التي ترهق كاهل المواطنين، ومنذ ذلك التاريخ لغاية الآن يعمل النظام في (٦١) جهة (١٧) وزارة، و(٣٥) هيئة ودائرة، و (٩) محافظات، وبلغ عدد الوثائق المرفوعة في النظام التي تم الغاء ترويج معاملة صحة صدور لها (١،٥٥١،٤٨٥) مليون وخمسمائة وواحد وخمسون ألف واربعمائة وخمسة وثمانون معاملة لغاية 2023/6/8 ، حسب موقع منصة أور ولم يتسنى التأكد من الطرف المستفيد أو مقيم معتمد خارجي، ويعمل النظام على إنشاء وأضافة رمز الاستجابة السريعة "QR" الخاص بكل وثيقة ليمكن المواطن من الاحتفاظ به وتقديمه للدوائر التي يقصدها، بُغية اطلاعها بشكلٍ مُباشرٍ على الوثيقة المطلوبة من خلال هذا الرمز، من دون الحاجة الى ترويج معاملة صحة الصدور [18].

3. مشروع الخدمة الارشادية

تم إنشاء مركز اتصالات يعتمد أحدث التقنيات كخدمة إرشادية للمواطنين عن آلية التقديم على الخدمات المتاحة ضمن بوابة "أور" كذلك في حالة مواجهة أي مشاكل أثناء التقديم على الخدمات المذكورة أنفاً وذلك من خلال الاتصال بالرقم المجاني (٥٥٩٩)، طيلة أيام الأسبوع من الساعة (٨) صباحاً ولغاية الساعة (١٢) منتصف الليل، وقد انضمت الى هذهِ الخدمة (٢٤) جهة حكومية متمثلة بـ (١٥) وزارة و(٩) هيئات، علماً أن كافة المكالمات مسجلة وموثقة لضمان جودة الخدمة المقدمة وتعمل ضمن بدالة إلكترونية متطورة[19].

4. الاستعلامات الالكترونية

نظام الكتروني يعمل من خلال نافذة للدخول الموحد، يُمكن المواطنين من الاستعلام والاستفسار الكترونياً، وترد الإجابة لهم عبر الرسائل النصية القصيرة من خلال الهواتف النقالة، بما ينعكس بالفائدة على تقليل زخم المراجعات للدوائر الحكومية وتسهيل

الإجراءات في حصول المواطنين على المعلومات ومتابعة طلباتهم، وقد جاءت عدد خدمات الاستعلامات بـ(٢٦) خدمة مفعلة في (٢٢) جهة تمثلت بـ(٨) وزارات و(١٤) جهة غير مرتبطة بوزارة، حيث أن بعض الوزارات لديها أكثر من خدمة استعلامات مثل الدفاع والتعليم العالي والبحث العلمي والصحة، وفيما يلي أبرز تفاصيل المشروع[20]:

أ. **أهداف المشروع:** يهدُف المشروع بشكلٍ أساسي الى تعزيز ثقة المواطن بالمؤسسات الحكومية وبأهمية معاملته ويُعلمه بجميع مراحل سيرها عبر خدمة الرسائل النصية للهاتف النقال ويستطيع المواطن الاستفسار والاستعلام عن أية خدمة يرغب بها ويمكنه من معرفة الوثائق والاجراءات المطلوبة ويمكنه من تقديم الطلبات الكترونيًا ومعالجتها وإنجازها بعد استكمال جميع المتطلبات الخاصة بالخدمة، كل هذا دون الحاجة لعناء الحضور.

ب. **الجهات المستفيدة:** كافة المؤسسات الحكومية.

ت. **نسبة الإنجاز:** 33.5% منجز.

ث. **الجهات المنفذة للمشروع:** وزارة التعليم العالي والبحث العلمي، وزارة الدفاع، وزارة الكهرباء، وزارة الصناعة والمعادن وزارة الصحة مجلس القضاء الأعلى، مؤسسة السجناء السياسيين الهيئة العراقية للسيطرة على المصادر المشعة، هيئة الأوراق المالية، وزارة التجارة، مجلس الدولة، وزارة التربية، هيئة التصنيع الحربي، ديوان الوقف السني، ديوان الوقف الشيعي، ديوان الرقابة المالية الاتحادي، الهيئة الوطنية للاستثمار، مؤسسة الشهداء، ديوان محافظة ميسان، المفوضية العُليا المستقلة للانتخابات، وأمانة بغداد.

ج. **عدد الطلبات الكلي:** 2133 طلباً.

ح. **المهمة:** إنشاء وإدارة الخدمة وتدريب الكوادر للعمل عليها.

5. دليل الخدمات العامة (العرض الحي الإلكتروني)

منصة توفر الوصف والشرح لكافة المتعلقات بالخدمات الحكومية التي على تماس مع حياة المواطن مما يتيح المعلومة للمواطنين دون الحاجة الى مراجعة الدوائر للاستفسار عن الوثائق المطلوبة من (المتمسكات والوقت المستغرق للإنجاز، التكاليف المالية.... الخ)، كما يوفر دليل متكامل للوزارات لغرض السعي لتحويل هذه الخدمات إلى خدمات الكترونية، يضم الدليل

حالياً (537) خدمة موزعة على (٤٩) جهة تمثلت بـ (٢٠) وزارة و(٢٩) جهة غير المرتبطة بوزارة[21].

6. منصة إنشاء الخدمات (Eservices)

منصة إلكترونية تم تأسيسها بملاكات وطنية خالصة، لإنشاء وتصميم الخدمات الإلكترونية دون الحاجة إلى كتابة كود البرامج، مما يتيح للمؤسسات الحكومية تحويل الخدمات الورقية إلى إلكترونية خلال أيام قليلة وبأوقات قياسية، وتم انجاز أكثر من ١٣٨ خدمة إلكترونية من خلال تلك المنصة موزعة على (٢١) جهة تمثلت بـ (14) وزارة و(7) جهات غير مرتبطة بوزارة.

7. نظام إدارة الوثائق الوطني

نظام إلكتروني مركزي لتداول البريد بين الوزارات كافة، حيث وصل عدد الوثائق المتداولة منذ إطلاق النظام حتى الان (161.051) وثيقة، حيث يؤمن سرعة في تبادل البريد بين الوزارات مما ينعكس ايجاباً على تسريع وتيرة إنجاز المعاملات الرسمية، ومعتمد في (٢٩) جهة توزعت على (٢٢) وزارة و(٧) جهات غير مرتبطة بوزارة[22].

جدول رقم (2): عدد الوثائق للمشروع الوطني لإدارة الوثائق لغاية 2023/6/2

8. منصة الاستعلام الذكي

منصة بحث في البيانات الحكومية المصدرة على شكل جداول وصفية باعتماد الذكاء الصناعي والشبكات العصبية في تصفية البيانات والتقصي السريع للوصول للبيانات المطلوبة من حيث التطابق أو التشابه أو الاحتواء الجزئي، تقدم كخدمة من دائرة مركز البيانات الوطني الى الجهات الحكوميّة والموطنين لتسهيل عميلة التكامل والبحث واستخلاص التقارير، ويعتبر تطبيق سلامات لمسحات كورونا أحد الأمثلة الأكثر نجاحاً لعمل هذه المنصة، حيث بلغ عدد النتائج المرفوعة لغاية الآن (٣،٢٩٥،٥٥٥) نتيجة، وعدد الرسائل النصية المرسلة للمواطنين (٥٢٢،٧٣٢) رسالة (وكما مبين في جدول رقم (3))، ومكنت المواطنين من الحصول على تقارير موثوقة لنتائج الفحص دون الحاجة الى مراجعة المراكز الصحية، كما تم إبلاغ المصابين بشكل آلي عبر الرسائل النصية القصيرة[23].

9. نظام التحقق من البطاقة الوطنية وإثبات الحياة

منصة الكترونية تعمل باستخدام الذكاء الاصطناعي يتم استخلاص ومطابقة بيانات البطاقة الوطنية واثبات حياة الافراد ويعد النظام البنية أساسية لاعتماد الرقم الوطني كأساس لتيسير انجاز المعاملات في كافة الدوائر الحكومة دون الحاجة لتكرار الطلب من المواطن أو إحضار الأوراق الثبوتية لتسريع انجاز المعاملات وتقليل الجهد والوقت والتكلفة[24].

10. نظام ادارة الوثائق الموحد (توثيق)

نظام استراتيجي موحد لتمكين المؤسسات الحكومية من إدارة الوثائق بشكلٍ كفوء وسلس وآمن استناداً الى الترتيب الهرمي للمؤسسة ووفقاً للصلاحيات الممنوحة لكل موظف أو مجموعة من الموظفين حسب الوصف الوظيفي، تم انجاز البناء البرمجي وإجراء الفحص الأمني له بجهود كوادرنا وإشراف من قبل مركز الخدمات الرقمية البريطاني (GDS) (وكما موضح في جدول رقم (4))[25].

11. نظام المواقع الحكومية

نظام إلكتروني الهدف منه عرض مواقع المؤسسات الحكومية مع وصف للخدمات التي تقدمها، إضافة الى بعض البيانات الاحصائية والصور التي تصفها، ليتسنى للمواطن الاستفادة من هذه البيانات في الوصول الى تلك المواقع عند المراجعة لإنجاز المعاملات، كما يمكن أن يتكامل مع خرائط كوكل مما يتيح للمواطن إمكانية رسم المسار للوصول الى الموقع سيراً أو من خلال وسيلة نقل، وكما مبين في جدول رقم (5)[26].

المطلب الثاني: حوكمة التحول الرقمي في العراق (التحديات، الفرص)

انتجت جائحة كورونا ضرورات وطنيّة الى توفير الخدمات عبر الانترنت للدول، بسبب القيود المفروضة نتيجة السياسات المتبعة من الحظر وإغلاق العديد من المؤسسات الخدمية الحكومية والخاصة، فقد دفع البلدان الى اللجوء الى الحلول الرقمية لتكون قادرة على العمل بفعالية مع عمليات الاغلاق الواسعة النطاق والوصل غير المتكافئ الى الانترنت، وأصبحت الفجوة الرقمية أكثر أهمية من أي وقت مضى، وقد أوضحت جائحة كورونا ضعف العراق في مجال الحكومة الالكترونية وضرورة الحاجة الى انتهاج سياسات جديدة (في فترة الجائحة) لحل المشاكل التي تفاقمت بعد الجائحة وكان على رأسها -التعليم- بكافة اشكاله.

وعند الرجوع الى أسباب تراجع العراق في مجال حوكمة التحول الرقمي، فيمكن البدء من الاحتلال الأمريكي للعراق وما تسببه هذا الاحتلال من تراجع أداء الدولة العراقية بكافة مستوياتها، ومن بعدها تغيير نظام الحكم الى النظام الحالي وما أتسم به المناخ الاجتماعي والسياسي في العراق بعدم الاستقرار، وبالإضافة الى الحروب المتعددة، أدت الى اضطرابات كبيرة سببها النزاعات الداخلية، وتسلل تنظيم داعش الإرهابي الى ثلثي المحافظات العراقية، وما أثقل كاهل الحكومة العراقية الاقتصادي وهروب الاستثمارات والشركات الأجنبية وعزوفها عن العراق، إذ واجه واضعوا السياسات مخاطر جيوسياسية عديدة، تمثلت بضعف الوضع المالي، واضطراب الاقتصاد، وضعف القطاع الخاص... إلخ، إذ يترافق كل ذلك مع انتشار الفساد والمحسوبيّة وضعف الخدمّات، ما أدى الى تراجع قدرة الحكومة في مجال مواكبة التطورات الإداريّة والخدميّة الحاصلة في العالم وعلى رأسها الحكومة الالكترونيّة الى حيّن تشكيل لجنة (22) سالفة الذكر، وعلى هذا الأساس سنحاول بيان أهم التحديات التي تواجه حوكمة التحول الرقمي في العراق وخصوصاً التحديات التي تواجه لجنة (22) لسنة 2020، واهم الفرص والمعطيات لتعزيز أدائها، وعلى النحو الآتي:

اولاً: الارادة والدعم السياسي

تعد القيادة السياسية الطريق لاعتماد السياسات والأجندات ذات الصلة بالحكومة الالكترونيّة وتنفيذها، ويكون تطبيق الحكومة الإلكترونيّة أولوية سياسيّة بين جميع القوى السياسيّة، ويجب الإعلان عن توفر الإرادة السياسيّة على أعلى مستوى ممكن من رئيس السلطة التنفيذيّة ومدها بالمشاريع القانونيّة من قبل البرلمان، ولكي يحدث ذلك الأثر المناسب من تحديد مسؤوليات التنسيق والتنفيذ، وكذلك تشجيع الشراكة بين القطاعين العام والخاص والتعاون مع المؤسسات الأكاديمية، ويجب أن تدرك الحكومة وقادتها أن الأجندة الرقمية ليست موضوعاً منفصلاً بل جزءاً من كل سياسة وخدمة فضلاً عن قدرتها على تغيير عقلية المسؤولين على جميع المستويات وإعادة هندسة الخدمات العامة الحالية والعمليات ذات الصلة، وضمان تنفيذ الاستراتيجيّات والتشريعات عبر إنشاء البينات المعنيّة وعلى القادة السياسيَّين مواصلة الاهتمام بقضية الحوكمة الإلكترونيّة والالتزام بتقليل الوقت والموازنة وحتى رأس المال السياسي، ومن الضروري أيضاً بناء القدرات الحكومة المفتوحة والحوكمة الإلكترونيّة باستمرار[27].

وعلى صعيد الإرادة السياسيّة فقد بذل العراق جهوداً للوصول إلى المستوى الأساسي من النضج، وفقاً لنتائج المقابلات التي أجارها الباحث مع الجهات المعنية فقد لاحظ أن هنالك دعماً سياسياً رفيع المستوى للسياسة العامة لتقديم وتطوير خدمات الكترونية وتكنولوجيات اتصال مختلفة ضمن المؤسسات الحكومية وفي التواصل مع المواطنين، ولكن بسبب عدم اعتماد وثائق سياسية أساسية على المستوى الحكومي، تتخذ معظم القرارات التنموية لكل حالة على حدة، ويوضع جدول الأعمال ويتم التخطيط في الغالب بشكل منفصل على مستوى كل مؤسسة.

1. التحديات

أن الجهة العامة الرئيسية المخولة بموضوع الحوكمة الإلكترونية عموماً في لجنة تنسيق وإدارة النشاط الحكومي باتجاه الحوكمة الإلكترونية (لجنة 22)، ولاحظ الباحث من خلال المقابلات التي أجراها مع رئيس وأعضاء اللجنة، أنه يسبب ضعفاً وجود سياسات أساسية وآليات مدعومة بتشريع قانوني لتنفيذ الحكومة الإلكترونيّة، يجري تحديد أولويات الخدمات والأنظمة التي يجب تطويرها وفقا للاحتياجات المؤسسيّة، وهناك بعض الأولويات العامة تعامل بوصفها أولويات في جميع المواضيع ومنها زيادة تكامل خدمات البطاقة الوطنيّة وتوسيع استخدامها، وتوفير مرافق أمنة وسيلة الوصول لتبادل البيانات وتخزينها، وكذلك تطوير مركز البيانات الوطني[28].

2. الفرص

بُغية تعزيز الإرادة السياسية ودفعها باتجاه استكمال مشروع الحكومة الالكترونية، فمن الضروري وضع واعتماد استراتيجيّة أساسيّة للحوكمة الإلكترونية على المستوى السياسي لفترة أطول وينبغي أن تتضمن الإستراتيجية إطاراً مفصلاً للتمويل والتنفيذ بالإضافة إلى رؤية لضمان البنية التحتيّة الأساسية لجميع المؤسسات الحكومية بالإضافة إلى ذلك فمن الضروري للسنوات المقبلة ضمان وجود مؤسسة تخطيط مركزيّة مخصصة، وتشجيع التعاون بين المؤسسات الحكوميّة، ويمكن الحصول على أفضل النتائج من نهج متعدد القطاعات عبر تعزيز التعاون مع الجهات المعنية مثل الأوساط الأكاديمية ومنظمات المجتمع المدني والقطاع الخاص خارج القطاع الحكومي، وفي نطاق يجب أن تكون استراتيجية الحوكمة الإلكترونيّة مصحوبة بخطةِ اتصالٍ استراتيجية للحوكمة الرقمية والخدمات الإلكترونيّة الجديدة، علاوةً على ذلك يجب على

كل وزارة صياغة استراتيجيتها الخاصة للتحول الرقمي وضع صبغة تعاون بين القطاعات وأن يشمل في نظام تعاون فعال مشاركة من قطاع الأعمال والأكاديميين والمجتمع المدني وكذلك مع السلطات الحكومية المحلية وأن يكون مستمراً بطبيعتهِ.

ثانيا: الدعم مالي

يتعين على الحكومات تطوير نماذج تمويل للخدمات الالكترونية لضمان استدامتها، إذ أن من الضروري التخطيط لتكلفة الملكية الكلية لأي حلولٍ رقمية للحكومة، بما في ذلك الخدمات الإلكترونية، ورغم أن إدخال الحكومة الالكترونيّة سيؤدي في النهاية الى توفير المزيد من الأموال وتقلل من التكاليف المرصودة للنظم التقليدية في تأدية الخدمات الحكومية؛ إلا أنها تؤدي الى تكلفة في بداية تأسيسها، على ذلك من الضروري توفير التمويل الكافي بطريقةٍ مستدامة على المدى المتوسط الى الطويل، ويفضل ذلك من خلال التخطيط المالي على المدى المتعدد السنوات[29].

1. التحديات

تمثلت أبرز التحديات التي تواجه حوكمة التحول الرقمي في قلة التخصيصات المالية المرصودة للمشاريع الرقمية وعلى رأسها المشاريع المقدمة من قبل (لجنة 22)، ولأسباب متعددة جرى ذكرها في الصفحات السابقة، فضلاً عن أن ضعف التخصيص مرتبط بالضعف الكبير بالبنى التحتية الرقمية سواءً على مستوى التطبيقات أو الأجهزة[30].

2. الفرص

تتمثل فرص تعزيز حوكمة التحول الرقمي في المجال الدعم المالي والفني بالآتي:

أ. ضمان الاتساق في التمويل العام لتكنولوجيا المعلومات، وينبغي أن تستند جميع قرارات التمويل الى استراتيجيات تخطيط وتنفيذ طويلة المدى، وأن تصل موازنة التحول الرقمي للمؤسسة الى 1% على الأقل من الموازنة الاجمالية لتقديم الحد الأدنى من الأموال من أجل تنمية قطاع الحكومة الالكترونية.

ب. ضمان الشفافية في عملية إعداد الموازنات في المؤسسات الحكومية ومن ضمنها موازنة تكنولوجيا المعلومات والاتصالات، حيث يوصى باستخدام الوسائل الالكترونية في عملية إعداد الموازنة، وأن يستند التخطيط المستدام للاستثمارات وتكاليف الصيانة الى مراجعة شاملة لاحتياجات البرامج والأجهزة للمؤسسات

العامة، ما يسمح برقابة أفضل ورصد التنفيذ الفعال، وتشمل شفافية الإعداد توحيد الإجراءات والتعاون ومشاركة الجهات المختصة، فضلاً عن اعتماد العملية على خطط التنمية السياسية والتكنولوجية القائمة.

ج. ضمان الوضوح والشفافية في هيكل موازنة تكنولوجيا المعلومات والاتصالات في كل مؤسسة، ويتم تعزيز ثقة المواطنين في المؤسسات عبر عمليات شفافة والمساءلة في عملية وضع الموازنة، التي بدورها تسمح بتنمية القطاع الرقمي وتحسين خدماته.

ثالثا: الإطار القانوني

لا توجد شروط قانونية لبدء عملية تطبيق الحوكمة الالكترونية؛ لكن يوجد قوانين عدة تحتاج الى مراجعة وهذه المراجعة يجب أن تجري في المراحل الأولى من تطوير الحوكمة الالكترونية، وينبغي ألا يكون هناك كثير من التشريعات المتخصصة بشأن الحوكمة الالكترونية، بل يجب دمج الآثار القانونية للتكنولوجيات المستخدمة في التشريع في مجموعة القوانين المتناثرة كلها، وقد تتطلب التغييرات الرئيسية في عمل المؤسسات الحكومية بشكل عام والخدمية بشكل خاص الى تغييرات رئيسيّة تتطلب تشريعات جديدة أو معدلة، وغالباً ما تدور قضية التحديث القانونية في قضايا التوقيع الالكتروني وحماية البيانات وقبول المعلومات الالكترونية... وغيرها[31].

1. التحديات

تبين للباحث عن طريق المقابلات التي أجراها مع رئيس وأعضاء لجنة (22)، بأن البرلمان العراقي لم ينته من مناقشاته التشريعية بشأن تبني قوانين لقبول وتطبيق واسع النطاق لمبادئ الحوكمة الإلكترونية، وتوجد بعض اللوائح التي تسمح ببعض عناصر الإدارة الإلكترونية، وعلى سبيل المثال في العام ٢٠١٢ اعتمد قانون المعاملات الإلكترونية العراقي لتوفير الأساس والإطار القانوني للمعاملات الإلكترونية والتوقيع الإلكتروني عبر وسائل اتصال حديثة، ولتشجيع قطاع الإنترنت كما يسمح القانون بالتحويل الإلكتروني للأموال وينظم مقبولية السجلات الإلكترونية ووزنها الإثباتي، بيد أن العراق ما يزال يفتقر إلى إطار مؤسسي (كهيئة إصدار شهادات) وبنية تحتية لتطبيق الإمكانيات المنصوص عليها في القانون[32].

ونوقش مشروع التشريع الخاص بقطاع الاتصالات على مدار سنوات ما أدى إلى إصدار ورقة خضراء بشأن مشروع قانون الاتصالات العراقي في عام ٢٠١٨ لكن التشريع لم يعتمد بعد، كما أن مشروع قانون الجرائم الإلكترونية قيد الإعداد منذ أكثر من عقد - فشل إقرار مشروع القانون الأول مرة في عام ٢٠١١[33]، وأعيد تقديمه إلى البرلمان في عام ٢٠١٩، بيد أنه طرح لاحقاً في عام ٢٠٢٠ بسبب ضغوط من المجتمع المدني ومنظمات حقوق الإنسان، حيث كان يخشى أن يعاقب مشروع القانون المعارضين في المجتمع المدني وأن يكون له أثر سلبي على حرية التعبير[34].

وقد يمكن القول بأنه لا توجد قوانين واضحة المقاصد في العراق تحكم قضايا حماية البيانات الرقمية في العراق، بل تستخدم تشريعات مختلفة من بينها قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩، والقانون المدني العراقي، وقوانين قطاعية أخرى (قوانين العمل، قوانين المصارف. إلخ) [35].

2. الفرص

تتمثل فرص تعزيز حوكمة التحول الرقمي في المجال الدعم القانوني بالآتي:

أ. تشكيل فريق قانوني أو تعزيز الفريق القانوني المتخصص للجنة (22) وإعادة النظر بكادر الفريق ورفدهم بالمتخصصين القانونيين عبر وضع معايير محددة لاختيار أعضاء الفريق، ويتم تشجيع التعاون مع الاستشاريين الدوليين والمحليين واعتماد أفضل الممارسات من البلدان الأخرى وعلى رأسها دولتي استونيا والامارات العربية المتحدة.

ب. ينبغي إجراء تحليل قانوني منهجي للركائز القانونية الأساسية للحوكمة الالكترونية، وتنظيم هذا التحول قبل الشروع في عملية تكوين الاستراتيجية طويلة المدى (المزمع كتابتها)، وسيوفر التحليل فهما للإجراءات القانونية الأساسية أو التعديلات اللازمة في اللوائح الحالية الضرورية للمضي قدمًا في أي خطط للحوكمة الالكترونية.

ج. مواصلة العمل على اعتماد التعديلات القانونية المعلقة بشكل أكثر نشاطاً ومن دون مزيدٍ من التأخير، ويشمل ذلك اعتماد قوانين لحماية البيانات الشخصية، والحق في الحصول على المعلومات والاتصالات، وإدخال التعديلات اللازمة على القوانين، بناءً على مشاورات مع مجموعة واسعة من الجهات المعنية ويمكن الاستفادة من الخبرات الاستونية والاماراتية إذا لزم الأمر.

رابعا: الهوية الرقمية

بُغية تعزيز أداء الحوكمة الرقمية في أي بلد من الضروري أن يتمكن المستخدمون من تعريف أنفسهم بطريقة آمنة، وهذا يتطلب تطوير مفهوم الهوية الرقمية وأدواتها، ويمكن أن يتضمن ذلك معرفًا رقميًا أو معرفًا للجوال مع توقيع رقمي، ويجب أن تكون التوقيعات آمنة بما يكفي للإعتراف بها كدليل في المحكمة أو في حالات مماثلة[36].

1. التحديات

من العوائق الرئيسية للتحول الرقمي وتطوير الخدمات الإلكترونية في العراق عدم وجود سجل هوية وطني موحد يمنح الحكومة فهماً واضحاً لسكان البلاد ويسمح بتحديد جميع العملاء باستخدام الخدمات العامة، وتوجد قاعدة بيانات الأشخاص الأكثر اكتمالاً في وزارة التجارة، حيث تستخدم للتمييز بين المستفيدين لغرض التقنين الغذائي الشهري، بيد أن قاعدة البيانات هذه لا تتعامل مع أفراد بل مع أُسر أي هناك بطاقة هوية واحدة لرب الأسرة وبقية أفراد الأسرة مدرجون على البطاقة نفسها، ولهذه البطاقة فقط رقم مميز لكن لا يوجد رقم مميز للأفراد، ويصدر رقم تعريف وطني مميز دائم مكون من ١٢ رقماً للمواطنين على البطاقة الوطنية الموحدة المستخدمة منذ عام ٢٠١٦، وتشتمل البطاقة على شريحة RFID والهدف هو إصدار بطاقة موحدة لكل مواطن عراقي، ولكن في الواقع، تم إصدار بطاقات موحدة لقرابة (34.428.757) مواطن[37] من أصل (43) مليون[38].

الوسيلة الرئيسية لتحديد الهوية عن بعد حالياً هي تركيبة اسم المستخدم / كلمة المرور وفي بعض المجالات المتخصصة (في المعاملات المالية أو الخدمات العسكرية مثلاً) تستخدم المؤشرات الحيوية (بصمات الأصابع أو العين أو غيرها) للتحقق من الهوية. لا يوجد حل تكنولوجي مباشر متاح للهوية الرقمية عن بعد، حيث لا يمكن لهذا الغرض استخدام شريحة RFID بسهولة بسبب ارتفاع تكاليف التحقق[39].

2. الفرص

تتمثل فرص تعزيز حوكمة التحول الرقمي في مجال الهوية الرقمية بالآتي:

أ. تشجيع نشر بطاقة الهوية الوطنية لتعزيز إدارة بيانات السكان، وينبغي أن تصبح بطاقة الهوية الوطنية هي الخدمات الحكومية الأساسية لهيكل تحديد الهوية، ما يوفر إمكانية

التحقق الموثوقة من الأشخاص، وبعد زيادة نسبة في عدد مستخدمي الهوية يمكن دراسة احتمالات أخرى لتقديم خدمات بناءً على رمز الهوية الرقمية ونشر التوقيعات الرقمية.

ب. دمج إدارة الهوية الوطنية ضمن إدارة بيانات السكان العامة، ويفضل تخصيص معرف مميز منذ الولادة وربطه لاحقاً بالهوية الوطنية، ما يسمح الاستخدام مدى الحياة.

ج. توسيع نطاق التعاون مع القطاع الخاص لجعل استخدام الهوية الوطنية أكثر ربحاً، وينبغي للحكومة تشجيع التعاون مع المصارف ومقدمي خدمات الاتصالات السلكية واللاسلكية وغيرها للحصول على حوافز إضافية لتحديد حالات استخدام الهوية الرقمية وتحديد الهوية عن بعد.

د. ضرورة طلب الاستشارة والتعاون من الجانب الاستوني في عملية تعزيز وتطوير الهوية الوطنية الرقمية وفتح مسارات وافاق جديدة لاستخداماتها في كافة الخدمات الحكومية.

خامسا: المهارات الرقمية

يتطلب التطور السريع للتكنولوجيات الرقمية من الموظفين الحكوميين والمواطنين اكتساب المهارات اللازمة لاستخدام الأدوات الجديدة والتمتع بإمكانات المجتمع الرقمي، وتزويد جميع المواطنين والموظفين الحكوميين بالمهارات اللازمة، اذ تحتاج السلطات الى متخصصين ذوي مهارات متقدمة في تكنولوجيا المعلومات والاتصالات وإدارة المشاريع للحفاظ على هيكلية تكنولوجيا المعلومات والاتصالات ودعم المستخدمين وإدارة مشترياتها وتنفيذ الاستراتيجية الرقمية للحكومة(40).

1. التحديات

على الرغم من أن نظام التعليم يخرج أكثر من **250,000** خريج سنويًا في جميع مستويات التعليم، فان هناك فجوة من ناحية عدم ملاءمة المهارات لأن الشباب لا يكتسبون دائماً المهارات المناسبة للوظائف المطلوبة، بما فيها المهارات الرقمية، حيث تعد المناهج الدراسة غير قادرة على تلبية متطلبات الاقتصاد الرقمي والمجتمع الرقمي، وهذا ايضاً سبب من أسباب تقدير أصحاب العمل للمؤهلات الرسمية(41).

وهنالك ضعف في النضج في مجال تكنولوجيا المعلومات عند الملاكات التخصصية في الوزارات، وهناك ما يقارب (4000) موظف مختص في التكنولوجيا، و(2780) منهم يحتاج الى تأهيل وزجهم في دورات تخصصية عالية المستوى ليتمكنوا من تنفيذ المشاريع

الرقمية للجنة (22) في وزاراتهم، وفي مقابل ذلك تلبي المهارات الرقمية للموظفين الحكوميين ما هو ضروري لأداء واجباتهم[42]، ونظراً لارتباطات المهارات التكنولوجية بالبنى التحتية التكنولوجية فإن العراق يعاني من ضعف في البنية التحتية مما يعوق استخدام التكنولوجيا بشكل فعال ويقيد إمكاناتها.

ومن جهة أخرى لا يزال التعليم العالي بالعراق يعاني من رتابة التخصصات والبطء في تحديث مسمياتها وخصوصًا تلك التي تتعلق بتكنولوجيا المعلومات والاتصالات بكل فروعها وتخصصاتها وأهمها الأمن السيبراني والذكاء الاصطناعي وعلوم البينات والحكومة ومعاييرها على الرغم من بعض المحاولات في السنتين الأخيرة التي شهدت افتتاح أقسام هندسية وعلمية في مختلف الجامعات الحكومية والأهلية ومناقشة أطاريح ورسائل تناقش وتهتم بهذه المواضيع المهمة.

2. الفرص

تتمثل فرص تعزيز حوكمة التحول الرقمي في مجال المهارات الرقمية بالآتي:

أ. رفع مستوى المهارات الرقمية لموظفي القطاع العام: ينبغي اجراء تقييم للقدرات الحالية للموظفين العموميين وتحديد احتياجات التدريب بناءً على النتائج، وتحديد خطة التعلم وينبغي تنظيم دورات تدريبية للموظفين الحكوميين تتضمن عناصر تكمل مهاراتهم المعلوماتية والرقمية وتزيد فهمهم للصحة الالكترونية، فتحقيق زيادة شاملة في المهارات الرقمية لموظفي الخدمة المدنية يساعد في تعزيز المستوى الأساسي للفهم الضروري لتنفيذ تدابير الحوكمة الالكترونية في العراق، وينبغي التركيز بشكلٍ خاص على الإدارة العليا والوسطى لضمان امتلاكهم فهماً قوياً للعناصر والمزايا الأساسية للحكومة الالكترونية.

ب. تعزيز التعليم التكنولوجي والاستثمار في البحث والتطوير، اذ ينبغي على الحكومة العراقية توفير الدعم المالي والتسهيلات للمؤسسات البحثية والتقنية لتطوير حلول تكنولوجية مبتكرة وتعزيز التطوير التكنولوجي في البلاد، فضلاً عن ضرورة التركيز على تعزيز برامج التعليم التكنولوجي في المدارس والجامعات وتوفير البنية التحتية اللازمة والموارد التعليمية المناسبة، وهذا يتم عن طريق التعاون مع وزارة التعليم العالي ومراكز التعليم المستمر في الجامعات العراقية لتنظيم دورات الزامية للموظفين العموميين في الاستخدام الأمثل لتكنولوجيا المعلومات والاتصالات وحماية المعلومات الشخصية في بيئة الانترنت، ويمكن

اعداد مناهج الدورات مع استشاريين دوليين والاستفادة من التجربة الاستونية والاماراتية في هذا المجال.

ج. رفع مستوى المهارات الرقمية للمواطنين: عبر مراجعة مناهج المدارس الابتدائية والمتوسطة والثانوية من قبل وزارة التربية، وتضمين مناهج جديدة تمكن الطلاب من الاستخدام الأمثل لتكنولوجيا المعلومات والاتصالات وحماية البيانات الشخصية في بيئة الانترنت، ويمكن اشراك خبراء دوليين لتحقيق هذا الغرض عبر التعاون مع دولتي استونيا والامارات العربية المتحدة نظراً لما تمتلكه من نجاحات واسعة في هذا المجال، فضلاً عن ذلك فمن الضروري الاستثمار في البنى التحتية للتكنولوجيا، اذ يمكن للحكومة العراقية والمؤسسات الخاصة التعاون لتطوير البنية التحتية التكنولوجية وتحسينها بما في ذلك توفير شبكات اتصال سريعة وموثوقة وتطوير مراكز بيانات متقدمة.

ومن خلال ما تقدم يمكن القول إن تحول الحكومة العراقية نحو مشروع تطبيق الحكومة الالكترونية ليس طريقًا إلى الرفاهية بل إنه واقع تفرضه التغيرات العالمية على الدول في العالم المتقدم أو الدول النامية، كما أن التقدم التكنولوجي للاتصالات والمعلومات الحديثة والمطالبة المتزايدة للمجتمع العراقي برفع جودة عمل المؤسسات الحكومية في العراق، كل هذه الامور قد فرضت على العراق التحول نحو تطبيق الحكومة الالكترونية وتطوير العمل الاداري للمؤسسات الحكومية ، كما يعد عامل الوقت من الادوات الرئيسية للتنافس بين المؤسسات الحكومية، حيث لم يعد هنالك مبرر لتأخير تنفيذ العمليات داخل المؤسسات الحكومية بسبب تطورها ولتوفر الفرص أمام المؤسسات الحكومية لتقديمها للخدمات وعدم تأخرها، لذلك فإنَّ عملية تطبيق الحكومة الالكترونية في المؤسسات الحكومية وخاصة من ناحية تأديتها للوظائف العامة يتطلب منها التخلي عن منهج العمل التقليدي الجامد والتحول إلى ما أصبح يعرف بالحكومة الالكترونية الذي يعتمد على الابتكار، والتخطيط الاستراتيجي ، ونظم المعلومات وتقنيات الاتصال الحديثة من جهة، وذات علاقة مباشرة بالقوى البشرية، فضلاً عن ذلك ضرورة تأمين الحكومة الالكترونية العراقية في الفضاء السيبراني، وهذا ما سنتناول واقعه وتحدياته في المبحث القادم.

المبحث الثاني: الامن السيبراني العراقي (الواقع، التحديات، الفرص)

واجه العراق تحديات كبيرة في مجال الفضاء السيبراني، فابتداءً من العزلة الدولية التي مر بها قبل عام (2003)، والعزلة المحلية عن العالم الخارجي التي فرضها النظام السابق، ومروراً بالأزمات التي تلت هذا العام من عدم الاستقرار على كافة المستويات، جعلته في حالة ضعيفة وغير قادر على امتلاك القدرات المطلوبة للتكيف مع تلك التحديات التي يفرضها واقع الفضاء السيبراني أو الاستعداد للانتقال من الفضاء الحقيقي إلى الفضاء الافتراضي، لذا وجد العراق نفسه أمام هذا الفضاء الواسع وسريع الحركة دون أن يمر بمراحل انتقالية، فالبنى المادية والبشرية في العراق ماتزال غير قادرة على التفاعل أو حتى المواكبة، مع تلك التحديات العديدة للفضاء السيبراني، وبالرغم من اقدام العراق على تبني سياسيات ومشاريع رقمية تهدف باتجاه التحول نحو حوكمة التحول الرقمي ضمن مشاريع السياسات العامة العراقية لمجلس الوزراء العراقي، إلا ان العراق يواجه تحدٍ استراتيجي وأمني بالغ الخطورة يضمن أمن وسلامة البيانات الرقمية العراقية ضمن منظومة أمن سيبراني متكاملة ومحصنة ضد الهجمات السيبرانية سالفة الذكر في الفصل النظري من هذه الدراسة، وعلى هذا الأساس يعالج هذا المبحث نشأة وامكانيات الأمن السيبراني في العراق وأهم التحديات والفرص التي تعزز هذا القطاع الأمني الهام، وعلى وفق المطالب الآتية:

المطلب الأول: الأمن السيبراني العراقي (البادرة التاريخية، أبرز الجرائم، الإمكانات)

يعد الفضاء السيبراني أحد أخطر التحديات الاقتصادية والأمنية الوطنية، فبعد أن تزايد الاعتماد على خدمات الإنترنت، تولدت ضرورة الحاجة إلى مركز الأمن السيبراني الوطني في العراق لتعزيز الوضع الأمني وحماية البنى التحتية وتتبع ومحاربة المجرمين والإرهابيين في البلاد وتعزيز حماية البيانات الرقمية ونظام المعلومات للمنظمات العامة والخاصة.

أولاً: البادرة التاريخية للأمن السيبراني واستراتيجيته في العراق

إن الفضاء السيبراني لا يختص حصراً بخدمات الانترنت وتكنولوجيا الاتصالات والمعلومات فحسب، وإنما يدخل في عدة مجالات أخرى مختلفة مثل البنى التحتية والخدمات الحكومية والمجتمعية، ولكن بمميزات وخصائص وتحديات مختلفة، تميز مفاهيم هذا الفضاء بالتعامل مع البيانات والمعلومات بحفضها وتعديلها وتبادلها من خلال أنظمة شبكيّة خاصة تحكمها ويديرها الأمن السيبراني، حيث أصبح الأمن السيبراني مفهومًا يمتلك ابعاداً وطنيّة

ودوليّة، حيث أن الامن السيبراني يتجسد ويؤثر في كل مفاصل الدولة الأمنيّة والاقتصّادية والاجتماعيّة ولكن بصيغة الكترونيّة، وبالرغم من المزايا التي يقدمها التقدم التكنولوجي عن طريق الخدمات الرقمية إلا أنه يمكن أن يشكل تهديدًا كبيرًا ويسبب أضرارًا واسعة على الأمن الوطني والتنمية الاقتصادية والبنى التحتية الحرجة، هذه التهديدات بدأت تتصاعد في الآونة الأخيرة وتصبح عابرة للحدود الوطنية، مما يجعل مواجهتها تحديًا كبيرًا ومعقدًا لجميع الدول، ونظرًا لحداثة التجربة ولوجود التهديدات والمخاطر التي يمكن أن تظهر في هذا العالم فلابد من بناء الأسس الصحيحة لإطار أمني متكامل يوفر الحماية الكافية لقطاع الاتصالات وتكنولوجيا المعلومات ويعزز دوره في تحقيق الأهداف التنموية العراقيّة، واستجابة العديد من لهذا الإدراك[43].

وبناءً على هذا السياق تم وضع الأمن السيبراني ضمن الأهداف المركزية للدولة العراقية ومر الأمن السيبراني العراقي بمراحل متعددة وكما يلي:

1. تم اصدار الأمر الديواني ذي العدد (5 س) في العام 2011 لتشكيل اللجنة الفنية العليا لأمن الاتصالات.
2. أقر مجلس الأمن الوطني في جلسته (23) لسنة 2015 إعادة تشكيل اللجنة الفنية العليا لأمن المعلومات والاتصالات بمهام أوسع وأنهى عمل لجان موازية لغرض توحيد الجهود الوطنية من أجلِ تنفيذ السياسّة والإستراتيجيّة الوطنية وتحقيق أمن الاتصالات والمعلومات (الأمن السيبراني) وتم اصدار الأمر الديواني ذي العدد (504) لسنة 2015 الذي حدد مهام وعمل اللجنة.
3. أشارت استراتيجيّة الأمن الوطني المقرة الى استحداث مؤسسة تتولى إعداد وتنفيذ سياسّة واستراتيجيّة وطنيّة لتحقيق الأمن السيبراني في الفقرة (6.3) في الفصل الثالث.
4. أقر مجلس الأمن الوطني في جلسته (3) لسنة 2017 تشكيل الفريق الوطني الدائم للاستجابة لحوادث الحاسبة لمواجه التهديدات السيبرانية على المستوى الوطني والتقليل من آثار الخروقات الأمنية الالكترونية وتنسيق الجهود الوطنية في هذا المجال وتحقيق مؤشرات السلامة السيبرانية حسب معايير الأمم المتحدة، وتم إصدار الأمر الديواني (66 س) لسنة 2017 لهذا الغرض وتم تكليف اللجنة الفنية العليا بكّابة استراتيجية الأمن السيبراني في نفس الجلسة.

5. وافق مجلس الأمن الوطني في جلسته (13) لسنة 2017 على إنشاء تشكيل مختص مستقبلًا يعنى بالأمن السيبراني وبما ينسجم مع أهداف الاستراتيجيّة الوطنيّة للأمن السيبراني على أن تنجز المهمة خلال ستين يومًا.
6. قرر مجلس الوزراء في جلسته الاعتيادية التاسعة والعشرين إقرار وثيقة السياسات والمعايير لأمن المعلومات ومشاركة البيانات التي أقرها مجلس الأمن الوطني في الجلسة رقم (19) لسنة 2020 وتتضمن الوثيقة الأدوار والمسؤوليات والمهام الوطنية وتؤكد على دور التشكيل المشار إليه أنفًا في إدارة هذا القطاع.
7. أقر مجلس الأمن الوطني في الجلسة رقم (1) لسنة 2022 إستراتيجية الأمن السيبراني دون استكمال تشكيل الكيان الوطني المختص بتنفيذ الاستراتيجيّة وإدارة هذا القطاع.

وتعمل استراتيجيّة الأمن السيبراني على توفير خارطة طريق متماسكة وبحوث علمية وآليات عمل لتنفيذ وتحقيق الرؤية الوطنية بشأن الأمن السيبراني، ويتم ذلك من خلال تحقيق مجموعة أهداف تتمثل بالآتي[44]:

1. حوكمة الأمن السيبراني الوطني.
2. رصد التهديدات ورسم المعالجات الاستراتيجية والتكتيكية والاستجابة الطارئة.
3. إعداد الخطط الإستراتيجية ضمن محاور العمل، وبناء وانشاء مراكز خدمات الحكومة الالكترونية ضمن مواصفات ومعايير أمن سيبرانية رصينة.
4. بناء القدرات وتهيئة الكوادر المتخصصة بالإضافة إلى زيادة مستوى الوعي بمجال الأمن السيبراني للعاملين.
5. التوعية الاجتماعية للأسرة والطفل وأصحاب الهمم كافة وبمختلف الفئات العمرية للتعامل مع الخدمات الرقمية المختلفة وتثقيفهم على التعامل مع المخاطر السيبرانية التي من المحتمل أن تستهدفهم وكيفية حماية معلوماتهم الشخصية في الفضاء السيبراني.
6. تنشيط الدور الأكاديمي وتوفير المراكز الخاصة بالبحث والتطوير لتشجيع الابتكارات والصناعات المرتبطة بالأمن السيبراني.
7. تفعيل التعاون الاستراتيجيّ على المستوى المحلي مع القطاعات الحكوميّة والخاصّة.
8. فحص وتدقيق الأجهزة والبرامج الإلكترونية المنتجة والمستوردة والمعروضة في السوق لمطابقة معايير سلامة الأمن السيبراني.

9. تفعيل التعاون على المستوى الوطني والإقليمي والدولي.

إن نطاق تطبيق هذهِ الإستراتيجية يستهدف مؤسسات القطاع العام والخاص ويشمل كذلك المجتمع العراقي بصورة عامة والفرد العراقي بصورة خاصة ويكون صلاحية تنفيذها من قبل الكيان الوطني للأمن السيبراني الذي سيتم تشكيله بواسطة الجهات الأمنية ذات العلاقة للمدة الزمنيّة الممتدة بين الأعوام 2022-2025 ضمن الخطة المعدة لتغطية متطلبات رفع مستوى الأداء وتذليل التحديات وتقليل المخاطر المتعلقة بالأمن السيبراني على المستوى الوطني والإقليمي والدولي، ومن الجدير بالذكر أن هذه الإستراتيجية سوف يتم مراجعتها وتحديثها وتطويرها وفقا للمستجدات في مجال الأمن السيبراني بالاعتماد على مؤشرات التقييم والمراقبة والتحديات أثناء تطبيق المبادرات والبرامج، ومقترحات الخبراء الوطنين والدوليين بشكل يحافظ على أهدافها ويحقق غاياتها بالاستعانة بأفضل الممارسات والآليات والمعايير، ويتم ذلك من خلال استحداث كيان وطني مستقل يكون مسؤولا عن وضع خطة العمل وتوزيع الأدوار لكافة المؤسسات الحكومية والأهلية ومتابعة تنفيذها وتقديم نسب الإنجاز لتحقيق المشاريع المذكورة في هذه الاستراتيجية وبالتنسيق مع فرق الاستجابة الفرعية في المؤسسات انفا[45].

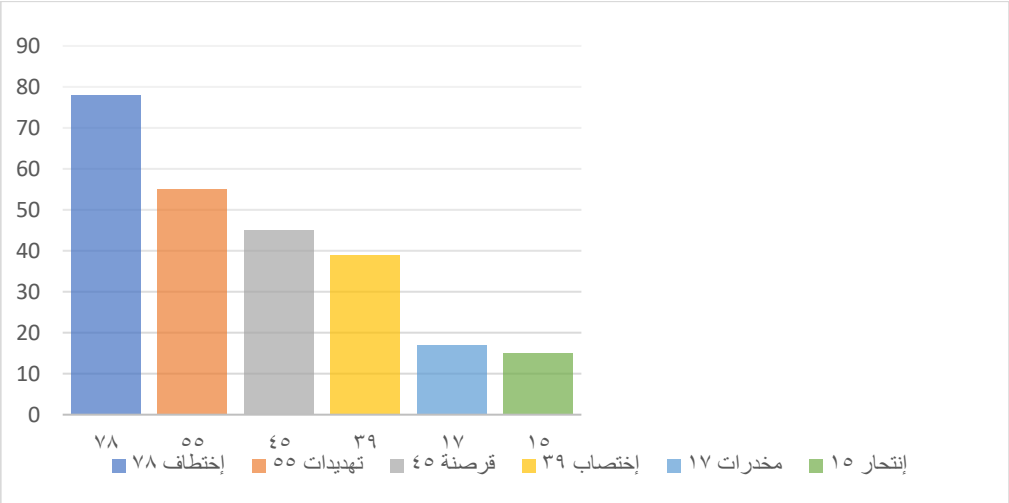
ثانيا: الجرائم السيبرانيّة في العراق

يعد قطاع الإنترنت العراقي من القطاعات غير المنظمة والضعيفة حالياً، مما يجعله من بين الأكثر حرية على مستوى العالم، بسبب عدم الاستقرار السياسي والأمني الحالي في العراق، لذا وفي ظل التسابق الدولي في هذا المجال والتسارع نحو استغلاله في كافة المجالات، فإن العراق بحاجة إلى مزيد من العمل لتطوير الأساسيات القانونيّة والتقنيّة والتنظيميّة وبناء القدرات لتوفير الأمن السيبراني الشامل لمواطنيها والشركات ومؤسسات الدولة، ولعدم وجود اهتمام يتناسب وأهمية هذا المجال، مع عدم وجود هيئة أو مركز وطني رئيسي يختص بهذا المجال، لوحظ أن البيانات في العراق شحيحة وغير دقيقة ونادراً ما يتم نشرها من قبل الحكومة العراقية التي قد تمثل بوزارة التخطيط أو جهاز الأمن الوطني، ومع ذلك، كشفت التقارير السابقة التي أصدرتها الحكومة العراقية أن أكثر الجرائم السيبرانية شيوعاً في العراق هي ضد الأشخاص بدلاً من أن تكون ضد الشركات أو الحكومات[46].

هناك العديد من الجرائم السيبرانية المتنوعة في العراق، مثل الاحتيال عبر الإنترنت، وسرقة الهوية، والصور الإباحية، والمطاردة السيبرانية، وانتهاك حقوق النشر، والوصول غير المصرح به، والبرامج الضارة والإرهاب السيبراني، فمن خلال سجلات مكتب التحقيقات الجنائية العراقي للسنوات (2006-2011)، تبين أن هناك ازدياداً كبيراً في حالات الجرائم السيبرانية بمتوسط نسبة سنوية تبلغ (46.2%) من مجموع الجرائم المرتكبة عبر وسائل الاتصالات، حيث تم تصنيف أعلى النسب في حالات الجرائم السيبرانية بحسب السنوات أعلاه كالآتي: جريمة غسيل الأموال في عام (2006)، القرصنة السيبرانية في عام (2007)، الجرائم الجنسّية في عامي (2008-2009)، السرقة في عام (2010)، والغش بأنواعه عبر الإنترنت (الاجتماعي التجاري أو العلمي) في عام (2011)[47].

وتسبب هذا الحادث في إرباك الناس وقلقهم من هشاشة الأمن السيبراني في العراق، حيث ينبغي أن تمتع الحكومة بالأمن السيبراني الكافي لمواجهة التجسس السيبراني والإرهاب السيبراني والحرب السيبرانية، ولا يتم تحقيق هذه الإمكانية إلا من خلال إنشاء مركز للأمن السيبراني يحتوي على عدد من المتخصصين في أمن الكمبيوتر والشبكات، والمتخصصين في تشريعات الإنترنت، وفي عام (2013)، وضح تقرير وزارة التخطيط في العراق أن منصة (Facebook)، كان الجزء الرئيسي الذي تم من خلاله ارتكاب قضايا الجرائم السيبرانية، وهناك بعض الحالات التي تم ارتكابها من خلال بعض المواقع الاجتماعية الأخرى مثل، تويتر (Twitter) وزوو (Zoo) وبادو (Badoo)، أما حالات الجرائم التي سجلت للعام (2013)، باستخدام الفيسبوك هي: (78) حالة اختطاف، (55) حالة تهديد، (45) حالة اختراق معلومات شخصية مثل الصور وملفات تعريف مرسلة ومزيفة، (39) حالة اغتصاب، (17) حالة مخدرات و (15) حالة انتحار محتملة[48]، وكما موضح في الشكل ادناه، والجدول رقم (1)

شكل رقم (1): حالات الجرائم السيبرانية باستخدام برنامج الفيسبوك لعام 2013



Source: Sattar J. Aboud، Cybercrime in Iraq، International Journal of Scientific & Engineering Research، Volume 5، No. 3، March- 2014، pp 422-425.

وتعرض موقع "مستشارية الامن الوطني" للاختراق الالكتروني، إذ نشر المخترقون صورة "كاريكاتورية" لمستشار الأمن الوطني السابق "فالح الفياض"، مع كتابة عبارة في الموقع: "أن موقعكم لم تقوموا بحمايته فكيف تحافظون على أمن الشعب"، ويقدم الجدول الآتي الوزارات العراقية التي اختراقها[49].

جدول رقم (1): اختراق المواقع الالكترونية لوزارات عراقية بين عام 2016 ومطلع العام 2017

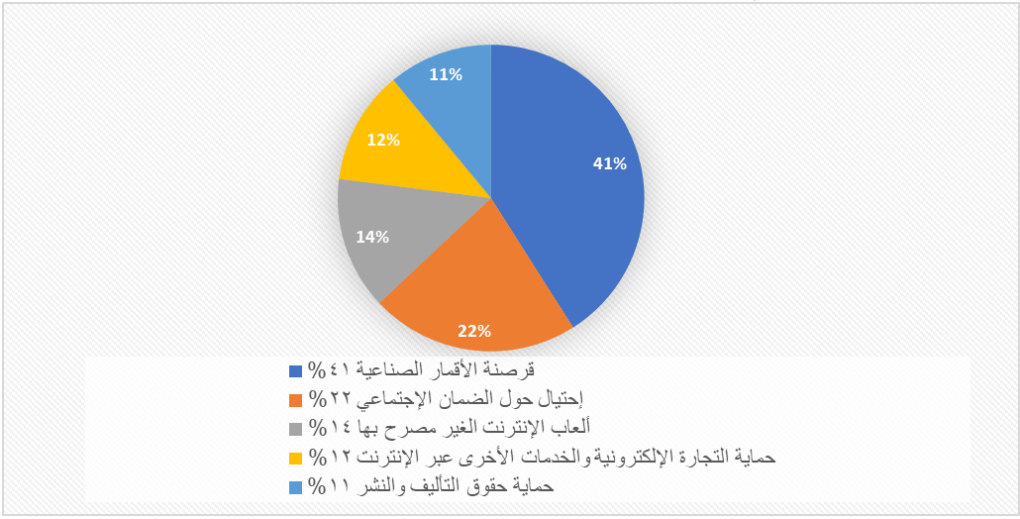
ت	اسم الوزارة	تاريخ الاختراق
1	موقع رئيس الوزراء العراقي	2016/3/23م
2	موقع مجلس النواب العراقي	2016/6/8
3	موقع وزارة الداخلية	2016/7/3
4	موقع الاستمارة الالكترونية للتعيين على ملاك وزارة الصحة	2016/8/22
5	وزارة الاتصالات	2016/10/11
6	وزارة الشباب والرياضة	2017/6/2
7	الموقع الرسمي للمفوضية العليا المستقلة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

المصدر: من إعداد الباحث بالاعتماد على: صلاح مهدي هادي الشمري وزيد محمد علي إسماعيل، الامن السيبراني كمرتكز جديد في الاستراتيجية العراقية، مجلة قضايا سياسية، العدد (62)، كلية العلوم السياسية، جامعة النهرين، 2020، ص280.

وفي أيلول عام (2019)، تعرض موقع جهاز الأمن الوطني العراقي للاختراق، وظهرت عليه رسالة موقعة بإسم جهة تطلق على نفسها اسم "ماكس برو" (M4X PrO)، وذكروا فيها عدداً من أسماء موظفين، وتم تحديد مهلة (72) ساعة، لتشكيل لجنة تحقيقية من رئاسة الوزراء بخصوص الموضوع[50].

ويمكن توضيح أنوع الجريمة في العراق، حيث أحتل النسبة الكبيرة في العراق هو قرصنة الأقمار الصناعية التي سجلت (183) حالة اختراق وبنسبة (41.0٪) من إجمالي الجرائم في العراق، يليها احتيالات حول الضمان الاجتماعي بـ (101) حالة بنسبة (22.0٪)، تليها ألعاب الإنترنت غير المصرح بها بـ (61) حالة بنسبة (14.0 ٪)، ثم حماية التجارة الإلكترونية والخدمات التي تقدم عبر الإنترنت بـ (53) حالة بنسبة (12.0٪)، ثم حماية حقوق التأليف والنشر مع (49) حالة بنسبة (11.0٪)[51]. ويوضح الشكل (2) أنواع الجرائم السيبرانية المتنوعة في العراق لعام (2013).

شكل رقم (2): أنواع الجرائم السيبرانية المتنوعة في العراق لعام (2013)



المصدر: من إعداد الباحث بالاعتماد على المصدر الآتي: Sattar J. Aboud، Cybercrime in Iraq، International Journal of Scientific & Engineering Research

إن مجال الفضاء السيبراني مجال واسع وفريد ومعقد ومتشعب، لذا يجب أن تشرع قوانين تنظيمية تصمم خصيصاً للجرائم السيبرانية وكافة العمليات في هذا المجال، فضلاً عن قانون العقوبات والقانون المدني، والقوانين الخاصة بالقطاعات المختلفة التي تتعامل مع

المعاملات الإلكترونية، وهذه التشريعات والقوانين من شأنها إرساء الأمن السيبراني كجزء من الأمن القومي.

ثالثا: الإمكانات العراقية في الأمن السيبراني

أخفق العراق في بناء الإمكانات السيبرانية، فضلاً عن عدم وجود مؤسسة رئيسية متخصصة في مجال الفضاء السيبراني فيه، وما هو موجود عبارة عن أقسام في دوائر مختلفة تفتقر للتنسيق أو التعاون المحترف في هذا الجانب وكلاً يعمل بمفرده[52]، باستثناء تأسيس فريق الاستجابة للأحداث السيبراني، وهو فريق وطني مشترك مختص بمجال الأمن السيبراني والاستجابة للحوادث السيبرانية وحماية البنية التحتية للإنترنت ونشر الوعي في مجال حماية الخصوصّية والحماية الذاتية للأفراد والمؤسسات على الإنترنت يعمل تحت إشراف مستشارية الأمن الوطني العراقي، يحمل الفريق على عاتقه مسؤولية تأمين وحماية الشبكات ومراكز البيانات الوطنية والمواقع الرسمية التي تعمل في مجال الفضاء السيبراني العراقي ويقوم بتنسيق الجهود الوطنية ودعم المؤسسات في القطاعين العام والخاص في حماية نفسها وخدماتها في الفضاء السيبراني.

ونظراً للصراع مع تنظيم داعش الإرهابي، وهبوط أسعار النفط في عام (2014)، انخفضت الموارد العامة للاستثمار في قطاع التكنولوجيا في العراق، وفي عام (2003)، والسنوات التالية، شهد العراق ازديادًا في ملكية الهواتف المحمولة كوسيلة لتجاوز أوجه القصور في البنية التحتية التكنولوجية، حيث تشير التقديرات، على سبيل المثال، إلى أن (95٪) من المجتمع العراقي لديه هواتف محمولة، ومنذ عام (2009)، إلى عام (2014)، نما قطاع المعلومات والاتصالات والتكنولوجيا بوتيرة مماثلة لباقي الاقتصاد وبنسبة (17.9٪)[53].

لكن التطورات الإقليمية لـ (داعش) عام (2014)، خلقت تباطئاً ملحوظاً في القطاع بالتزامن مع تدهور المالية العامة بسبب الأزمة الاقتصادية، لذا استمر هذا القطاع بالتخلف عن الخدمات مقارنة بالدول المجاورة، ومع ذلك، لدى العراق إمكانات هائلة، من المحتمل أن يستعيد قطاع التكنولوجيا أيضاً بعض إقدامه السابق ومواصلة التطوير حتى إن لم تكن هناك أولوية وطنية له، فإن أهمية الحلول التكنولوجية وإمكانياتها في القضايا اليومية قد تجذب في حد ذاتها التمويل اللازم للقطاع لمواصلة التوسع[54].

يلاحظ أن تطوير قطاع التكنولوجيا بطيء ويحتاج إلى مزيد من الاهتمام للنمو، وأن قطاع التكنولوجيا لم يحقق سوى قدراً ضئيلاً من التطور مقارنة بالدول الأخرى في المنطقة، وكانت الاتصالات والمدفوعات المحمولة هي القطاعات التقنية التنافسية السائدة في العراق، في حين يتبين أن مجالات التكنولوجيا الأخرى متأخرة، كالذكاء الاصطناعي، وبرمجيات أجهزة الكمبيوتر، وتطوير وبرمجة قواعد البيانات، وتطوير مواقع الويب، والأعمال التجارية عبر الإنترنت، والدفع الرقمي، والتسويق الرقمي، وتصميم الرسوم البيانية، وتطوير التطبيقات.

وعلى الرغم من أن الشركات الأجنبية هي التي تهيمن على صناعة الاتصالات السلكية واللاسلكية (مثل زين وكورك)، إلا أن وزارة الاتصالات العراقية تدير ثلاث شركات هي (شركة الاتصالات والبريد العراقية، والشركة العامة لنظم المعلومات، وشركة السلام)، وهي مسؤولة عن شبكات الألياف الضوئية وإدارة نطاقات الذكاء.

تشير الدلائل إلى أنه ما يزال هناك مجال لمزيد من تطوير الخدمات التقنيّة في العراق، لاسيما في مجال الاتصالات وتوفير خدمة الإنترنت، وقد يأخذ هذا شكل خدمات متخصصة، مثل التجارة الإلكترونيّة التي تمثل منصة مفتوحة أمام الأسواق الخارجية وما لها من عوائد تدعم الاقتصاد العراقي، والتي يمكن أن تكون بيئة جذابة لأولئك الذين يبدؤون برأس مال محدود أو قد يكونون غير قادرين على تلبية احتياجات تكلفة البدء بمثل هذا النوع من العمل أو التجارة، مثل فئة الشباب، (الذين تتراوح أعمارهم بين 15 و 24 عاما) وهم نسبة تشكل حالياً ما يقارب (19.83٪) من سكان العراق الذي يقدر عدد سكانه (38،872،655)، بحسب تقديرات وكالة الاستخبارات المركزية الأمريكية لشهر تموز من عام (2020)[55].

إن الافتقار إلى البنية التحتية والإنفاق العام المكرس لتطوير قطاع التكنولوجيا ترك عبء الاستثمار في هذا القطاع للشركات الخاصة، ولتشجيع تطوير صناعة التكنولوجيا، يمكن للحكومة أن تتخذ أولى الخطوات عبر وجود سياسات ولوائح واضحة لتوجيه هذا القطاع، فضلاً عن نظام لتجنب الاحتكارات وحقوق براءات الاختراع والحماية القانونية ضد النسخ، فضلاً عن معدلات الضرائب المدعومة للأعمال، ومع ذلك، هناك عدة عوامل تستمر في إعاقة تطوير التكنولوجيا المدعومة من القطاع الخاص، كالافتقار إلى اندماج السوق، وصعوبة تأمين الاستثمارات، والعوائق التنظيميّة والقانونيّة، وانعدام الثقة في شركات التكنولوجيا، ونقص العمالة الماهرة[56].

لذا، يُنصَح الحكومة العراقيّة بأن تشجع تطوير صناعة التكنولوجيا واتخاذ خطوات لتسهيل استثمارات القطاع الخاص، وإن دور حاضنات التكنولوجيا والقطاع غير الحكومي الذي يعمل في العراق لا يقل أهمية عن تطوير مهارات رواد الأعمال وتقديم منح لهم لبدء أو توسيع الابتكارات التكنولوجية، إن اتخاذ خطوات في هذا الاتجاه يساعد على تمكين قطاع التكنولوجيا العراقي من اللحاق بالاقتصادات التي انطلقت فيها التكنولوجيا.

المطلب الثاني: الامن السيبراني العراقي (التحديات، الفرص)

اولاً: تدابير امن الحوكمة الالكترونية

تتطلب تهديدات الإنترنت المتزايدة في العالم من الإدارات العامة التركيز على تدابير أمن الحوكمة الإلكترونية، وإدراك التهديدات التي تتعرض لها، وعلى المؤسسة المنسقة تنظيم وضع قواعد وتدابير أمن المعلومات ذات الصلة ومراقبتها والإشراف عليها، وينبغي إنشاء مؤسسة معينة على شكل فريق استجابة لطوارئ الكمبيوتر/ فريق استجابة للأحداث السيبرانية، وإنشاء عمليات تدقيق مناسبة، ويجب أن تكون جميع الوزارات والسلطات على دراية بالإجراءات الأمنية المناسبة وأن تستخدمها، وينبغي إنشاء إطار لأمن الفضاء الإلكتروني ونظام التدابير الأمنية بموجب قوانين[57].

1. التحديات

تقر المؤسسات الحكومية بالحاجة إلى سياسات أمن إلكتروني جادة وتتخذ التدابير المناسبة بقدر ما تسمح به مواردها المتاحة ولكن في كثير من الحالات لا تسمح مخصصات تمويل تكنولوجيا المعلومات والاتصالات بإجراءات أمنية منسقة، ولذا تترك مسؤولية الاستعداد للتهديدات الالكترونية ومكافحتها للأفراد المعنيين بتكنولوجيا المعلومات والاتصالات أو تسند إلى شركات من القطاع الخاص مسؤولين أيضاً عن البنية التحتية للمؤسسة، وانسجاماً مع حاجة العراق الى الأمن السيبراني تأسس فريق الاستجابة الوطني للحوادث السيبرانية لمواجهة أحداث القضاء الالكتروني في العراق تحت إشراف مستشار الأمن الوطني العراقي، ولكن ليس لهذا الفريق حضور عام نشط، حيث لم يحدث موقعه الالكتروني وقناته على وسائل التواصل الاجتماعي منذ تأسيسه في العام ٢٠١٩، وأدى عدم وجود سياسة متماسكة لأمن المعلومات إلى عدم احتفاظ بعض المنظمات باتصالات

خارجية عبر الإنترنت أو تقديم خدمات إلكترونيّة ممكنّة أخرى خوفاً من عدم القدرة على التعامل مع الحوادث السيبرانيّة المحتملة[58]، فضلاً عن ذلك لا يوجد لدى العراق تشريعات محددة للتعامل مع الجرائم السيبرانيّة، ويستخدم قانون العقوبات رقم (111) لسنة 1969 وقانون مكافحة الإرهاب لمكافحة الجرائم السيبرانية والالكترونية، وفي العام 2010 توصلت جامعة الدول العربية والعراق ضمناً، الى اتفاق بشأن الاتفاقية العربية لمكافحة جرائم تكنولوجيا المعلومات، وكان القصد وضع سياسّة جنائيّة مشتركة بشأن الهجمات الالكترونيّة غير القانونيّة والجرائم المماثلة في الدول العربية[59].

وعلى الرغم من إقرار وثيقة أمن المعلومات ومشاركة البيانات، إلا أنه لم توجد جهة معينة مسؤولة على تطبيق الفقرات الخاصة بأمن المعلومات، وتشكلت وأُلغيت اللجنة الفنية للاتصالات والمعلوماتيّة، ثم أُعيد تشكيلها، كما أن ملف الأمن السيبراني يشهد تقاطعات بين كثير من المؤسسات الحكومية التي هي: (الأمن الوطني، والمخابرات، والاتصالات، ومستشارية الامن القومي)، وقد تم حديثاً تشكيل فريق لوضع المقترحات النهائيّة بشأن تشكيل اداري يعنى بالأمن السيبراني، وبانتظار تحديد المهام وتهيئة المتطلبات الضروريّة لذلك)، وهناك في جهاز المخابرات فريق الاستجابة للأحداث السيبرانية، يقدم دعماً في هذا المجال، لكن يتطلب المزيد من الأدوات والتقنيات والاتفاقيات مع جهات دولية لتحقيق اماناً سيبرانياً عالي المستوى، فضلاً عن النقص في المعرفة لدى موظفي المؤسسات في موضوع الأمن السيبراني، وعدم ادراكهم لخطورة تسريب البيانات أو قرصنة حساباتهم، فمثلاً الموظف يضع كلمة مرور (1 2 3 4 5 6)، أو يعطي كلمة المرور الخاصة به الى زميله الآخر في العمل، وغيرها من الجوانب التي تُعرض الحسابات للاختراق بسبب الأهمال وعدم المعرفة[60].

2. الفرص

تطرح الدراسة جملة من الفرص والتدابير في مجال أمن الحوكمة الالكترونيّة عبر النقاط الآتية:

أ. اعتماد تحليل موحد وآلية اعتماد موحدة لسياسة الأمن السيبراني وتفعيل استراتيجية الأمن السيبراني العراقية في جميع مؤسسات الدولة، وينبغي تحديد مسؤوليات مؤسسية متخصصة، مثل ضرورة إدارة التهديدات مركزيا وإيجاد تعاون دولي فعال.

ب. تكليف فريق الاستجابة الوطني بإدارة الحوادث السيبرانية والإبلاغ عليها، إلى جانب تحسين رؤية أنشطتهم من أجل زيادة الوعي العام تحديد الحد الأدنى من متطلبات أمن الفضاء الإلكتروني لسلطات القطاع العام ومقدمي الخدمات الحيويّة، وتحديد البنية التحتيّة الحيوية بوضوح وتطبيق الحد الأدنى من متطلبات الأمن السيبراني، وأن يلتزم مقدمو الخدمات الرقمية ومشغلو الخدمات الأساسيّة بإخطار السلطات الحكومية المعنية بأي حوادث تمس الأمن السيبراني.

ج. تزويد المؤسسات العامة بالموارد اللازمة لضمان البنيّة التحتيّة للأمن السيبراني، وأن تشمل الموارد تمويلاً كافياً للموظفين وبرامج تدريب إضافية لجميع الموظفين العموميين ومكونات البنيّة التحتيّة الأساسيّة لضمان المستوى الأساسي للأمن السيبراني.

ثانيا: البنى التحتية للأمن السيبراني

انطلاقاً من مبدأ أن (الأمن السيبراني أوكسجين التحول الرقمي) فان توفير البنى التحتية للأمن السيبراني شرط أساسي للحكومة الالكترونيّة، وتحقيق حد أدنى من قدرة البنية التحتية لتكنولوجيا المعلومات والاتصالات ضروري لتنفيذ مشاريع الحوكمة الإلكترونية وتأمينها، بالإضافة الى ذلك تشكل التحديات التقليدية كالحروب والأزمات وعدم الاستقرار العام وكل ما يمس الأمن الوطني العراقي من تهديدات داخلية أو خارجية، عائقاً أمام مواكبة العالم الحديث المتمثل بالتقدم التكنولوجي والتقني وغيرها من العلوم الحديثة والتي ظهرت تلبية لمتطلبات تثبيت أركان الحكومة الإلكترونية وتعزيز ديمومتها وتحصينها من المخاطر السيبرانية، ويمكن أن تكون مواكبة إستراتيجية وعمليات الأمن السيبراني تحدياً يتمثل في قدرة الدولة على التكيف مع التغيير السريع في المجالات العامة عموماً، لا سيما في شبكات الحكومة والمؤسسات العامة والخاصة، فغالباً ما تستهدف التهديدات السيبرانية الأصول السرية أو السياسية أو العسكرية أو البنية التحتية للدولة[61].

1. التحديات

إن غياب مكونات البنية التحتية للأمن السيبراني أو عدم كفايتها في المؤسسات الحكومية هو أحد التحديات الرئيسة أمام الأمن السيبراني العراقي وتسهيل الاتصالات في المؤسسات، ويتعلق ذلك بقلة التخصيصات المالية المرصودة، وتقادم الأجهزة بسبب اجراءات التقشف التي تزامنت مع أحداث 2014.

2. الفرص

تطرح الدراسة جملة من الفرص في هذا المجال إذ من الضروري أن تتعاون الحكومة العراقية مع القطاع الخاص والشركات الدولية لتطوير البنى التحتية للأمن السيبراني العراقي، بالإضافة الى تبني مشاريع مشتركة تنموية على المستوى الإقليمي والدولي، ويشمل ذلك الوصول الى آليات التمويل العام لتعزيز البنى التحتية وديمومتها.

ثالثاً : التعاون الدولي

من أجل الاستفادة من المزايا التي يوفرها التعاون الدولي في ميدان العلاقات الدولية للأمن السيبراني، من المهم ان التشارك الدول في التعاون الإقليمي والدولي، فهذا التعاون يساعدها في تبادل الدروس المستفادة وبناء مشاريع مشتركة وحتى الدخول في اتفاقيات دولية أو اتحادات دولية لغرض الأمن السيبراني(62).

1. التحديات

لا يمكن التقليل من قيمة التعاون الدولي سواءً من حيث تبادل الممارسات الجيدة أو الموارد المالية التي قد ينطوي عليها الأمن السيبراني، ولكن الحصول على المساعدة الدولية والاستفادة منها بشكل كامل يتطلب امتلاك القدرات الداخلية والاستعداد، وتتولى حالياً لجنة التنمية الدولية المشكلة حديثاً ضمن الأمانة العامة لمجلس الوزراء تنسيق قضايا التنمية الدولية والمشاريع ذات الصلة، وحتى هذه اللحظة لم تفعل آلية التعاون الدولي ببرامج ومذكرات تعاون حقيقية، وحتى لو كان هنالك أمثلة لجهات دولية قد تعاونت مع العراق بشأن الامن السيبراني لكن لم تكن مثمرة ولم تحقق المستوى المطلوب، ومن أبرز أمثلة التعاون الدولي توقيع الحكومة العراقية في العام 2021 مذكرة تفاهم مع مصر في مجال تكنولوجيا المعلومات والاتصالات بهدف تبادل الخبرات في عدد من المجالات كالبنية التحتية للاتصالات والتحول الرقمي وبناء القدرات والابتكار، وأمن الفضاء الإلكتروني، والتشريع والإطار التنظيمي..... إلخ. بالإضافة إلى ذلك، أنشأ البلدان شركة مشتركة لتنفيذ مشاريع التحول الرقمي وتطوير الخدمات الإلكترونية(63)، كما وضعت مجموعة البنك الدولي إطاراً للشراكة القطرية لجمهورية العراق للفترة المالية ٢٠٢٢-٢٠٢٦ تم تنظيمه لتحسين الحوكمة الالكترونية وتقديم الخبرات وتعزيز رأس المال البشري ولكن ابتعدت تلك الشراكة عن آليات التعاون السيبرانية، حيث تضمنت لائحة الشراكة تغطية خمس عمليات رئيسية تشمل إقامة نظام مالي

متكامل ونظم للمعلومات الإدارية، والحوكمة، وتبسيط ممرات التجارة والنقل، وتطوير أنظمة الري والموارد المائية، وامدادات المياه والصرف الصحي[64].

2. الفرص

تطرح الدراسة جملة من الفرص والتدابير في مجال التعاون الدولي عبر النقاط الآتية:

أ. ينبغي أن تضع الحكومة استراتيجية واضحة للتعاون الدولي والشراكات في مجال تكنولوجيا المعلومات والاتصالات، وان تصوغ الاحتياجات التفصيلية للمواضيع ذات الأولوية للتعاون الدولي وان تضع اطاراً لمؤسسة معينة تتولى مسؤولية التعاون السيبراني.

ب. على الحكومة العراقية أن تضمن تمثيل السياسة الخارجية والعلاقات الدولية بشكل جيد في القنوات السيبرانية، وعرض اهتمامات الامن السيبراني في العراق على الدول الاخرى والمنظمات الدولية وكذلك الشركات التكنولوجيا، ويوصى بتوقيع مذكرات تفاهم مع نقاط عمل محددة بشأن المبادرات الرقمية مع الحكومات ذات الأهداف الرقمية المشتركة، والبحث بنشاط عن فرص التعاون الرقمي مع المنظمات الدولية التي تقدم الكفاءات المناسبة والنماذج المرجعية والدعم في المبادرات الرقمية.

نظراً لانعدام الرؤية المستقبلية وضعف القيادة الإدارية التي تمر بها منظومة التخطيط الإستراتيجي للعراق، التي تمثل أحدى السمات الرئيسية للعصر الحديث، بات التخبط واضحاً في مخرجات الإدارة التي انعكست على المسيرة التنموية للفرد والدولة العراقية، لاسيما أن العراق في هذه المرحلة الحساسة يحتاج إلى رؤية تخطيطية واضحة وشاملة لحوكمة التحول الرقمي والامن السيبراني، من خلال وضع برنامج حكومي ثابت الأركان مع أساليب تخطيطية واجب اتباعها لمواجهة تحديات المرحلة القادمة وتحقيق الأهداف الوطنيّة المنشودة، بمعنى التفكير والتخطيط قبل الأداء بوضع حلول لمشكلات الدولة العراقية لتحسين أداء المنظومة الإستراتيجية الخاصة بالتحول الرقمي والامن السيبراني في ضوء الإمكانات المتاحة،

فضلاً عن ذلك إن منظومة الأمن الوطني (الإستراتيجي) للعراق، تواجه جملة من التحديات التي يمكن تصنيفها بالتحديات المرئية (التقليدية) وغير المرئية (سيبرانية)، وتتجلى أخطرها بتلك التي تتظهر بالصورة غير المرئية، فلا يمكن التماسها بصورة مباشرة إلا عن طريق البحث والاستقراء التحليلي والتقني، وتشكل هذه التحديات تهديداً إستراتيجياً من شأنها أن تؤثر على الأمن الإستراتيجي (للفرد والدولة) فضلاً عن مسيرة التحول الرقمي الذي تسعى الى

تحقيق الحكومة، وبالتالي ان هذه التحديات في التحول الرقمي ستشمل معظم القطاعات والمؤسسات الحكومية وغير الحكومية، التي تتمحور حول البنية التحتية الارتكازية للدولة لتصل إلى الأمن الإدراكي للمواطن، وتتراوح هذه التحديات ما بين التهديدات السيبرانية للمنظومة الرقمية للدولة، وزيادة عدد السكان من دون أن يصيب هذه الزيادة تخطيط إستراتيجي يواكب التطورات والتحديات المحدقة بمؤسسات الدولة الرسمية وغير الرسمية، فتشكل تحدياً كبيراً لمنظومة الأمن الإستراتيجي للعراق، وبالتالي باتت الضرورة الملحة في تركيز الجهود البحثية والاستشرافية وتسلطها في هذا المجال، لاسيما في ظل الزيادة الملحوظة للتحديات المحدقة بمنظومة الأمن الوطني العراقية بشقها السيبراني لارتباطه وتماسه المباشر مع باقي قطاعات الأمن للدولة.

الخاتمة

تبشر التطورات التكنولوجية السريعة بدخول الحكومات والمؤسسات بمراحل قد توصف بأنها شديدة التحدي والإثارة أيضاً، فمما لا شك فيه أن التقنيات الناشئة ستلقي بالمزيد من الفرص والضغوط على كاهل الحكومات، كي تصبح أكثر ذكاء وابتكارا في أدائها لأدوارها والقيام بمسؤولياتها، ولكن سيتعين على الحكومات الانتقال من الهياكل البيروقراطية الحالية، التي تتميز بنمط واهتمام مرتكز على الداخل التنظيمي إلى هياكل مرنة أكثر انفتاحاً وتكون متمحورة حول احتياجات المواطن ومتطلبات المجتمع، وهو نفس الاتجاه الذي بدأت تسلكه الدولة العراقية في مشاريع التحول الرقمي.

ولكن ولكي يحدث ذلك، تحتاج الحكومة العراقية إلى تطوير قدرات جديدة ونماذج عمل مبتكرة تمنحها إمكانات التكيف والاستجابة، فحوكمة التحول الرقمي ومشاريعها يفترض أن تعمل على دعم جهود الحكومات في الانتقال من النهج التشغيلي الحالي، الذي يميل إلى التفاعل مع الأحداث (Reactive) إلى أسلوب استباقي (Proactive) مستشرف للمستقبل ويعالج المخاطر المستقبلية التي قد تنشأ في الفضاء السيبراني الآمن للحوكمة الرقمية ومستوعباتها، ولن يحدث ذلك إلا إذا قررت الحكومة تركيز دوائر اهتماماتها على المحاور الأساسية والتي تنشأ أكبر النتائج، بدلاً من القيام بمشاريع كثيرة في وقت واحد.

وعلى غرار ذلك، فإن الحكومة العراقية وخاصة في المشاريع التكنولوجية الكبيرة والمعقدة، بحاجة إلى تضييق دوائر اهتمامها، والتأكد من مدى تركيزها في تحقيق الأهداف،

وقد تستخدم مثل هذه المفاهيم كمنهجية لتقييم خياراتها المتاحة، ولتصميم مجموعات من الإجراءات الهادفة وتنفيذها في نطاقات عمل محددة ومبرمجة للتنفيذ في أطر زمنية تتوزع الأدوار بين المؤسسات الحكومية كافة، وأن الحكومة العراقية تحتاج إلى أكثر من مجرد الانبهار والتركيز على الممكنات التكنولوجية، وينبغي عليها أن تبذل جهوداً متواصلة لإحداث تحول على المستوى الداخلي أولاً وإلى أن تتمكن من التوسع خارج جدرانها؛ أي أنها يجب أن تعمل وتضمن تكامل وترابط أنظمتها الداخلية لجميع إداراتها وأقسامها وتحقيقها لمستويات الأداء والكفاءة والفعالية المنشودة خاصة فيما يتعلق باحتياجات متلقي الخدمة، عندئذ فقط سيكون بمقدورها التقدم والاستدامة في هذا المجال.

الاستنتاجات

1. لا تزال المؤسسات الحكومية في العراق تعتمد المعاملات الورقية إلى حد كبير، في ظل ضعف النظرة العامة بخصوص البيانات العمومية المتاحة، وكذلك ضعف آليات جمع البيانات يجب أن تتم عملية جمع البيانات وإدارتها في شكل رقمي ، مما يسمح بتطوير إطار عمل التشغيل البيني.
2. لم يتحقق هدف اعتماد منظومة الحكومة الالكترونية كبديل لنمط الإدارة الحالية الذي اكدت عليه خطة التنمية الوطنية 2018-2022، ولم يتم إعادة النظر في مؤسسات الخدمة المدنية واستخدام تكنولوجيا المعلومات والاتصالات في تقديم الخدمات وفي تعزيز ركائز الحوكمة الرقمية.
3. ثمة ضعف واضح في القوانين والتشريعات الخاصة بالتحول الرقمي والامن السيبراني، اذ تأخر مجلس النواب العراقي في سن القوانين المطلوبة لتفعيل تطبيقات الحكومة الالكترونية المحلية، وثمة تلكؤ واضح في اللجان البرلمانية المتخصصة بهذا الشأن، لذلك لم يتم استخدام تكنولوجيا المعلومات والاتصالات من اجل تحقيق خدمات حكومية أفضل تقدم بسهولة الى المواطنين.
4. عدم وجود مؤسسة مختصة في التحول ارقمي والامن السيبراني، الى جانب العديد من التحديات السياسية والقانونية والفنية والإدارية تواجه تطبيقات الحكومة الالكترونية المحلية والأمن السيبراني في العراق، وأدت الى ضعف واضح في تقديم

الخدمات المعلوماتية والتفاعلية الى المواطنين في الحكومة المركزية وحتى في المحافظات غير المنتظمة بإقليم.

5. ضعف التمويل المالي مما يشكل عائق امام عملية التحول الرقمي والمن السيبراني في العراق، وتكافح السلطات الحكومية حالياً من أجل الموافقة على تكاليف التطوير والتنمية الرقمية اللازمة، وهناك نقص في البنية التحتية الأساسية في العديد من المؤسسات، وإن التمويل المتقطع والتوقعات المتضاربة للمؤسسات لتمويل مشاريعها التنموية المخطط لها يحد بشكل كبير من عملية التحول الرقمي والتقدم الإنمائي والأمن السيبراني.
6. يشكل فقدان مكونات وعناصر البنية التحتية أو عدم كفايتها في المؤسسات الحكومية أحد التحديات الرئيسية التي يتم مواجهها عند التقدم والإنشاء للخدمات الإلكترونية وتسهيل الاتصالات عبر المؤسسات (بما في ذلك الأمن السيبراني) ويشمل ذلك على وجه الخصوص الوصول إلى الخدمات الأساسية المستقرة والميسورة التكلفة مثل الكهرباء أو الوصول إلى الإنترنت أو تغطية الشبكة الخلوية، وكذلك تمويل احتياجات الأجهزة والبرامج الداخلية، بما في ذلك متطلبات إدارة البيانات وتخزين المعلومات فيما يتعلق باحتياجات الأمن السيبراني الأساسية.
7. إن أحد العقبات الرئيسية للتحول الرقمي وتطوير الخدمات الإلكترونية في العراق هو ضعف سجل البطاقة الوطنية الموحدة، حيث يعتبر أحد العوامل المهمة الذي من شأنه أن يمنح الحكومة فهذا واضحا لسكان البلاد ويسمح بتحديد العملاء باستخدام الخدمات العامة.
8. ثمة ضعف واضح في رأس المال البشري، بعبارة أخرى يعاني العراق من المهارات الرقمية خاصة بين الشباب، لأن المناهج الدراسية وعلى مختلف مستويات التعليم حتى الآن لا تلبي متطلبات الاقتصاد الرقمي والمجتمع الرقمي.
9. ضعف القدرات المهنية المحلية وقلتها في مجال أمن المعلومات المتقدمة والأمن السيبراني وهذا يتطلب العمل الجاد على تدريب وتطوير كوادر مهنية محترفة في القطاع الحكومي والخاص تؤهلها على مواجهة التحديات السيبرانية.

التوصيات

1. وضع واعتماد استراتيجية تحول رقمي طويلة الأجل بُغية معالجة غياب السياسات الأساسّية للحكومة الإلكترونية والامن السيبراني في العراق وآليات الاستدامة، ينبغي على الحكومة وضع واعتماد استراتيجية تحول رقمي طويلة الأجل، والتي من شأنها أن تضمن الاتساق في التمويل العام لتكنولوجيا المعلومات والاتصالات، وتحدد الإعداد التنظيمي لتنفيذها، ذلك من شأنه أن يؤدي الى استراتيجية تحول رقمي رفيعة المستوى من شأنها أن تأخذ بنظر الاعتبار العناصر والهياكل الأساسية لنظام الادارة الرقمية (بما في ذلك التنسيق الحكومي الرقمي ، وهيكلية المؤسسة ، وإطار قابلية التشغيل البيني ، والمراجعة القانونية....وما إلى ذلك).
2. انشاء مؤسسة مستقلة للتحول الرقمي ويفضل أن تكون غير سياسية لتنسيق الحكومة الإلكترونية، يسمح موقف القيادة الواضح سياسياً في النظام الحكومي بالتواصل الواضح وتنسيق أكثر انسيابية بين المؤسسات الأخرى.
3. تفعيل آليات التشغيل البيني عن طريق إعطاء الأولوية لرقمنه الوثائق والبيانات الورقية الموجودة لأن هذا يشكل الشرط الأساسي للتنمية المستندة والقائمة على البيانات، وينبغي التركيز على رقمنه وجرد البيانات الأساسية الإلزامية عن السكان (أي السجل المدني والشركات والأراضي والممتلكات) ولتنفيذ الإطار التقني للتشغيل البيني المتبادل.
4. وضع استراتيجية للأمن السيبراني ووضع متطلبات الأمن السيبراني بموجب تشريع قانوني لينظم عمل جميع سلطات القطاع العام، إلى جانب تعيين سلطة مختصة للإشراف، ويجب إعادة فريق الاستجابة للأحداث السيبرانية CERTالحكومية الى العمل وتكليفه بإدارة الحوادث الأمنية والإبلاغ عنها.
5. بالنظر إلى أن اعتماد العديد من الإجراءات القانونية المهمة في مجال حوكمة التحول الرقمي والامن السيبراني؛ إلا ان جميع القوانين الحالية لا تأخذ في الاعتبار الفروق الدقيقة للإدارة الرقمية بشكل كاف، عليه ينبغي إجراء تحليل قانوني منهجي حول اللبنات الأساسية للبناء القانوني للإدارة الإلكترونية والامن السيبراني واعتماد الأحكام القانونية المفقودة، واجراء دراسات دقيقة لجميع

التشريعات وتشخيص التعديلات اللازمة في القوانين والأنظمة الناظمة لعمل مؤسسات الدولة، للمضي قدما في أي خطط للإدارة الإلكترونية.

6. يجب ضمان التمويل العام لتكنولوجيا المعلومات والاتصالات، حيث يجب أن تسلك جميع قرارات التمويل إلى استراتيجيات التخطيط والتنفيذ طويلة المدى وفقًا لأفضل الممارسات أن تبلغ ميزانية التحول الرقمي للمؤسسة 1% على الأقل من الميزانية الإجمالية لتقديم الحد الأدنى من الأموال لتنمية القطاع الرقمي.
7. من الضروري أن تكون البطاقة الوطنيَّة الموحدة في البنية أو الهيكل الأساسيّ لتحديد الهوية في الخدمات الحكومية، مما يوفر إمكانية التصديق الموثوق به على الأشخاص بعد الوصول إلى الزيادة النسبية في استيعاب الهوية الوطنية، لتسهيل تقديم المزيد من الخدمات التي تعتمد على اساس رمز الهوية الرقمية.
8. ينبغي تعميم تعزيز المهارات الرقميّة عبر المناهج الدراسية على جميع المستويات، كما ينبغي تنظيم حملات توعية عامة خارج القطاع العام، وعلى وزارة التربية مراجعة وتنقيح مناهج المدارس الابتدائية والمتوسطة والثانوية التي تشمل مواضيع تخص الاستخدام الأمثل لتكنولوجيا المعلومات والاتصالات وحماية البيانات الشخصية في بيئة الإنترنت.

المصادر والمراجع:

---

(1) Midea Sabah Ali, Selvakumar Manickam, A Brief Review of Cybersecurity Issues in Iraq, National Advanced Center of Excellence, Universiti Sains Malaysia, Technical Report, Malaysia, April, 2018, p16.

(2) جان سيريل فضل الله، التخطيط لبناء قاعدة تطبيقية لتقييم خدمات الحكومة الالكترونية في العراق، المجلة العراقية لبحوث السوق وحماية المستهلك، العدد (2)، 2012، ص88.

(3) مريم خالص حسين، الحكومة الالكترونية، مجلة كلية بغداد للعلوم الاقتصادية الجامعة، العدد (4)، كلية بغداد للعلوم الاقتصادية الجامعة، 2013، ص456.

(4) مرتضى احمد خضر، تطبيق الحكومة الالكترونية في العراق: الحلو والافاق المستقبلية، رسالة ماجستير (غير منشورة)، كلية العلوم السياسية، جامعة تكريت، 20189، ص128.

(5) محمد مدحت، الحكومة الالكترونية، المجموعة العربية للتدريب والنشر، القاهرة، 2016، ص229.

(6) معوقات تنفيذ قانون التوقيع الالكتروني والمعاملات الالكترونية رقم (78) لسنة (2012) في العراق، ندوة الجامعة المستنصرية، الجامعة المستنصرية، شبكة المعلومات الدولية (الانترنت)، على الرابط: https://uomustansiriyah.edu.iq/web_article.php?post_id=g=ar ، تاريخ الزيارة: 2023/9/1.

(7) التقرير الاستهلالي (توفير الأولويات الاستراتيجية للإدارة الالكترونية، وخرائط الطريق، وخطط التنفيذ)، الإصدار (2)، مؤسسة اكاديمية الإدارة الالكترونية (EGA)، بغداد، 2022، ص2.

(8) لجنة الامر الديواني (22) لسنة 2020، لجنة إدارة وتنسيق النشاط الحكومي باتجاه الحوكمة الالكترونية، الأمانة العامة لمجلس الوزراء، بغداد، 2023، ص3.

(9) لجنة الامر الديواني (22) لسنة 2020، لجنة إدارة وتنسيق النشاط الحكومي باتجاه الحوكمة الالكترونية، مصدر سبق ذكره، ص4.

[10] مقابلة اجراها الباحث مع الدكتور حميد الغزي/ الأمين العام لمجلس الوزراء العراقي ورئيس لجنة (22)، بغداد، بتاريخ 2023/8/23.
[11] مقابلة اجراها الباحث مع الدكتور حميد الغزي/ الأمين العام لمجلس الوزراء العراقي ورئيس لجنة (22)، بغداد، بتاريخ 2023/8/23.
[12] المصدر نفسه.
[13] لجنة الامر الديواني (22) لسنة 2020، مصدر سبق ذكره، ص5.
[14] مقابلة اجراها الباحث مع الدكتور حميد الغزي/ الأمين العام لمجلس الوزراء العراقي ورئيس لجنة (22)، بغداد، بتاريخ 2023/8/28.
[15] الكراس التدريبي لنظام إدارة المستندات، الأمانة العامة لمجلس الوزراء/ مركز البيانات الوطني، بغداد، 2023، ص2.
[16] مقابلة اجراها الباحث مع الدكتور حميد الغزي/ الأمين العام لمجلس الوزراء العراقي ورئيس لجنة (22)، بغداد، بتاريخ 2023/10/14.
[17] Similar web, top websites ranking most visited websites in Iraq, available on: https://www.similarweb.com/top-websites/iraq/, Accessed on: 25/9/2023.
[18] المشاريع التكاملية المركزية لمركز البيانات الوطني، دائرة مركز البيانات الوطني، الأمانة العامة لمجلس الوزراء، بغداد، 2023، ص7-8.
[19] المصدر نفسه، ص9-10.
[20] المشاريع التكاملية المركزية لمركز البيانات الوطني، مصدر سبق ذكره، ص10.
[21] المشاريع التكاملية المركزية لمركز البيانات الوطني، مصدر سبق ذكره، ص11.
[22] المشاريع التكاملية المركزية لمركز البيانات الوطني، مصدر سبق ذكره، ص14.
[23] الموقع الرسمي لمنصة سلامات، وزارة الصحة العراقية، شبكة المعلومات الدولية (الانترنت)، على الرابط: https://salamat.ur.gov.iq/pcr_result.aspx ، تاريخ الزيارة: 2023/9/29.
[24] الموقع الرسمي لبوابة اور الالكترونية للخدمات الحكومية، نظام التحقق من البطاقة الوطنية واثبات الحياة، شبكة المعلومات الدولية (الانترنت)، على الرابط: https://ur.gov.iq/ ، تاريخ الزيارة: 2023/9/29.
[25] المشاريع التكاملية المركزية لمركز البيانات الوطني، دائرة مركز البيانات الوطني، الأمانة العامة لمجلس الوزراء، بغداد، 2023، ص16.
[26] المشاريع التكاملية المركزية لمركز البيانات الوطني، دائرة مركز البيانات الوطني، الأمانة العامة لمجلس الوزراء، بغداد، 2023، ص16.
[27] غونزالو بيزارو وداني وزن وآخرون، مصدر سبق ذكره، ص 61.
[28] مقابلة اجراها الباحث مع الدكتور حميد الغزي/ الأمين العام لمجلس الوزراء العراقي ورئيس لجنة (22)، بغداد، بتاريخ 2023/10/14.
[29] غونزالو بيزارو وداني وزن وآخرون، مصدر سبق ذكره، ص63.
[30] مقابلة اجراها الباحث مع الدكتور حميد الغزي/ الأمين العام لمجلس الوزراء العراقي ورئيس لجنة (22)، بغداد، بتاريخ 2023/10/14.
[31] فطيمة الزهراء لواطي، معوقات تطبيق الحوكمة الالكترونية في المؤسسات العمومية ذات الطابع الإداري، رسالة ماجستير (غير منشورة)، كلية العلوم الاقتصادية والتجاري وعلوم التسيير، جامعة محمد خيضر/ بسكرة، الجزائر، 2015، ص146.
[32] مقابلة اجراها الباحث مع الدكتور حميد الغزي/ الأمين العام لمجلس الوزراء العراقي ورئيس لجنة (22)، بغداد، بتاريخ 2023/10/14.
[33] صفاء عياد، قانون جرائم المعلوماتية في العراق: معلق الى حين، شبكة المعلومات الدولية (الانترنت)، على الرابط: https://smex.org/ar/%D9%82 %D9%82/ ، تاريخ الزيارة: 2023/11/11.
[34] قانون جرائم المعلوماتية العراقية، هيومن رايتس ووتش، شبكة المعلومات الدولية (الانترنت)، على الرابط: https://www.hrw.org/reports/iraq0712arForUpload.pdf ، تاريخ الزيارة : 2023/11/11.
[35] مريم خالص حسين، مصدر سبق ذكره، ص249.
[36] جوليا كلارك وآخرون، دليل الممارس لمساعدة البلدان في مسيرتها نحو الهوية الرقمية، مدونات البنك الدولي، شبكة المعلومات الدولية (الانترنت)، على الرابط: https://blogs.worldbank.org/ar/voices/new-practitioners-guidation-journey ، تاريخ الزيارة: 2023/11/12.
[37] مقابلة اجراها الباحث مع اللواء الحقوقي صلاح مهدي جبار الشمري/ مدير مديرية البطاقة الوطنية الموحدة، بغداد، بتاريخ 2023/10/10.
[38] مقابلة اجراها الباحث مع الدكتور ضياء عواد كاظم/ رئيس الجهاز المركزي للإحصاء/ عضو لجنة 22 لسنة 2020ورئيس فريق عمل نظام الموارد البشرية والرواتب، بغداد، بتاريخ 2023/10/16.
[39] مقابلة اجراها الباحث مع الدكتور حميد الغزي/ الأمين العام لمجلس الوزراء العراقي ورئيس لجنة (22)، بغداد، بتاريخ 2023/10/14.
[40] دليل تقييم المهارات الرقمية، الاتحاد الدولي للاتصالات/ قطاع التنمية، 2020، ص4.

(41) مقابلة اجراها الباحث مع الدكتور حميد الغزي/ الأمين العام لمجلس الوزراء العراقي ورئيس لجنة (22)، بغداد، بتاريخ 2023/10/14.

(42) مقابلة اجراها الباحث مع الدكتور حميد الغزي/ الأمين العام لمجلس الوزراء العراقي ورئيس لجنة (22)، بغداد، بتاريخ 2023/10/14.

(43) فريق الاستجابة للأحداث السيبرانية، استراتيجية الامن السيبراني العراقي 2022-2025، بغداد، 2022، ص3.

(44) فريق الاستجابة للأحداث السيبرانية، استراتيجية الامن السيبراني العراقي 2022-2025، مصدر سبق ذكره، ص7.

(45) فريق الاستجابة للأحداث السيبرانية، استراتيجية الامن السيبراني العراقي 2022-2025، مصدر سبق ذكره، ص8.

(47)Al Tamimi & Company - Haydar Jawad and Aro Omar, Cybercrime Legislation in Iraq, Lexology.com, September, 2017. https://www.lexology.com/library/detail.aspx?g=5cac76e7-3a6c-4b8e-8ed9-a41c15357354

(47)Sattar J. Aboud, An Overview of Cybercrime in Iraq, The Research Bulletin Jordan ACTM, Vol. 2, No. 2, January 2012, p31

(48) Sattar J. Aboud, Cybercrime in Iraq, International Journal of Scientific & Engineering Research, Volume 5, No. 3, March- 2014, pp 422-425.

(49) صلاح مهدي هادي الشمري وزيد محمد علي إسماعيل، الأمن السيبراني كمرتكز جديد في الاستراتيجية العراقية، مجلة قضايا سياسية، العدد (62)، كلية العلوم السياسية، جامعة النهرين، 2020، ص280.

(50) مؤسسة سكاي نيوز عربية الإخبارية، اختراق موقع جهاز الأمن الوطني العراقي، أبو ظبي، متاح على الموقع الآتي: https://www.skynewsarabia.com/middle-east/1286344

(51) Sattar J. Aboud, Cybercrime in Iraq, International Journal of Scientific & Engineering Research, 3Volume 5, No. 3, March- 2014, pp 42

(52) مركز الإعلام الرقمي، العراق يحتل مركزا متواضعا في الأمن السيبراني متاح على الرابط الآتي: https://dmc-iq.com/2019/03/31/%D8% /

(53) International Organization for Migration, IOM Iraq – 2019, Technology and Innovation In Iraq, A Market Assessment of Tech Sector Businesses in Iraq, P.4.

(54) International Organization for Migration, IOM Iraq – 2019, OP. Cit, P.

(55) Cia.gov. (2019). Middle East: Iraq, the World Factbook - Central Intelligence Agency. Available at: https://www.cia.gov/library/publications/the-worldfactbook/geos/iz.html].

(56) International Organization for Migration, IOM Iraq – 2019, Technology and Innovation In Iraq, A Market Assessment of Tech Sector Businesses in Iraq, P.4.

(57) علي حمد الخوري، الحكومة الرقمية: مفاهيم وممارسات، المنظمة العربية للتنمية الإدارية، جامعة الدول العربية، القاهرة، 2018، ص203.

(58) مقابلة اجراها الباحث مع الأستاذ مراد عبد الصمد هادي/ رئيس فريق الاستجابة الوطني للحوادث السيبرانية، 2023/11/1، بغداد.

(59) الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الأمانة العامة لجامعة الدول العربية، إدارة الشؤون القانونية، القاهرة، 2010، ص17.

(60) مقابلة اجراها الباحث مع الأستاذ مراد عبد الصمد هادي/ رئيس فريق الاستجابة الوطني للحوادث السيبرانية، بغداد، 2023/11/1.

(61) علي زياد العلي, التحديات غير المرئية للأمن الوطني العراقي, مركز البيان للدراسات والتخطيط, مقال منشور عبر شبكة المعلومات الدولية (الإنترنت) على الموقع: https://www.bayancenter.org/2018/06/4565

(62) ينظر بتصرف: سعاد عبد الله محمد واحمد حامد علي، الامن السيبراني في دول مجلس التعاون لدول الخليج العربية بمنظور جيوبولتيكي معاصر، مجلة جامعة الانبار للعلوم الإنسانية، العدد (3)، جامعة الانبار، 2020، ص382.

(63) وزير الاتصالات وتكنولوجيا المعلومات المصري والنظير العراقي يبحثان تعزيز التعاون في مجال تكنولوجيا المعلومات والاتصالات ، موقع الهيئة العامة للاستعلامات، شبكة المعلومات الدولية (الانترنت)، على الرابط: https://www.sis.gov.eg/Story/219743/%D3?lang=ar

(64) وثيقة مجموعة البنك الدولي، استراتيجية الشراكة مع جمهورية العراق للسنوات المالية 2022-2026، البنك الدولي، 2022، ص9.

ملف العدد
الأمن السيبراني
درع التحول الرقمي العراقي
(بين التحديات الراهنة وضرورات المستقبل)

رؤية استراتيجية تحليلية لواقع الحوكمة الرقمية في العراق
التحديات والفرص

أ.م.د. مروان سالم العلي
جامعة الموصل/ كلية العلوم السياسية

إنَّ تبني مُبادرات الحوكمة الرقمية على المستوى المحلي العِراقي مِن شأنهُ تحسين استجابة الحكومة لاحتياجات المواطنين، والحدُ مِن البيروقراطية والأعباء الإدارية على المسؤولين الحكوميين. هذا الأمر يوفر فرصة عظيمة لِمُعالجة الافتقار إلى مُبادرات حوكمة واقعية في البلد. وبالتالي فإن تمكُن الحكومة العِراقية مِن تسخير إمكانات التقنيات الرقمية لإحداث تغيير إيجابي وتطوير في مؤسسات الدولة، يُساعد ذلك على فهم مدى تبني الحكومة للتقنيات الرقمية ودمجها في عملياتها وخدماتها، ويوفر رؤية استراتيجية واضحة مُفيدة لفهم تحديات وفرص الحكومة الرقمية في سياق النظُم السياسية، على نحوٍ يُقلل مِن التحديات ويزيد مِن الفرص، بيد إنّ عملية التحول الرقمي في العِراق مُعقدة وصعبة، وقد تستغرق وقتاً للتنفيذ الكامل، وتحقيق الفوائد الكاملة مِن المُهم أَنَّ تستمر الحكومة العِراقية في الاستِثمار في التقنيات الرقمية بالشكل الأمثل واعتمادها، مع مُعالجة التحديات التي أعاقت جهودها للتحول الرقمي، مثل محدودية الوصول إلى التكنولوجيا ونقص المهارات الرقمية

الكلمات المفتاحية: الحوكمة الرقمية، الحكومة الالكترونية، العراق، التحديات، الفرص.

An analytical strategic vision of the reality of digital governance in Iraq: Challenges and opportunities

Assistant professor. Dr. Marwan Salem Al-Ali
College of Political Science/University of Mosul

Adopting digital governance initiatives at the Iraqi local level would improve the government's responsiveness to citizens' needs, and reduce bureaucracy and administrative burdens on government officials. This provides a great opportunity to address the lack of realistic governance initiatives in the country. Therefore, if the Iraqi government is able to harness the potential of digital technologies to bring about positive change and development in state institutions, this helps to understand the extent to which the government has adopted digital technologies and integrated them into its operations and services, and provides a clear strategic vision useful for understanding the challenges and opportunities of digital government in the context of political systems, in a way that reduces... challenges and increases opportunities. However, the process of digital transformation in Iraq is complex and difficult, and may take time to fully implement

الاستلام	الارجاع	القبول
2024/1/15	2024/3/8	2023/5/21

and realize the full benefits. It is important that the Iraqi government continues to invest in and adopt optimal digital technologies, while addressing the challenges that have hindered its digital transformation efforts, such as limited access to technology and lack of skills. digital

Keywords: digital governance, e-government, Iraq, challenges, opportunities.

المُقدمة

تعد الحكومة الرقمية أَولوية رئيسة للحكومات في عالمنا المُعاصر، إِذ تسعى أَغلب الأَنظمة السياسية المُعاصِرة إلى تحسين كفاءة أَجهزتها الحكومة وفعاليتها، عن طريق الاستجابة في تقديم الخدمات للمواطنين. وفي العِراق، تُمثِل الرقمنة تحديات وفرصاً على حدٍ سِواء، إِذ تعمل الحكومة على تسخير إِمكانات التقنيات الرقمية لإِحداث تغيير إِيجابي وتطوير في مؤَسسات الدولة؛ وبتوظيف نموذج نضج الحكومة الرقمية في الحالة العراقية؛ ليُساعدنا على فهم مدى تبني الحكومات للتقنيات الرقمية ودمجها في عملياتها وخدماتها، ويوفر رؤَية واضِحة مُفيدة لفهم تحديات وفرص الحكومة الرقمية في سياق النظُم السياسية. فعن طريق تحليل جهود التحول الرقمي في العِراق، وتقرير (برنامج الأُمم المُتحدة الإِنمائي لعام2023)، يمكننا الحصول على نظرة ورؤَية استراتيجية ثاقبة للوضع الحالي للتحول الرقمي في العِراق، وتحديد مجالات التحسين والنمو في العالم الحديث، أَصبح التحول الرقمي عامِلاً حاسِماً للنجاح والقدرة التنافُسية، وتتبنى الحكومات في جميع أَنحاء العالم بشكلٍ مُتزايد التقنيات الرقمية، لتحسين كفاءة عملياتها وفعاليتها. والعِراق ليس استثناءً مِن هذا الاتجاه، فقد بُذلت جهود حثيثة في السنوات الأَخيرة ولا تزال الجهود مُستمرة لتحويل قطاعاتها ووظائفها المُختلِفة رقمياً. ويُلاحظ في العِراق ضعف الحوكمة الرقمية، وهذا ناجم عن الظواهر السلبية التراكمية التي ترجع إِلى عقود عانى مِنها العِراق مِن ضعف الجهاز الإِداري، مِما شكل تحدياً كبيراً أَمام تحقيق البرامج والمشاريع التنموية، وهدراً في الجهود والطاقات والأَموال.

أَهمية البحث:

تكمنُ أَهمية البحث في كونهُ يتناول واحدةً من أَبرز مُتطلبات العصر لنهوض وتقدم الدول وهي الحوكمة الرقمية ولاسيما في دولتنا العِراق في ظل التحديات التي يُعاني منها العراق من تطبيقها بشكلٍ كامل وفعال، اذ تظهر الحاجة إِلى الحوكمة الرقمية بوصفها أَداة فاعِلة مِن أَدوات الإِصلاح، إِذ تُمارس مِن خِلالها السلطة السياسية والاقتصادية والإِدارية دوراً في

إدارة الموارد الاقتصادية لتدوير عجلة الاقتصاد الوطني مِن أَجل النهوض بمؤَسسات الدولة سِواءً أَكانت العامة مِنها أَو الخاصة والمُجتمع المدني في طريق تحقيق النمو الاقتصادي والرفاهية المُجتمعية. كما تبرز أَهمية البحث في الوقوف على أَبرز مُحدِدات تطبيق الحوكمة الرقمية في العِراق، وتقديم أَبرز الحلول والفرص التي مِن المُمكن أَنَّ تُساعد صانع القرار العِراقي مِن تطبيقها على أَرض الواقع.

إِشكالية البحث:

يستكمل العِراق في المؤَسسات الحكومية، مشروع الحوكمة والأَتمتة، عبر إِطلاق منصات إِلكترونية وربط دوائر الدولة ببرامج مركزية، هدفها الحدُ مِن البيروقراطية الإِدارية والحدُ مِن الفساد، لتعزيز مفاهيم الشفافية والسلامة الرقابية، لكن ما مدى فاعلية هذه المنصات؟، وهل يمكن لجميع العِراقيين الوصول إِليها بسهولة؟. العمل فعلياً يسير بإِيقاع بطيء، مُقارنةً بما تم إِقرارهُ قبل نحو ثماني سنوات حين شرعت الحكومة بالمضيّ نحو تفعيل الحوكمة الإِلكترونية والانتِهاء مِن التعامُل الورقي، في ظل ما تواجهه الحوكمة الرقمية في العِراق مِن تحديات عديدة.. ومِن هُنا فان إِشكالية البحث تكمنُ في الإِجابة على تساؤَل رئيس مفادهُ ما هي أَبرز التحديات والفرص المطروحة لإِقامة الحوكمة الرقمية في العِراق..

فرضية البحث:

يقوم البحث على فرضية مفادها، كُلما تمكنت الحكومة العِراقية مِن تسخير إِمكانات التقنيات الرقمية لإِحداث تغيير إِيجابي وتطوير في مؤَسسات الدولة، وبتوظيف نموذج نضج الحكومة والحوكمة الرقمية في الحالة العِراقية، كُلما ساعدنا ذلك على فهم مدى تبني الحكومة للتقنيات الرقمية ودمجها في عملياتها وخدماتها، ويوفر رؤَية استراتيجية واضِحة مُفيدة لفهم تحديات وفرص الحكومة الرقمية في سياق النظُم السياسية، على نحوٍ يُقلل مِن التحديات ويزيد مِن الفرص.

هدف البحث:

يهدف البحث إِلى تسليط الضوء على المجالات الرئيسية التي يمكن فيها تنفيذ مُبادرات الحوكمة الرقمية، مع التركيز على ضمان نجاحها مِن خِلال النظر في عوامل النجاح الأَكثر أَهمية.

ولتحقيق النجاح تقدم البحث بمجموعة من التوصيات في مُقدِمتها ضرورة أن تقوم الحكومة العِراقية بتقييم مدى استعدادها لتنفيذ مُبادرات الحوكمة الرقمية، بِما في ذلك الكفاءة الفنية وفهم التقنيات الرقمية لموظفيها، فضلاً عن استعدادهم لتبني طرق جديدة للعمل. كما يهدف البحث إلى استِكشاف تحديات الحكومة الرقمية في العِراق وفرصها، ودِراسة أَبرز التحديات التي تواجه الحكومة الرقمية والفوائد المُحتملة.

هيكلية البحث:

انطلاقاً مِن إشكالية البحث وفرضيتهُ، تم تقسيم البحث فضلاً عن المُقدمة والخاتمة والاستنتاجات إلى مِحورين رئيسين، تناول المِحور الأَول؛ تحديات الحوكمة الرقمية في العراق. بينما تناول المِحور الثاني فرص تطبيق الحوكمة الرقمية في العِراق.

المِحور الأول: تحديات الحوكمة الرقمية في العِراق

طالت التطورات الكبيرة التي شهدتها العقود الماضية مُختلف جوانب الحياة السياسية والاقتصادية والاجتماعية والثقافية، وقد كان لازدياد وعي المواطنين، ولارتفاع مستوى توقعاتهم، الدور الكبير في التأثير على أداء المُنظمات والمؤَسسات، بحيث اتخذت مُختلف الوسائل والسُبل المُمكِنة وسخرتها في سبيل تقديمها لخدماتها بسرعة ودقة وكفاءة وفعالية.

وما أَنَّ ظهرت شبكة الانترنت حتى تسارعت العديد مِن الدول للاستفادة مِنها في أدائها لوظائفها ومهامها، حيث برز إلى الوجود ما يُعرف بمفهوم الحكومة الرقمية (E-Government) أَول مرة في الأقطار العربية فقد تبنت كُل مِن مصر وإمارة دُبي والأَردن هذا المفهوم وبدأَت بالعمل نحو تطبيقهُ تبعها مُعظم الأَقطار العربية ومِنها العِراق وسلطنة عُمان والبحرين والسعودية وتونس[1].

إذ شرعت الحكومة العِراقية بعد نقل السيادة في حُزيران/يونيو2004 بانتهاج آليات الاقتصاد الرقمي في محاولة مِنها لردم الفجوة التقنية والمعرفية بين الاقتصاد العِراقي والاقتصاد العالمي وصولاً إلى تحقيق التطبيقات العلمية والعملية في شتى المجالات لتقديم أَفضل الخدمات لعموم المواطنين إلاَّ ان هذا المشروع يحتاج إلى[2]:

- الشفافية ووضوح سياقات الحقوق والواجبات.
- تحقيق المُشاركة السياسية الفاعِلة وتسهيل الإجراءات.

- تحسين مستويات الخدمات المُقدمة وتطوير أَداء الإِدارة المالية.
- استقلال تكنولوجيا المعلومات وتطبيقاتها المُختلفة لتطوير الإِدارة العامة وذلك مِن خِلال توسيع قاعدة المُستخدمين لشبكات المعلومات والخدمات الالكترونية.
- التخلُص مِن الأَساليب الروتينية والقضاء على البيروقراطية بأَشكالها المُختلفة والعمل على تقديم خدمات أَفضل وبتكاليف أَقل.
- تحقيق مفهوم الشراكة بين مؤَسسات القطاعين العام والخاص بمعناها الحقيقي.
- تحديد الخدمات التي سيتم تقديمها الكترونياً مِن قِبل الدوائر الحكومية المُختلفة مثل تقديم هذه الخدمة مِن قِبل دائرة الضريبة، ودوائر المرور العامة، ومؤَسسات الضمان الاجتماعي، ودوائر الكهرباء والاتصالات، وتطوير البُنى التحتية لتكنولوجيا المعلومات، وتطوير الجوانب التشريعية للحكومة الالكترونية، وتطوير المهارات والإِمكانات البشرية العامة في هذه المجالات.

هذا يعني إِنَّ عملية التحول الرقمي في العِراق، لم تخلُ مِن التحديات والعقبات، فالحوكمة ظاهرةٌ مُعقدةٌ لها انعكاساتها على التنمية البشرية والاقتصادية والاجتماعية، غير أَنَّ مسالة تطبيق الحوكمة ونجاحها في العِراق تستوجب التعرُف على التحديات أَو المعوقات الرئيسة للحوكمة الرقمية في العِراق والتي تم إِيجازها على وفق الفقرات الآتية[3]:

أَولاً: تحديات ثقافية – تكنولوجية

1. **محدودية الوصول إِلى التكنولوجيا والبُنية التحتية الرقمية** وعدم وجود شبكة اتصالات تُغطي جميع مناطق العِراق، إِضافة إِلى ارتفاع كُلفة الاتصالات لاحتِساب كُلفة استخدام الانترنيت، في حين هُنالك تقدُماً في زيادة انتشار الإِنترنت وتوافر أَجهزة مثل الهواتف الذكية، إِذ لا يزال هُناك تفاوتات كبيرة في الوصول إِلى التكنولوجيا بين المناطق الحضرية والريفية، وكذلك بين المجموعات الاجتماعية والاقتصادية المُختلِفة. لذا يمكن أَنَّ تخلق هذه الفجوة الرقمية حواجز أَمام اعتماد واستِخدام التقنيات الرقمية، مِما يُعيق قدرة المؤَسسات في إِيصال خدماتها لباقي شرائح المُجتمع.

2. **الافتقار إلى المهارات والقوى العاملة الرقمية,** إذ إنَّ الوتيرة السريعة للتغير التكنولوجي تعني أنَّ هُناك طلباً مُستمراً على العُمال ذوي الخبرة في التقنيات الناشئة. فضلاً عن البيروقراطية لمؤَسسات الدولة الذي يخلق عقبات أَمام المشاريع الرقمية.
3. **ارتفاع نسبة الأُمية الرقمية:** إنَّ أَهم التحديات التي تواجه التحول مِن تقديم الخدمات الحكومية التقليدية وصولاً إلى تقديمها الكترونياً تتمثل بتدني قدرات مُستخدمي شبكة الانترنت بشكلٍ خاص ومهارات مُستخدمي تكنولوجيا المعلومات بشكلٍ عام. وبمُجرد الاطلاع على إحصاءات تتعلق بعدد مُستخدمي الإنترنت في العِراق، مُقارنةً بنسبة الأَمية الرقمية خصوصاً بين الشباب، يمكن استقراء صعوبة الوصول بالنسبة لكافة المواطنين البالغين للخدمات الحكومية. وبحسب موقع" داتا ريبورتال"، فإنَّ عدد مُستخدمي الإنترنت، حتى كانون الثاني/يناير2022 وصل إلى (20,58) مليوناً، ما يُعادل نصف سُكان العِراق تقريباً، الذي قُدّر في كانون الثاني/يناير2022، بـ (41,67) مليوناً، (56,8%) مِنهُم في الفئة العمرية (18-64)، أَي مِمن يُتوقع أَنهم قد يحتاجون للوصول إلى خدمات حكومية. أَما مُعدل الأُمية الإلكترونية، فيُقدر بين الشباب (15عاماً-24 عاماً) بـ (60%) وفق مُنظمة "اليونيسف "التابِعة للأُمم المُتحدة (تموز/ يوليو2022)[4].
4. **عدم فاعلية الحكومة الإلكترونية:** تبنت الحكومة العِراقية ضمن برنامجها الحكومي (2014/ 2018)، تطبيق الحكومة الالكترونية لرفع الكفاءة والإنتاجية وغلق الفساد، وعلى الرغم مِن وجود الحكومة الإلكترونية في العِراق على شبكة الانترنت حيثُ تُسمى حكومة المواطن الإلكترونية، والتي يمكن مِن خِلالها تقديم الطلبات إلى(52) جِهة رسمية مِن وزارات ومُحافظات وجِهات أَخرى، إلاَّ انها لا تزال غير فعالة بشكلٍ حقيقي حيثُ يمكن الاطلاع على المعلومات والإجراءات، مع إمكانية تنزيل الاستِمارات المطلوبة مِن دون إنجاز المُعاملات إلاَّ بشكلٍ محدود، أَي أنها لم تعمل كما هو الحال في البُلدان المُتقدمة وبعض دول المنطقة ولاسيما البحرين والسعودية ودولة الكويت ودولة قطر، وهو ما يؤَكد محدودية دور الحكومة الإلكترونية في العِراق هو احتلالها المرتبة(141) ضمن مؤَشر تطوير

الحكومة الإلكترونية التابع للأُمم المُتحدة[5]. هذا المؤَشر الذي يتضمن (193) دولة، ويتم بنائه على ثلاث مؤَشرات: مؤشر خدمة الانترنت مؤشر البُنية التحتية للاتصالات السلكية واللاسلكية مؤَشر رأَس المال البشري حيثُ تقع هذه الدول ضمن المراكز الخمسين الأُولى على مستوى العالم، إذ تحتل البحرين المرتبة(24) والإمارات(25) والكويت(40) والسعودية(44) وقطر(48) في عام (2016)، علماً أَنَّ هذا التقرير يصدر كُل سنتين مرة واحدة وتتراوح النسبة المئوية لِمُستخدمي الانترنت لهذه الدول مِن (70 إلى80%) مِن مجموع السُكان، لاسيما وأَنَّ استِعمال الانترنت يُعبر عن ثلاث قضايا وهي: الأُمية، مدى توفر البُنى التحتية، الدخل، بينما النسبة المئوية لِمُستخدمي الانترنت في العِراق تتراوح مِن بين (20 إلى 25%) مِن مجموع السُكان[6].

5. الوقوف على الحوكمة الإلكترونية يتطلب بالضرورة الوقوف على المرحلة التي تقف عليها المؤَسسات العِراقية بشكلٍ عام، بين ما يُعرف بالإدارة الإلكترونية، وبين الحكومة الإلكترونية، وبين الحكومة الذكية، التي بدأَت دول المنطقة العمل بموجبها، أَما نحنُ في العِراق: فما زلنا على اعتاب المرحلة الأُولى، مُمثلةً بالإدارة الإلكترونية وبشكلٍ محدود، حين بدأَت الكثير مِن القطاعات بالإعداد لقواعد بيانات وآليات ترابط رقمي، لم يجر تشبيكها بعد بالقطاعات والمؤَسسات الأُخرى المُرتبطة بإتمام تقديم الخدمة أَو المُنتج للمُستهدف بها، بوصفها عملية تكامُلية. وقد يكون أَبرز ما يحول دون إكمال مثل هذا الترابط الذي يكون بمنزلة الركن الأَساس في انطِلاقة الحكومة الإلكترونية المنشودة، إعلان الإدارات العُليا للكثير مِن المؤَسسات خشيتها مِن انتهاك قواعد بياناتها أَو خصوصياتها في حال تشبيكها مع مؤَسسات خارِجة عن صلاحياتها، نتاج عدم وعيها بآليات ومُتطلبات مثل هذا الترابط، وما حدود قواعد البيانات التي يتم مُشاركتها لإتمام الأَعمال!...[7].

ثانياً: تحديات سياسية- قانونية- أَمنية

1. أن أَبرز تحدٍ مِن المُمكن أَنَّ يواجه العِراق بشأَنَّ الرقمنة، فهو (الأَمن السيبراني) وكيفية المُحافظة على خصوصية البيانات الخاصة والعامة للدولة. إذ تتأَثر عملية التحول الرقمي في العِراق بالمخاوف الأَمنية وخصوصية البيانات مع ازدياد الهجمات السيبرانية

وظهور (الإرهاب الالكتروني)، سيكون ضمان أَمن بيانات الدولة وحمايتها، مِن مسؤَولية السلطات الرسمية مع استِمرارها في التحول الرقمي، وضمان الأَمن القومي العِراقي.

2. **تخلُف مؤَسسات الدولة:** إِنَّ نِظام الحكومة الالكترونية هو نِظام مُرتبط بدرجة أَساس، بمستوى التطور الذي يوجد في مؤَسسات الدولة والمؤسسات الخاصة على حدٍ سِواء، فإِذا ما تم تقييم درجة التطور الموجودة في هذه المؤَسسات نجدها بدرجة محدودة وهي لا تُضاهي التقدُم الحاصل في بعض الدول المجاوِرة، لذلك لا جدوى مِن تطبيق نِظام الحوكمة الرقمية في ظل التخلُف وبطء التطور الذي تشهدهُ مؤَسسات الدولة، ناهيك عن نشاطات القطاعات الأَخرى وهي ما زالت تُعاني في الكثير مِن مفاصلها تخلُفاً في الوسائل والآليات[8].
3. إِنَّ معوقات تطبيق النِظام الالكتروني في العِراق تعتمد على مِحورين: المِحور الأَول هو البيئة والتشكيلة السياسية في العِراق وأَثرها على الوضع الراهن، لاسيما وأَنَّ مِن أَهم مفاصل الانترنت هو عدم وجود الكهرباء، ثانياً ثقافة الشعب العِراقي وهي تحتاج لبرامج مُعينة قد تستغرق فترات زمنية لاحقة خصوصاً وأَنَّ العِراق هو في عِداد المُستهلك لِكُل شيء وغير مُصدَّر[9].
4. **النِظام السياسي:** إِنَّ الحكومة الالكترونية هي نموذج جديد للعلاقة الأَفقية والعمودية، خصوصاً وان العلاقة الأَفقية هي عِبارة عن العلاقة بين الجمهور ومؤَسسات الدولة، والعلاقة العمودية هي علاقة بين مؤَسسات الدولة القطاع العام ومؤَسسات القطاع الخاص والأَهلي، فأَنَّ التحدي الحقيقي يكمنُ في وجود إِرادة نِظام سياسي يسعى إِلى سد الفجوة بينهُ وبين الجمهور، ويهتم كثيراً بسهولة وشفافية وصول الجمهور لمؤَسسات الدولة.
5. **النِظام القانوني والبيروقراطي:** إِنَّ التحدي الأَكبر والحقيقي الذي يقف أَمام تطبيق الحوكمة الرقمية في العراق هو النِظام البيروقراطي المعمول بِه ووجود النظام القانوني الذي عفى عليه الزمن، هذا النِظام في الكثير مِن مفاصلهُ يقف بالضد مِن الانتقال إِلى الحكومة الالكترونية، فعلى سبيل المِثال البطاقة الوطنية إِصدار حكومي لكن النِظام المعمول بِه في الدولة يرفض التعاطي مع هذا النموذج الجديد، ويسعى أَيضاً إِلى

محاولة التشبُث بمشروع جلب المُستمسكات الرسمية الأَربعة، هذا الأَمر يحتاج إِلى إِعادة النظر بسلة القوانين التي تحكُم الوزارات العِراقية جميعاً، وأَيضاً الجِهات غير المُرتبطة بوزارة، بل الأَدهى مِن ذلك هو عدم وجود تشريع حكومي يهتم بتطبيق الحوكمة الرقمية في العِراق[10]. أَضف إِلى ذلِك هُناك مسالة اعتاد عليها المسؤَول الإِداري في العِراق، وهي محاولة تاليه المسؤَول الإِداري والوقوف أَمام مكتبهُ ومحاولة الثناء عليه مِن أَجل تمشية مُعاملاتهم، وهو غير مُعتاد على تقبُل ثقافة عدم وجود المحسوبية، أَيضاً هُناك سبب أَخر يتعلق بتخلُف القوانين خاصةً قانون الاستثمار هذا القانون نفسهُ هو أَحد معوِقات الاستِثمار في العِراق لأنه ينص مثلاً على وجود النافِذة الواحِدة فما الغاية مِن وجود هذا النص، وبالمُقابل ليس هُناك من ربط بين سلطة اتخاذ قرار رخصة المشروع الاستثماري، لذا لا بُد مِن الذهاب نحو الدولة الرشيقة والمرنة، وأَنَّ لا نكون أَسرى للدولة الجامِدة التي مِن طبيعتها العمل على ضرب مصالح الناس، وهي بطبيعة الحال دولة غير مُنتِجة، فالحكومة الالكترونية حكومة تهتم بالناس وتهتم بالوقت، وهي تسعى إِلى المزيد مِن الإِنتاجية وتستثمر الوقت[11].

6. **تواضع الجهود الحكومية نحو تحقيق الأَهداف وغياب الإِرادة السياسية نحو تطبيق الحوكمة الرقمية؛** على الرغم مِن التراجُع في مستوى الخدمات وعدم الاستقرار الأَمني في العِراق فلا زالت الجهود الحكومية العِراقية متواضعة نحو تحقيق التنمية الحقيقية وتوفير مُتطلبات الحوكمة الكفؤة في البلد[12] فنِظام الحوكمة الرقمية بِما يتيز بِه مِن آليات يصل إِلى درجة عالية مِن الشفافية مِما يجعل كُل أَعمال الحكومة مكشوفة أَمام المواطنين لذلك هذه الإِرادة السياسية الحالية تعمل بالضد مِن وجود النِظام الإِلكتروني.
7. **تدويل المؤَسسات:** تُعد تدويل المؤَسسات الحكومية مِن أَخطر وأَكبر المُعوِقات التي تواجه تحقيق الأَهداف التنموية في العِراق، أَي أَنَّ أَغلب المؤَسسات أَصبحت أَشبه بدول لها قوانينها الخاصة التي تختلف في داخلها عن الاخرى وسيطرة حزب أَو جِهة مُعينة على كُل مؤَسسة ووزارة والتي تؤَدي بالنتيجة إِلى ظهور عدم التعاون والنسق التشارُكي بين هذه الجِهات[13].

8. بروز تحديات أُخرى تكمنُ في غياب التخطيط الاستراتيجي السليم، وغياب الاستِقرار السياسي.

ثالثا: تحديات اقتصادية

1. انتِشار الفساد الإداري والمالي:

يُمثل الفساد ظاهرة مُتجذرة منذُ نشوء الدولة العراقية وغِلى يومنا هذا، لكنها في الحقيقة تتميز بالتذبذب وعدم الاستقرار، في حين مثلت حقبة ما بعد عام2003 تحولاً تاريخياً لتلك الظاهرة، لأنها اضحت مُشكِلة عامة برزت بشكلٍ كبير في اثناء الاحتلال الأَمريكي للعراق وبعدهُ، وتمثلت مِن خلال سرقة المال العام أَمام الضعف الواضح في الرقابة الحكومية، مع تراكُم المشاريع الوهمية التي نفذتها شرِكات وهمية أَيضاً، حتى أَصبح ثقافة ظاهرة تارةً، وبُنية محمية تارةً اخرى[14]. ولا يختلف اثنان في القول، إِنَّ انتشار الفساد يضعف الجهود الحقيقية نحو تحقيق التنمية وتوفير الخدمات المُجتمعية بصورة كامِلة، ويُعد مِن أَبرز المُسبِبات لكثير مِن الأَزمات في العِراق والتي مِنها الخلل الأَمني أَيضاً. وعادةً ما يرتبط ظهور الفساد بغياب الحوكمة الرقمية، وينتج عنه العديد مِن الآثار السلبية والخطيرة، فانتِشار الفساد الناتج عن غياب الحوكمة الرقمية يعمل على هروب الاستثمارات الأَجنبية، إِلى جانب ذلك فان للفساد تكاليف اقتصادية أَخرى، مِنها انخفاض الإِنفاق الحكومي على المشاريع الاجتماعية، وزيادة سوء تخصيص الموارد، والتحدي الأَكبر الذي يواجه مُطبق الحوكمة هو اتساع نطاق الفساد ليشمل الأَجهزة الحكومية المسؤَولة أَساساً عن مُحاربة الفساد، لان الحكومات الفاسِدة دائماً ما تقف في وجه الإِصلاحات التشريعية، وذلك لحرصهم على استِمرار المناخ الفاسد الذي يمنحهم مكاسب كبيرة[15]. وفي هذا السياق يقول رئيس مركز مؤسسة النهرين لدعم الشفافية، محمد الرُبيعي "أَنَّ "القوى الفاسِدة تحاول إِبقاء التعامُل الكلاسيكي البيروقراطي في دوائر الدولة بِما يُعزَّز حضورها غير الشرعي في استهلاك المال العام، وصعوبة مُراقبة حركة العقود المالية والاستثمارية وغيرها مِن المنافذ التي تدر الأَموال"[16].

وقد أَقرت هيئة النزاهة العِراقية المُرتبطة بالبرلمان في عام2018 بأَنَّ العِراق فقد بسبب الفساد الحكومي نحو(320) مليار دولار في السنوات الخمسة عشر الماضية للعام المذكور. وقد تسلمت مِنذُ إِنشائها قبل عدة أَعوام الاف القضايا المُتعلقة بالفساد، بلغت

في الربع الأَول فقط مِن هذا العام (9832) حُسِم منها (4443) قضية. ففي عام2017 حل العِراق في المركز (169) بين (180) دولة على مؤَشر الفساد الذي تنشرهُ مُنظمة الشفافية الدولية. ويُصنف مؤَشر إِدراك الفساد البُلدان والأَقاليم على أَساس مدى فساد قطاعها العام[17]. وهذا ما جعل (مُنظمة الشفافية الدولية) تضع العِراق على قائمة الدول الأَشد فساداً، وكما مُبين في الجدول رقم (1).

الجدول ذو الرقم (1) يُبين مؤَشر مُدركات الفساد للأَعوام 2003-2022

السنة	عدد الدول المُشتركة	تسلسُل العراق	السنة	عدد الدول المُشتركة	تسلسُل العراق
2003	130	113	2013	177	171
2004	146	129	2014	175	170
2005	194	170	2015	168	161
2006	163	160	2016	176	166
2007	180	178	2017	180	169
2008	180	178	2018	180	168
2009	180	176	2019	180	162
2010	178	175	2020	180	157
2011	183	175	2021	180	160
2012	176	169	2022	180	157

الجدول مِن إِعداد الباحث بالاعتماد على: مُنظمة الشفافية الدولية، مؤَشر مُدركات الفساد، مُتاح على الرابط:

https://www.tr.coansparency.org/country/IRQI

وعليه، يظل القضاء على الفساد واحِداً مِن أَكبر التحديات التي تواجه العِراق وتطبيق الحوكمة الرقمية، والذي انعكس أَثاره على الاداء المؤَسسي الحكومي وعلى كفاءة تنفيذ برامج التنمية[18].

وفي ضوء تِلك التحديات كان لزاماً التوجه نحو إِصلاح حقيقي ومُكافحة الفساد، وعليه تعد مسالة وجود رقابة داخلية أَمراً حيوياً ومُهِماً لأي دولة، إِذ لا تكون الحوكمة الرقمية فاعِلة بدون نظام فعال للرقابة الداخلية.

2. محدودية قدرات القطاع العام وانخفاض نسبة التعامُل والتعاون بين مؤُسساتهُ

فضلاً عن ضعف العلاقة بين القطاع العام والخاص وضرورة تدعيم التشاركية بين القطاعين: وكما يندرج موضوع الثقة بين المواطن والحكومة في بوتقة الإِنجاز التنموي الفعال، يذهب موضوع الثقة والتعاون بين القطاع الخاص والعام (الحكومي) أَيضاً في الحيز نفسه، فهُناك هروب كبير للاستثمارات ورؤَوس الأَموال إِلى خارج العِراق في العقد الأَخير بسبب تراجُع الثقة بين القطاع الخاص والعام، ومِما زاد الوضع تأَزماً هو ضعف الجهود الداعِمة

حكومياً للقطاع الخاص في العِراق، فالدول المُتقدِمة توظف القطاع الخاص مَن أَجل تحقيق استثمارات وتقليل الإنفاق العام وتحقيق التنمية الحقيقية في البلد، لكن للأَسف قد تراجع دور القطاع الخاص في العقد الأَخير حتى يُكاد أنَّ يختفي مِن الناتج المحلي الإجمالي الذي كان يُقارب الثلث من إجمالي الناتج الإجمالي المحلي قبل عام 2003[19].

3. ضعف استِخدام التكنولوجيا المالية:

يُعاني العِراق مِن ضعف في استِخدام التكنولوجيا المالية، فعلى الرغم مِن انتِشار استخدام الهاتف النقال بشكلٍ واسع، إذ بلغت نسبة مُستخدمي الهاتف النقال أَكثر مِن (96%)، لعام 2019، بينما بلغت نسبة مُستخدمي الانترنت ما يُقارب(50%) مِن إجمالي السُكان، لكن لا زال استخدام التكنولوجيا المالية محدودة قياساً إلى عدد مُستخدمي الهاتف النقال، وحسب إحصائيات عام 2018 بلغ حجم التحويلات المالية ما يُقارب(400) مليون دينار عراقي فقط مِن خِلال الهاتف النقال، وهو مبلغ ضئيل، يعكس ضعف السياسات الحكومية في نشر وتوفير البُنى التحتية سِواءً كانت قوانين أَو مؤَسسات مُتخصِصة في تعزيز الشمول والتنمية المالية ومِن ثُم تعزيز التكنولوجيا المالية[20].

4. **غياب البُنى التحتية وقلة الكوادر المُتخصِصة** في إدارة نِظام حكومي الكتروني ناجح في العِراق.

ان الدخول في العِراق لا زالت لا توجد فيها عدالة وهذا مِما يؤثر بشكلٍ كبير على استخدام الانترنت. كما انه مِن أَجل تطبيق الحوكمة الرقمية في العِراق فانه لا بُد مِن إصلاح النِظام المصرفي كي نُسدد الرسوم والأَجور التي تطلبها الحكومة.

رابعا: تحديات اجتماعية

1. **قلة الوعي المُجتمعي:** يُعد الوعي مِن النقاط المُهِمة في تعزيز الحوكمة الرقمية في العِراق، فكُلما أَرتفع مؤَشر الوعي والإدراك المُجتمعي بأَهمية المشروع الحكومي كُلما تزايدت فرص النجاح والإنجاز، ولاسيما إذا ما علمنا ان مفهوم الحكومة الالكترونية مفهوم

حديث على أَسماع العِراقيين يحتاج إلى تثقيف إعلامي واسع لهذا المفهوم والفوائد المتوخاة منهُ[21].

2. **الثقافة الاستهلاكية للفرد العِراقي وغياب ثقة المواطن بالوسائل الحديثة** هذا مِما جعلهُ عازِفاً عن اللجوء إلى مثل هذه الأَنظمة.

وعليه، إنَّ ما نحتاج إليه هو جهود حثيثة أَكثر مِن القطاع الحكومي مع توفر وعي مُجتمعي عالي، فلا يمكن الوصول إلى تنمية حقيقية دون وجود هذه العوامل المُساعِدة، وهو ما يفتقر له العِراق أخيراً.

المحور الثاني: فرص التحول نحو الحوكمة الرقمية في العِراق

إنَّ الهدف الرئيسي مِن تطوير المؤسسات والقواعد الحاكِمة هو الوصول إلى الحوكمة الموجهة للتنمية، بحيث يتم الارتقاء بحياة الفرد. فالحوكمة الرقمية تتطلب قيادة تنمية بشرية شامِلة قائمة على أَساس خياراً ديمقراطياً حراً بعيداً عن دائرة التأَثير، وبذلك تكون الحوكمة هي الإدارة الجيدة لجميع المؤَسسات في الدولة مِن خِلال سياسات وآليات ومُمارسات تقوم على الشفافية والمُشاركة والمُساءلة وسيادة القانون ومُكافحة الفساد وتسعى لتحقيق العدالة وعدم التمييز بين المواطنين والاستجابة لاحتياجاتهم وتتحرى الكفاءة للوصول بالسياسات والخدمات لأَعلى مستوى مِن الفعالية بشكلٍ مرضي للجميع. فهل تعي المؤَسسات العراقية أَهمية العمل بنظم الحوكمة الرقمية فيها؟، وهل تقف قناعات الإدارات العليا للقطاعين العام والخاص على فوائدها وعوائدها؟، وهل وفّرت الأَجهزة المعنية بتنظيم البُنى التحتية الرقمية في البلاد مُتطلباتها؟، وهل تقف ضرورات فهمها عند المُختصين بتكنولوجيا المعلومات في تلك المؤسسات، دون بقية الإدارات العُليا والتنفيذية والرقابية؟، وهل وظّفت الأجهزة الرقابية آلياتها وأدواتها على وفق ما تستدعيه الحاجة إلى العمل بقواعد الحوكمة، بوصفها آليات تنظيم مسارات الأعمال في المؤسسات والرقابة عليها، وبِما يفضي إلى الارتقاء بمستويات الخدمة والإنتاج؟.

وعليه وبعد عرض أَبرز التحديات التي مِن المُمكن أنَّ تواجه العِراق للتحول رقمياً، فإنَّ السؤَال المطروح، ما هي الحلول المُمكِن اتخاذها لمُعالجة تلك التحديات والسير قدُّماً لتطبيق الحوكمة الرقمية؟، لا شك إنَّ هذه الميزة (الرقمنة) تُقدَّم أَيضاً مجموعة مِن الفرص

والحلول لتحسين العمليات الحكومية، وتقديم الخدمات ودفع عجلة التنمية الاقتصادية وتحقيق الحوكمة الرقمية في العِراق، والتي تم إِيجازها بالفقرات الآتية:

أولاً: فرص ثقافية - تكنولوجية

1. **توفير خدمة الانترنت:** إِنَّ أَهم أَسُس تقدُم الحكومة الالكترونية والحوكمة الرقمية هو ان تتوفر خدمة الانترنت العالي، وأَيضاً ان تستخدم نسبة عالية مِن الناس الانترنت وأَنَّ يكون هُناك تطور في رسم الاتصالات السلكية واللاسلكية، والغريب ان العِراق أَطلق حكومة المواطن الالكترونية من دون أَنَّ يوفر كُل تلك الأَسُس[22]. لكن مع ذلك نما المشهد الرقمي في العِراق بثبات على مدى السنوات القليلة الماضية، مع زيادة عدد الأَشخاص الذين يستخدمون منصات مُختلِفة، بِما في ذلك التجارة الإِلكترونية، والبنوك، وتوصيل الركَّاب، وتوصيل الطعام، وغيرها مِن الحلول الرقمية. لقد أَبرزت جائحة كوفيد-19 أَهمية التحوُّل الرقمي في العِراق، مع حاجة الشرِكات والمؤَسسات إِلى التكيُّف مع العمل عن بُعد والتواصل عبر الإِنترنت. لقد اعترفت الحكومة بهذه الحاجة وتعمل نحو تحسين البُنية التحتية الرقمية وتوسيع وصول الإِنترنت على مستوى البلد. أَصبح التحول الرقمي أَمراً بالغ الأَهمية للشرِكات والمؤَسسات للبقاء في المُنافسة. على الرغم مِن تحديات البُنية التحتية والمعرفة الرقمية، يوفر العِراق فُرَصاً كبيرة للنمو والابتكار الرقمي. ومع ذلك، فإِنَّ الاستِثمارات الاستراتيجية في التكنولوجيا والتعليم ضرورية للتقدُم المُستدام والإِدراج الرقمي. وبكونها أَكبر مزوِّد لخدمة الإِنترنت في العراق، لعبت شركة ايرثلنك للاتصالات دوراً مُهِمّاً في تعزيز الثورة الرقمية مِن خِلال تحسين الاتصال ووصول الإِنترنت للملايين مِن الناس في البِلاد، مِما ساعد الشرِكات على الازدهار، ومكَّن الطُلاب مِن الوصول إِلى تعليم أَفضل، وسهَّل التواصل بين الأَصدقاء والعائلة، مِما يُعزِّز النمو الاقتصادي ويُحسِّن العلاقات الاجتماعية في العِراق[23].
2. **توقيع مُذكرات تفاهُم رقمية:** وقع العِراق في تموز/يوليو2022، مع برنامج الأُمم المُتحدة الإِنمائي، مُذكرة تفاهُم لتعزيز الخدمات الرقمية وبِناء القدرات في مجال الحوكمة الإِلكترونية، ركزت على تسخير وزيادة استخدام تكنولوجيا المعلومات والاتصالات لتحديث العمليات والأَنظمة الحكومية وتحسين الخدمات للمواطنين وتعزيز الاقتصاد

الرقمي. ووفقاً للأَمانة العامة لمجلس الوزراء، استطاعت الحكومة العِراقية عبر مشروعها التنفيذي مِن رفع أَكثر مِن (75) ألف وثيقة إِلكترونية وجعلها متداولة أَمام المُستخدمين لتِلك المواقع[24].

3. **إِطلاق المشاريع الرقمية:** أَطلقت الحكومة العِراقية في ايار/مايو2021، بوابة إِلكترونية تُسمى" بوابة أَور للخدمات الحكومية"، يشرف عليها مركز البيانات الوطني في الأَمانة العامة لمجلس الوزراء. وهي موقع إِلكتروني يتيح وصول المواطنين إِلى الخدمات الإِلكترونية التي تُقدمها وزارات الدولة والدوائر غير المُرتبطة بوزارة، عبر نافذة واحِدة، وتُعّدٌ مِن العناصر الأَساسية في مشروع الحوكمة الرقمية. وأَطلقت بغداد، عام2014، مشروعاً تحت اسم "حكومة المواطن الإِلكترونية"، بالتعاون مع الوكالة الأَميركية للتنمية الدولية(USAID)، في أَول إِعلان عن عزم العِراق على التوجه نحو الحكومة الرقمية، لكن المشروع تعثر مرات عدة ولم يكتمل[25].

4. **تدعيم نظام الحكومة والحوكمة الالكترونية :** يُعد برنامج الحكومة الالكترونية عنصراً فعالاً في تطوير عمل القطاع العام في العِراق، وسعى العِراق نحو تنفيذ سياسات مُتقدِمة بشأَن الحكومة الالكترونية والتي تعد أَداة مُهِمة يمكن أَنَّ تُعزز الشفافية والمُساءلة وتحقيق المساواة والعدالة الاجتماعية للوصول نحو اقتصاد متنوع مبني على أَساس المعرفة (الحوكمة الرشيدة). ولاسيما بعد أَنَّ تزايدت أَهمية الخدمات الإِلكترونية والرقمية في عصرنا، حيثُ أَنها توفر العديد مِن المزايا للمؤَسسات والجِهات في تحسين جودة الخدمات وتقليل الأَخطاء(*). ولأَهمية موضوع الحوكمة انبثقت مِنها آليات مُشتركة تُساهم في تحقيقها، مِنها الحوكمة الالكترونية، والتي تعني استِخدام تكنولوجيا المعلومات في إِنجاز المُعاملات وتقديم الخدمات المرفقية وكذلك استخدام وسائل الاتصال لتحسين وتعزيز ركائز الحُكم الرشيد[26]، وهو مفهوم يختلف عن الحكومة الالكترونية التي تعني استخدام التكنولوجيا والمعلومات والاتصالات مِن أَجل تقديم الخدمات الحكومية للمواطنين وقطاع الأَعمال ومؤَسسات المُجتمع المدني، ويُشير هذا المفهوم إِلى استِخدام نتائج ثورة المعلومات والاتصالات مِن هاتف وفاكس وحاسوب وانترنت وغيرها، وذلك لتقديم خدمات حكومية ذات جودة وكفاءة وفعالية إِضافة إِلى تسهيل عملية الوصول إِلى المعلومات وتفعيل دور المواطن إِزاء المُشاركة في عمليتي الرقابة والمُساءلة. وبالتالي تفترض الحكومة

الالكترونية وجود علاقة بين (المؤسسات الحكومية- المؤسسات الحكومية، المؤسسات الحكومية-المواطن، المؤسسات الحكومية- القطاع الخاص، المؤسسات الحكومية- الموظف)[27]. **وهذا ما تم توضيحه في الشكل ذور الرقم (1) والشكل ذو الرقم (2).** وينبغي لتدعيم نِظام الحوكمة الالكترونية وتسهيل تطبيقهُ الاهتمام بموضوعات مُتعددة ذات صلة وطيدة به، مِن ذلك البُنية التحتية للاتصالات الالكترونية، والبطاقات الائتمانية، وتأَمين المعلومات ومُكافحة القرصنة الالكترونية، وتنظيم التجارة الالكترونية، وعلى الرغم مِن صعوبة تطبيق الحوكمة الالكترونية، بيد أَنَّ هذا النِظام فرض نفسهُ على مُختلف دول العالم التي تُريد أَنَّ تُساير الركب وتتعايش مع الأَخرين، ذلك لان إِنجاز الأَعمال أَو تأَدية الخدمات بطريقة الكترونية يُحقق جودة الأَداء ويوفر الجهد المبذول، وبذلك أَصبحت الحكومة الالكترونية حتمية يجب السعي لتطبيقها في كُل دولة عصرية تُريد أَنَّ تواكب تطورات عصر الثورة الرقمية ولا تتخلف عن نهضة المعلومات العالمية[28].

الشكل ذو الرقم (1) يُبين بعض أنواع الخدمات الالكترونية

الشكل ذو الرقم (2) يُبين بعض أنواع الخدمات الرقمية

1. **مُكافحة الأمية الالكترونية:** إذ أنَّ هُنالك عدداً مِن المواطنين الذي لا يُتاح لهُم التعامُل مع الكمبيوتر أَو الدخول على شبكة الانترنت لأَسباب تعليمية أَو اقتصادية، وهو ما يُسمى بالفجوة الرقمية، وللتغلُب على هذا العائق ينبغي إِدخال مادة الكمبيوتر ضمن منهاج التعليم العام، واتاحة فرص الحصول على أَجهزة كمبيوتر مُنخفِضة لتكون في متناول عامة الناس ومُكافحة أُمية الانترنت وتدريب الشباب الخريجين على استخدام الكمبيوتر[29].
2. **إِعداد الكوادر المؤَهلة:** إِعداد الكوادر المؤهلة الكافية مِن الموظفين والفنيين للتعامُل مع نِظام الحكومة الالكترونية، وذلك سِواءً عن طريق التعيين أَو إِعادة التدريب والتأَهيل، إِذ لا شك أَنَّ العنصر البشري هو المُحرك الفاعل أَو المُبدع لأَجهزة التقنيات الالكترونية.
3. **استخدام أَدوات الدفع الالكتروني:** شهد العِراق في الفترة الأَخيرة تطوراً في استخدام أَدوات الدفع الالكتروني، إِذ يتجه العِراق نحو استِخدام تِلك الأَدوات لإِصلاح الاقتصاد، وسحب النقد الموجود داخل المنازل باتجاه القطاع المصرفي، ومُكافحة الفساد المالي والإِداري داخل المؤَسسات الحكومية[30] ويوضح رئيس مجلس المسار الرقمي العِراقي صفد الشمري في حديث لـ(المدى)، ان "موضوع الأَتمتة مشروع مطروق على الصعيد العالمي، مِنذُ مُنتصف القرن العشرين، فالأَتمتة هي أَنَّ تدخل في قطاعات الأَعمال بشكلٍ عام، لكن ما علاقة الأَزمة بالرقمنة؟، مُستدرِكاً حينما صارت الأَدوات الرقمية

بالذات بعد الثمانينيات القرن الماضي هي بديلة الأَجهزة، فبالتالي أَصبحت الأَزمة اليوم تعني بالرقمنة، وهي أن تدخل الأَجهزة الرقمية لقطاعات الأعمال المختلفة، وكُل أَجهزة الدولة، وفي كُل أجهزة القطاع الخاص". وأَشار إلى ان "المُشكِلة في العِراق أنَّ هذه الإدخالات التي وضعت الأتمتة لا تتم بالضرورة بصورة صحيحة أو منهجية، وكان مِن المُفترض ان تعمل على التعاون الرقمي الذي يتطلب مِنك أن تقوم على وفق مبادئ مُعينة"[31].

4. ضرورة الإسراع بتحويل كُل عُمل الدولة العِراقية إلى إلكترونية، وبهذا سيحدُ بشكلٍ كبير مِن عمليات الفساد وابتزاز المواطنين، فضلاً عن انه يلغي الروتين القاتل في تمشية المُعاملات اليومية. فضلاً عن أَهميَّة الاستفادة مِن التطور التكنولوجي والثورة المعلوماتية؛ بغية التحوُّل الرقميّ والحوكمة الإلكترونيَّة لدورها في مُكافحة الفساد، وتوفير الجهد وسرعة إنجاز الأَعمال وتخفيض التكاليف، وتحقيق النزاهة والشفافية الإداريَّة في مُؤسَّسات الدولة كافة[32].

5. **التشبيك الرقمي والحكومة الالكترونية:** حينما نتحدث عن حكومة إلكترونية، فإنها ليست نِظاماً رقمياً مُمكناً إنجازهُ خِلال اليوم أَو يومين أَو سنة أَو سنتين، ومِن ثُم تعمل عليه الحكومة الرقمية مِن دون تشبيك رقمي بين الوزارات، وبالتالي عندما نتحدث عن حكومة إلكترونية من دون تشبيك معناهُ إنهُ سوف لن يكون لدينا حكومة إلكترونية لِمُدة 50 سنة تقريباً، فبالتالي علينا أَنَّ نتحرك على التشبيك ومِن ثُم تنتقل إلى موضوعة الحكومة الإلكترونية[33]. فهناك مفهوم آخر يجري الحديث عنهُ، وهي الحوكمة الرقمية، واليوم الحوكمة هي نِظام رقابي على الأَداء التنفيذي، والمُفترض أَنَّ لديه أَداء مُعين أَو أَنَّ تقوم بمُراقبتهُ مِن خِلال الحوكمة، وحينما يُعلن عن إنجاز حوكمة رقمية الاتجاه، فيجب ان تكون لدينا حكومة الكترونية حتى تتحقق الحوكمة، وبالتالي فماذا ستُراقب إذ لم يكُن لدينا حكومة الكترونية؟ فما يجري اليوم هو عملية أتمتة وليست حوكمة، وموضوعات الاشتراكات التي تتعرض لها جِهة الدولة ووزارات الدولة، وتعود إلى عدم وجود مجلس أَعلى أَو هيئة عُليا للأمن السيبراني في العِراق، إذ يجب أَنَّ يكون لدى الحكومة ردع سيبراني لهذه الوزارات[34]. ومِن ثُم فان الحكومة العِراقية عليها تطبيق الحوكمة والتحول الرقمي وأَنظمة الأتمتة لتحقيق عدة أَهداف، ومِنها الشمول المالي، والتحول المالي نحو

الحكومة الإلكترونية. فهُناك تعامُلات إلكترونية بدل التعامُلات الورقية، وهذا هو جزء مِن التحول العالمي لاقتصاد المعرفة، وأيضاً المعلومات الذكية والأَمن السيبراني لتشمل التحول الرقمي وكُل المجالات وليس فقط في المجالات النقدية وإنما أَيضاً بمستوى تقديم الخدمات وفق حكومة إلكترونية. كما أَنَّ هُناك أَيضاً التعامُلات الورقية التي تحولت إلى تعامُلات الكترونية، وهذا طبعاً مِن شأَنهُ أَنَّ يخلق ثورة إلكترونية في العِراق، وإصلاح اقتصادي شامل بتطبيق الشمول المالي، وأَيضاً تطبيق برامج الكترونية حديثة تُسهِم بِمُكافحة الهدر والفساد في المال العام.

ثانيا: فرص سياسية-قانونية

1. **إصدار التشريعات اللازمة:** لم تعد التشريعات الموجودة ما قبل الثورة الرقمية صالِحة لِمُسايرة التطور الالكتروني وتحقيق الأَهداف المرجوة، وظهرت الحاجة إلى تطوير هذه التشريعات لتتوافق مع نِظام الحكومة الالكترونية، بِما يتضمن ذلك مِن تنظيم عملية التعاقُد مِن خِلال شبكة المعلومات وتنظيم عملية التوثيق الالكتروني(35).
2. **مُكافحة الفساد الإداري والمالي:** لا يختلف اثنان في القول، إنَّ واحِدة مِن أَهم مُتطلبات تطبيق الحوكمة الرقمية في العِراق هو وجوب مُكافحة الفساد أَو الحدِ منه، وفي الأَغلب الأَعم يرتبط ظهور الفساد بغياب الحوكمة، وبغية القضاء على ظاهرة الفساد يتوجب اتباع استراتيجيات الحوكمة في إِطار عمل مؤَسسي يسعى إِلى مُكافحة الفساد بِكل صورهُ ومظاهرهُ وتسريع عجلة التنمية(36).
3. **دِراسة تجارب الأَخرين:** إِنَّ نِظام الحكومة الالكترونية حديث، لذلك هو بِحاجة إِلى الكثير مِن الدِراسات والتساؤَلات، ومِن المُفيد لنجاح تطبيقات ذلك النِظام التعرُف على أَكبر قدر مِن المعلومات عن تجارب الأَخرين في هذا المجال، وأَبرز الإِنجازات المُتحقِقة جِراء تطبيق الحكومة الالكترونية، فضلاً عن دِراسة العقبات التي تواجه تطبيقها.
4. **سن قانون يُسمى قانون المواطن،** وهو يتضمن إِلزام جميع الدوائر أَنَّ تنتقل إِلى الوضع الالكتروني، وأَنَّ تُحدِد مُدة لإِنجاز المُعاملة والرد على المواطن بالسلب

أَو الإيجاب، وأَنَّ يُناقش هذا القانون على مستوى المراكز البحثية قبل الذهاب للحكومة وحتى لا ينحرف عن مسارهُ وكي نجعل من الحكومة عنوان لخدمة المواطن وليس العكس[37].

ثالثا: فرص اقتصادية

أَدى التطور السريع للتقنيات الرقمية إلى ظهور ظاهرة "الاقتصاد الرقمي" والأَخير هو اقتصاد يقوم على التقنيات الرقمية والمعلوماتية والاتصالات، إذ تؤثر التحولات الرقمية على جميع المجالات الإنتاجية وكذلك على النشاط الاقتصادي والاجتماعي، والخدمات اللوجستية، والتسويق، خدمات الإدارة العامة. ويوفر الاقتصاد الرقمي التفاعُل بين مؤَسسات الأَعمال في مجالات كثيرة مثل إنشاء واستِخدام تقنيات ومُنتجات جديدة، وخدمات الاتصالات، والأَعمال التجارية الإلكترونية، والتجارة الإلكترونية، والأَسواق الإلكترونية، والخدمات عن بُعد. لذلك يعد الاقتصاد الرقمي أَحد الأَسباب الرئيسية للانتقال إلى الثورة الصِناعية الرابِعة. لكن على الصعيد المحلي يُعاني العِراق -كما سبق القول- مِن ضعف في استِخدام التكنولوجيا المالية، فما هي الفرص الاقتصادي :

1. هُنالك حاجة ماسة لدعم سياسات محو الأمية المالية ونشر المعرفة المالية مِن خِلال وزارة المالية والبنك المركزي العِراقي ومُنظمات المُجتمع المدني والمؤَسسات ذات العلاقة، بِما يُساهم في نشر الخدمات المالية لِكُل فئات المُجتمع وهذا سوف يُساهم في مواجهة البطالة ودعم النمو والتنمية الاقتصادية ورفع المستوى المعيشي لكافة أَفراد المُجتمع[38].ففي عصر الثورة الرقمية والثورة الصِناعية الرابعة، يعد تطوير صناعة التكنولوجيا المالية العِراقية أَولوية. هذه الصِناعة ذات أَهمية كبيرة لأنها تُساهم في نمو الرفاهية والتقدُم الاجتماعي والاقتصادي. لذلك، هُناك حاجة إلى دعم شامل لتطوير التقنيات المالية الرقمية الجديدة. أَدوات هذا الدعم هي دعم إنشاء وتنفيذ الابتكارات المالية الرقمية، وتحفيز الشرِكات الناشئة الرقمية، ودعم الشرِكات في تنفيذ التقنيات المالية الرقمية، وتشكيل سوق رقمية. ومِن وجهة نظر القطاع الخاص، يؤَدي استخدام التقنيات الرقمية وتطويرها إلى خفض التكاليف وزيادة مستوى الربحية والتكيُف بشكلٍ أَفضل مع مُتطلبات السوق. ومِن المتوقع ومِن خِلال تسريع تطبيقات الذكاء الاصطناعي، بالإضافة إلى التقنيات الرقمية

الأَخرى، والتي سيتم استخدامها، إلى جانب البيانات الكبيرة، يمكن التنبؤ بتفضيلات المُستهلك، وتعزيز الأمن السيبراني، وتحسين كفاءة كُل مِن الشرِكات المالية التقليدية والرقمية.

2. إمكانية زيادة الكفاءة والإنتاجية وخلق فرص عمل؛ تتمثل إحدى الفوائد الرئيسية للتحول الرقمي في القدرة على تبسيط العمليات وأتمتتها، ومِن هُنا فإِنَّ اعتماد العِراق للتكنولوجيات الرقمية والاستثمار فيها لديه القدرة على تحقيق مجموعة مِن الفوائد، بِما في ذلك تحسين الكفاءة والإنتاجية في العمليات الحكومية مِن خِلال الاستفادة مِن التقنيات الرقمية مثل تحليلات البيانات والأتمتة، وتعزيز تقديم الخدمات العامة، وزيادة الشفافية والمُساءلة، ويمكن مُتابعة هذا خِلال اتباع وزارة الداخلية في إِصدار البطاقة الموحدة ووزارة التجارة للبطاقة التموينية (الغذائية). ويمكن للحكومة العِراقية تقليل الوقت والموارد اللازمة لإِكمال المهام، مِما يؤَدي إِلى توفير التكاليف واستِخدام أَكثر فعالية للموارد. ومع ذلك، يجب مُراعاة البُعد الأَخلاقي في خضم الاستِفادة مِن تقنيات الذكاء الاصطناعي[39].

3. لا بُد مِن تحرير الاقتصاد ووضع الضوابط المُناسِبة، وأَنَّ تكون لدينا تجارب شعبية لتدعيم واقع النظُم الالكترونية وأَنَّ تبدأَ الحركة مِن الناس وليس مِن الحكومة.

4. مِما سبق دعونا نقول، إِنَّ للحوكمة الرقمية مسارات عديدة أَهمُها، مسار الاصلاحات الاقتصادية، أَي تحديث القطاع العام، والشراكة بين القطاعين العام والخاص، وتبني نهج الحكومة الالكترونية. ومسار النفاذ إِلى العدالة، أَي الدستور وحقوق الإِنسان والقضاء الصالح، ومسار الإِصلاح المؤسساتي مِن خِلال الرسوم الجمركية واللامركزية وإِعادة تنظيم الإِدارة، وأَخيراً مسار إِشاعة ثقافة حقوق الإِنسان وتطبيق النزاهة والشفافية في الوظيفة العامة، وتقوية الرقابة والمُساءلة في أَداء الخدمات العامة.

الخاتمة

يتجه المُجتمع الحديث بسرعة نحو الثورة الصِناعية الرابعة وما يدعى عصر الرقمنة، إذ تدخل البيانات وتتسرب التكنولوجيا إلى كُل شيء. إنَّ التحوُّل الرقمي هو عملية تبنّي التقنيات الرقمية ودمجها في نماذج الأَعمال، وبالتالي صنع نماذج جديدة للأَعمال تُعيد تشكيل الأَسواق على نحوٍ أَسرع مِن أَي وقت مضى. إذ أَدى التحوُّل الرقمي إلى تعطيل الأَعمال التجارية التقليدية باستِخدام تقنيات أَو مُنتجات أَو خدمات وعمليات مُبتكرة. لقد سمح للكثيرين باستكشاف الفجوات المُتبقية في السوق وخلق حلول لها، لتصبح مصدراً مُستمراً لريادة الأَعمال.

وتعد الحكومة الرقمية أَولوية رئيسة للحكومات في عالمنا المُعاصر, إذ تسعى أَغلب الأَنظمة السياسية المُعاصِرة إلى تحسين كفاءة أَجهزتها الحكومية وفعاليتها، عن طريق الاستِجابة في تقديم الخدمات للمواطنين، وفي العِراق، تواجه "الرقمنة" تحديات وفرصاً على حدٍ سِواء، إذ تعمل الحكومة على تسخير إِمكانات التقنيات الرقمية لإِحداث تغيير إِيجابي وتطوير في مؤَسسات الدولة؛ وبتوظيف نموذج نضج الحكومة الرقمية في الحالة العِراقية؛ ليُساعدنا على فهم مدى تبني الحكومات للتقنيات الرقمية ودمجها في عملياتها وخدماتها، ويوفر رؤَية واضِحة مُفيدة لفهم تحديات وفرص الحكومة الرقمية في سياق النظُم السياسية.

الاستنتاجات

1. تعود أَهمية تطبيق استخدام التكنولوجيا في الأَعمال الحكومية أَو ما يُسمى الحكومة الالكترونية إِلى ما ينتج عنها من تبسيط في الإِجراءات والمُعاملات الحكومية ونقلها نوعياً مِن الأَطر اليدوية إِلى الأَطر التقنية الالكترونية المتطورة والارتقاء بكفاءة العمل الإِداري وارتفاع مستوى وجودة الأَداء الحكومي وتوفير الوقت والجهد والمال على المستوى الوطني.
2. تُعد الحوكمة منظومة مُتكامِلة لثلاثة محاور رئيسة للإِصلاح (الإِدارة، المالية، القضاء) ترتكز على أَسُس القانون وعلى مدى المُشاركة، فضلاً عن الشفافية والمُساءلة والكفاءة والاستجابة.

3. وفقاً لتقارير الدوَّامة الرقمية (Digital Vortex Report) الصادِرة مؤَخراً تُعد وسائل الإِعلام والترفيه والمُنتجات والخدمات التقنية والاتصالات، أَكثر القطاعات التي ستتأَثر بالتحوُّل الرقمي في السنوات القادِمة.
4. عن طريق تحليل جهود التحوّل الرقمي في العِراق، وتقرير (برنامج الأُمم المتحدة الإِنمائي لعام 2023)، يمكنُنا الحصول على نظرة ثاقبة للوضع الحالي للتحول الرقمي في العِراق، وتحديد مجالات التحسين والنمو في العالم الحديث، أَصبح التحول الرقمي عامِلاً حاسِماً للنجاح والقدرة التنافسية، وتتبنى الحكومات في جميع أَنحاء العالم بشكلٍ مُتزايد التقنيات الرقمية، لتحسين كفاءة عملياتها وفعاليتها. والعِراق ليس استثناءً مِن هذا الاتجاه، فقد بذلت جهود حثيثة في السنوات الأَخيرة لتحويل قطاعاتها ووظائفها المُختلِفة رقمياً.
5. إِنَّ عملية التحول الرقمي في العِراق، لم تخلُ مِن التحديات والعقبات، فالحوكمة ظاهرةٌ مُعقدةٌ لها انعكاساتها على التنمية البشرية والاقتصادية والاجتماعية، إِذ يُعاني العِراق مِن تحديات عديدة في هذا المجال تحديات سياسية واقتصادية وأَمنية وقانونية وثقافية-تكنولوجية. لكن على الرغم مِن تحديات البُنية التحتية والمعرفة الرقمية، يوفر العِراق فُرَصاً كبيرة للنمو والابتكار الرقمي، فرصاً سياسية واقتصادية وثقافية-تكنولوجية.
6. إِنَّ فكرة الحكومة المحلية تقوم على أَساس تمتع الهيئات المحلية بصلاحيات واسِعة مِن خِلال مُمارسة مهامها التي تؤَديها في ظل سيادة الدولة وفق ما تنص عليه القوانين النافذة، التي رافقت نشوء وتطبيق النِظام اللامركزي في العِراق بعد عام2003 والتي بدأَت مِنذُ كتابة الدستور النافذ لعام2005 وقانون المُحافظات رقم21 لسنة 2008 ومع استمرار التطورات التكنولوجية والثورة الرقمية، أَصبح مِن الضرورات على الدولة المُعاصِرة أَنَّ تتبنى تِلك التقنيات الخاصة، بالاتصالات والمعلومات في تطوير معلوماتها ولغرض تقديم الخدمة العامة الى السُكان المحليين وقد عملت المؤسسات المحلية على تطبيق مشروع نِظام الحكومة الالكترونية التي تتمثل في تغيير نمط وأَسلوب تعامُل وتفاعُل المؤَسسات كافة على اختلاف أَنواعها في تقديم الخدمات الحكومية إِلى المواطنين.
7. يعد مشروع الحكومة الالكترونية العِراقية أَو الرقمية مشروعاً ضخماً يهدف إِلى إِعادة خلق الحكومة ومؤسساتها وإِداراتها مِن جديد باتخاذ إِجراءات عصرية مُبتكرة لأداء الأَعمال عن طريق تطويع التقنية وتسخيرها في تنفيذ الإِجراءات الحكومية والذي يجعل الجودة

والتميُز شِعار الحكومة الالكترونية الجديدة ويحولها إلى مؤَسسة اقتصادية تكنولوجية تُنافس القطاع الخاص وفي مُقدمتها الجودة وكسب رضا المُستفيد وتوفير الوقت والجهد مِن مواطنين- مُستثمرين وغيرهم.

8. تعكس الحكومة الإلكترونية استعمال الدوائر والأَجهزة الحكومية للمعلومات التكنولوجية (مثل شبكات الاتصالات، الأنترنت، والموبايل المحوسب) التي لديها القدرة على تحويل العلاقات بين المواطنين والمُنشآت، وأجهزة الحكومة الأَخرى. ويمكن لهذه التكنولوجيا ان تخدم مجموعة متنوعة مِن الأَهداف المُختلفة لتحسين تقديم الخدمات الحكومية للمواطنين وتحسين التفاعُل مع قطاع الأَعمال والصِناعة، وتمكين المواطن مِن خِلال الحصول على المعلومات، أَو إدارة حكومية أَكثر كفاءة.
9. إنّ عملية التحول الرقمي في العِراق مُعقدة وصعبة، وقد تستغرق وقتاً للتنفيذ الكامل، وتحقيق الفوائد الكاملة مِن المُهم أَنَّ تستمر الحكومة العِراقية في الاستِثمار في التقنيات الرقمية بالشكل الأمثل واعتمادها، مع مُعالجة التحديات التي أَعاقت جهودها للتحول الرقمي، مثل محدودية الوصول إِلى التكنولوجيا ونقص المهارات الرقمية.

التوصيات

1. الابتعاد عن فكرة أنّ الدولة هي المورد الوحيد للخدمات الاجتماعية والذهاب إِلى تفعيل مبدأَ المُشاركة مع القطاع الخاص في تحديد احتياجات التنمية.
2. إِلزام كافة أَجهزة الدولة بالعمل وفق معايير الإِفصاح والشفافية وعرض مُخرجات عملها على الجمهور باعتباره الهدف الأول الذي تسعى لخدمتها كافة تلك الأجهزة.
3. الحد مِن البيروقراطية والروتين المُعقد في الاداء الوظيفي والسعي إِلى تنفيذ مُتطلبات المواطن وتخفيف أعباء المُتابعة.
4. التنسيق مع مراكز التدريب والتطوير في الجامِعات، فضلاً عن نشر الوعي الالكتروني لدى المواطنين وقطاع الأعمال ومُنظمات المجتمع المدني، وضرورة عقد ورش دورية وندوات علمية مُختصة في مجال الحوكمة الالكترونية التي تسهم بتعزيز الرؤى والأَفكار لدى المنظومة العلمية الأَكاديمية العِراقية.
5. وفي ظل الظروف والتحديات الكبيرة التي نعيشها في بلدنا العِراق فنحنُ اليوم بِحاجة إِلى منهجية وبذل جُهد شامل على الصعيد الوطني والاقليمي وعلى مستوى المُحافظات لتطوير

البُنية التحتية، وعلى آلية تنفيذ فاعِلة لسياسات وبرامج الحكومة، والمواطنون على اختلاف شرائحهم ومهنهم ومستوياتهم الثقافية والتعليمية هُم جزء مِن عملية إِعادة بِناء الدولة وهو الشرط الأَساسي لتحقيق التنمية والاستقرار وعلى المدى البعيد.

6. إنَّ الحوكمة الرقمية تتطلب قيادة تنمية بشرية شامِلة قائمة على أَساس خياراً ديمقراطياً حراً بعيداً عن دائرة التأَثير، وبذلك تكون الحوكمة هي الإِدارة الجيدة لجميع المؤَسسات في الدولة مِن خِلال سياسات وآليات ومُمارسات تقوم على الشفافية والمُشاركة والمُساءلة وسيادة القانون ومُكافحة الفساد وتسعى لتحقيق العدالة وعدم التمييز بين المواطنين والاستجابة لاحتياجاتهم وتتحرى الكفاءة للوصول بالسياسات والخدمات لأَعلى مستوى مِن الفعالية بشكلٍ مرضي للجميع.
7. لتدعيم الحوكمة الالكترونية في العِراق وتسهيل تطبيقها يجب الاهتمام بالبُنية التحتية للاتصالات الالكترونية، والبطاقات الائتمانية، وتأَمين المعلومات ومُكافحة القرصنة الالكترونية، وتنظيم التجارة الالكترونية.

المصادر والمراجع

[1] مروان سالم العلي (واخرون)، الحوكمة الرشيدة وإدارة المؤَسسات الدستورية في الدولة العِراقية: التحديات والمُعالجات، ط1، شركة الأكاديميون للنشر، عمان،2022، ص266-278.

[2] مروان سالم العلي، الاقليمية الجديدة والنِظام الدولي: دِراسة في التأثير والتأثر، ط2، دار السنهوري للنشر، بيروت،2023، ص876-882.

[3] للاستزادة حول تلك التحديات يُنظر: علياء حسين خلف وسناء حسين خلف، دور الحوكمة الرشيدة في تحقيق التنمية، مجلة الفتح، العدد69، اذار 2017، بحث مُتاح على الرابط: www.alfatehmag.uodiyala.edu.ig

[4] موقع أَرفع صوتك، الحوكمة الالكترونية.. سير "بطيء" وقوى "فاسِدة" تدفعها للوراء، بحث مُتاح على الرابط: https://www.irfaasawtak.com/iraq/2023/04/26

[5] مروان سالم العلي (واخرون)، المُتغيرات الاقليمية والدولية المؤثِرة في النِظام العالمي للقرن الحادي والعشرين، ط1، شركة هاتريك للنشر، اربيل،2024، ص38-40.

[6] عصام حاكم، الحكومة الالكترونية وتحديات التطبيق في العِراق، مقال مُتاح على الرابط: https://fcdrs.com/polotics/633.17-01-2017

[7] صفد الشمري، فرص نجاح الحكومة الالكترونية في العِراق، مقال مُتاح على الرابط: https://dcc-iq.com/?p=42309.13-09-2022

[8] مروان سالم العلي، مكانة الاقليمية الجديدة في الاستراتيجية الأمريكية الشامِلة، كيف جسد العِراق بوابة التغيير في الشرق الأوسط الكبير؟، ط2، دار المُعتز للنشر، عمان،2022، ص159-161.

[9] عصام حاكم، الحكومة الالكترونية وتحديات التطبيق في العِراق، مقال مُتاح على الرابط: https://fcdrs.com/polotics/633.17-01-2017

[10] مروان سالم العلي (وآخرون)، العِراق: التحديات الوطنية والدولية وسُبل مواجهتها: رؤَى مُستقبلية، ط1، دار المُعتز للنشر، عمان،2023، ص193-195.

[11] عصام حاكم، الحكومة الالكترونية وتحديات التطبيق في العِراق، مصدر سبق ذِكرهُ.

[12] مروان سالم العلي، رؤية استراتيجية تحليلية لواقع الحوكمة الرشيدة في العِراق: التحديات والمُعالجات، الندوة العلمية الثالِثة عشر الموسومة:"حوكمة السلطة كمؤشر لقياس الأداء الحكومي"، كُلية العلوم السياسية، جامِعة الموصل، 2019/3/13.

[13] عمار جعفر مهدي، الحوكمة في العِراق بين الهدف والمُعوِقات، مقال مُتاح على الرابط: https://www.ankasam.org/ar

[14] حيدر علي عبد الله، الفساد والنزاهة في العِراق، ط1، دار الدكتور للطباعة والنشر، بغداد،2014، ص26.

[15] الأَمين نصبة، أَهمية تطبيق مبادئ الحوكمة في النِظام العام: دِراسة حالة بلدية قمار الوادي، رِسالة ماجستير غير منشورة، كُلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامِعة الشهيد حمه لخضر بالوادي، الجزائر،2015، ص20.

[16] نقلاً عن: موقع أَرفع صوتك، الحوكمة الالكترونية.. سير "بطيء" وقوى "فاسِدة" تدفعها للوراء، مقال مُتاح على الرابط: https://www.irfaasawtak.com/iraq/2023/04/26

[17] مروان سالم العلي، الحربُ ضد الفساد أَخطر مِن الحرب ضد داعش، مقال مُتاح على الرابط: https://www.democraticac.ed=58915

[18] محمد مُصطفى سُليمان، حوكمة الشرِكات ومُعالجة الفساد المالي والإداري: دِراسة مُقارِنة، الدار الجامعية للنشر، مصر، 2006، ص33. كذلك: حيدر علي عبد الله، الفساد والنزاهة في العِراق، مصدر سبق ذِكرهُ، ص89-100.

[19] مروان سالم العلي، رؤية استراتيجية تحليلية لواقع الحوكمة الرشيدة في العِراق: التحديات والمُعالجات، مصدر سبق ذكرهُ.

(20) أحمد حسين بتال، الاقتصاد الرقمي وتحديات تطور تكنولوجيا المال في العِراق، مقال مُتاح على الرابط: https://www.uoanbar.edu.iq/RAECollege/News_Details.php?ID=223

(21) عبد الرحمن نجم المشهداني، مفهوم الحكومة الالكترونية ومعوقات نجاحها في العِراق، مقال مُتاح على الرابط: https://almadapaper.net/sub/06-418/p19.htm

(22) أحمد محمود القيسي، الحوكمة الرقمية في العِراق: التحديات والفرص، مقال منشور على الموقع: https://kerbalacss.uokerbala.edu.iq/wp/blog/2023/10/11

(23) المهلب الزيدي، تزايد الحلول الرقمية، مقال منشور على الموقع: https://www.kapita.iq/content/issue/tzayd-alhlol-alrkmy-aaad-tshkyl-aaadat-almsthlk-alaaraky-oaaad-thdyd-almstkbl

(24) موقع أرفع صوتك، الحوكمة الالكترونية.. سير "بطيء" وقوى "فاسِدة" تدفعها للوراء، مقال منشور على الموقع: https://www.irfaasawtak.com/iraq/2023/04/26

(25) المصدر نفسهُ.

(*) هُناك فرق بين مُصطلح "الخدمات الإلكترونية" ومُصطلح "الخدمات الرقمية". إذ تُشير الخدمة الإلكترونية عادةً إلى أي خدمة يتم توفيرها أو إدارتها أو الوصول إليها مِن خِلال وسائل إلكترونية، يمكن أنَّ تشمل هذه الخدمات التي تستخدم التكنولوجيا التناظرية أو الرقمية، تشمل أمثلة الخدمات الإلكترونية التلفزيون خدمات الاتصالات مثل :والراديو والهاتف (التناظري والرقمي).ومِن الأمثلة على الخدمات الإلكترونية خدمات . خدمات البث التلفزيوني والإذاعي.الهواتف الأرضية، والهواتف المحمولة، وَأجهزة الفاكس أما الخدمة . أنظمة الأمن مثل كاميرات المُراقبة وأنظمة الإنذار.للمُعاملات المصرفية (ATM) الصراف الآلي الرقمية تُشير بشكلٍ خاص إلى الخدمات التي تستخدم التكنولوجيا الرقمية، وهذا يعني أنَّ المعلومات يتم تستفيد الخدمات الرقمية (0s and 1s تخزينها ونقلها ومُعالجتها على شكل تسلسُل مِن الأرقام الثُنائية(من الإنترنت والحوسبة السحابية والتقنيات المُتقدمة الأُخرى لتوفير الخدمات مثل الخدمات المصرفية كما وتُشير أيضاً الخدمات الرقمية إلى .عبر الإنترنت والتجارة الإلكترونية والبث ووسائل التواصل الاجتماعي الخدمات التي تستخدم التكنولوجيا الرقمية على وجه التحديد، والتي تتضمن تمثيل البيانات ومُعالجتها بتنسيق ثُنائي (0و1)، وغالباً ما تكون هذه الخدمات قائمة على الإنترنت أو تعتمد على شبكات الكمبيوتر مواقع . الخدمات المصرفية والمُعاملات المالية عبر الإنترنت: ومِن الأمثلة على الخدمات الرقمية.لتقديمها و Spotify و Netflix . خدمات البث مثلeBay و Amazon التجارة الإلكترونية مثل (WhatsApp) منصات الاتصالات الرقمية مثل البريد الإلكتروني وتطبيقات المُراسلة مثلYouTube ، ما هو الفرق بين RMG. للاستزادة ينظر: Twitter, Facebook ووسائل التواصل الاجتماعي مثل الخدمات الالكترونية والخدمات الرقمية؟، مقال مُتاح على الرابط:https://www.rmg-sa.com

(26) للاستزادة حول تلك المُتطلبات يُنظر: علياء حسين خلف وسناء حسين خلف، دور الحوكمة الرشيدة في تحقيق التنمية، مصدر سبق ذِكرهُ.

(27) Saugata,B., and Masud, R,R., Implementing E-Governance Using OECD Model (Modified) and Gartner Model (Modified) Upon Agriculture of Bangladesh. IEEE, 2007, P. 4244-1551.

كذلك يُنظر: طارق فاروق الحصري، الاقتصاد الدولي، ط1، المكتبة العصرية للنشر، المنصورة،2010، ص215-240.

(28) فؤاد جمال عبد القادر، إطلالة على مشروع قانون التجارة الالكترونية،2009، مقال مُتاح على الرابط: https://www.egypt.gov.eg.

[29] محمود القدوة، الحكومة الالكترونية والإدارة المُعاصِرة، ط1، دار أُسامة للنشر والتوزيع، عمان،2010، ص195.

[30] سلام زيدان، لمواجهة الفساد والسيطرة على المال.. العِراق يلزم مؤسساتهُ بتطبيق الدفع الالكتروني، بحث مُتاح على الرابط: https://www.aljazeera.net/ebusiness/2023/1/26

[31] أثير علي عبد الكاظم وسرى نوفل بهجت، الحوكمة والحكومة الالكترونية، مُحاضرة الكترونية، كُلية مدينة العلم الجامِعة، بغداد، كانون الثاني2022.

[32] بغداد اليوم، كيف سيسهم التحول الرقمي والحوكمة الالكترونية بالقضاء على الفساد؟، تقرير مُتاح على الرابط: https://baghdadtoday.news/235182-10-11-2023

[33] زعتر معلوف ونجلاء رباشي واخرون، الحوكمة الرقمية: تحديات وفرص من أَجل مواطنة شاملة للجميع، ندوة علمية أَقامها المجلس النيابي اللُبناني، بالتعاون مع الجمعية البرلمانية الفرنكوفونية، لُبنان، 23 تشرين الثاني2022.

[34] ذو الفقار المحمداوي، العِراق يتجه صوب التحول الرقمي.. مختصون لن يتحقق إلاَّ بعد خمسون عاماً، تقرير مُتاح على الرابط: https://almadapaper.net/view.php?cat=303367.23-12-2023

[35] Bartlett Rossel and (Others), Conceptualizing, Governance, Management,2007, P.399-407.

[36] مروان سالم العلي، استراتيجيات مُكافحة الفساد: سرطانٌ يفتكُ بالعِراق، مقال مُتاح على الرابط: https://annabaa.org/arabic/goodgovernance/18191

[37] عصام حاكم، الحكومة الالكترونية وتحديات التطبيق في العِراق، مصدر سبق ذِكرهُ.

[38] أحمد حسين بتال، الاقتصاد الرقمي وتحديات تطور تكنولوجيا المال في العِراق، مصدر سبق ذِكرهُ.

[39] الزُهيري طلال ناظم، مُبادرات الحوكمة الالكترونية في العِراق وعوامل نجاحها، مجلة الحوكمة: المسؤولية الاجتماعية والتنمية المُستدامة، المُجلد5، العدد1، كُلية العلوم الاقتصادية التجارية، الجزائر، اذار/مارس2023، ص25-28.

ملف العدد
الأمن السيبراني
درع التحول الرقمي العراقي
(بين التحديات الراهنة وضرورات المستقبل)

العراق
بين ضرورات التحول الرقمي وتحديات المحافظة على أمنه الوطني

د. يونس مؤيد يونس مصطفى
جامعة الموصل/ كلية العلوم السياسية

أدى التقدم التكنولوجي وظهور شبكة المعلومات الدولية-الانترنيت- والوسائط الالكترونية التي تعمل وفق هذه الشبكة، وسهولة حصول مواطني الدول على هذه التقنيات التكنولوجية في البيئة الاستراتيجية العالمية الى وضع الخطط الاستراتيجية التي تسهل حياة مواطنيها في الحصول على الخدمات الضرورية والكمالية التي يحتاجونها بكبسة رز واحدة، وبدقائق معدودات عبر الالواح الرقية التي هي في متناول اليد، ومغادرة الاجراءات الادارية الروتينية المعقدة والبطيئة. اذ نحن اليوم نعيش في عصر السرعة، ويعد هذا التطور والتحولات نحو التحول الرقمي والادارة الالكترونية والحكومة الالكترونية جزء من مؤشرات المواطن العالمية. والعراق لابد ان يواكب الدول العالمية والاقليمية المتحولة رقمياً وقطعت اشواطًا متقدمة في هذا المجال، والعراق على الرغم من قيامة بعمليات للتحول الرقمي على مستوى العديد من مؤسسات الدولة الرسمية الا انه يواجه تحديات لوقف عجلة التحول الرقمي منها مرتبط بالمواطن البسيط، ومنها مرتبط بمؤسسات الدولة، ومنها مرتبط بعمليات الجريمة المنظمة والارهابية التي تستهدف مؤسسات الدولة رقمياً وتكنولوجياً.

الكلمات المفتاحية: العراق، التحول الرقمي، الأمن الوطني، تحديات التحول، الامن الالكتروني.

Iraq is between the necessities of digital transformation and the challenges of maintaining its national security

Dr. Younis Moayad Younis Mustafa
University of Mosul/College of Political Sciences

Technological advancement, the emergence of the international information network - the Internet - and the electronic media that operate according to this network, and the ease of access by citizens of countries to these technological technologies in the global strategic environment have led to the development of strategic plans that facilitate the lives of their citizens in obtaining the necessary and complementary services they need with one click of rice. In just a few minutes, through the digital panels that are at hand, you can avoid the complex and slow routine administrative procedures. Today, we live in an era of speed, and this development and transformations towards digital transformation, electronic management, and electronic government are part of the global citizen indicators. Iraq must keep pace with

الاستلام	الارجاع	القبول
2024/02/04	2024/04/12	2024/05/17

global and regional countries that are digitally transforming and have made advanced strides in this field. Iraq, despite undertaking digital transformation operations at the level of many official state institutions, faces challenges to stop the wheel of digital transformation, some of which are linked to the simple citizen, and some of which are linked to state institutions, including Linked to organized crime and terrorist operations that target state institutions digitally and technologically.

Keywords: Iraq, digital transformation, national security, transformation challenges, electronic security.

المقدمة

العراق جزء من البيئة الاستراتيجية العالمية، إذ أصبح اصبح لازمًا عليه ان يواكب التطورات، نتيجة ارتباط فواعل البيئة الاستراتيجية ببعضها، سواءً اكانوا دولًا أم مؤسسات وشركات ام افراد، وهذا الارتباط يولد ان تلتحق الدول المتأخرة رقميًا بالدول المتقدمة رقميًا ولو نسبيًا، كمرحلة أولية ثم التدرج في هذا التحول والتطور، لأن التعاملات العالمية أصبحت في اغلبها رقميًا وتكنولوجيًا.

فالعراق بعد أن عاش فترة مظلمة منعزلًا بعيدة عن التطور والانفتاح الرقمي والتكنولوجي التي عاشته الدول الأخرى في أوقات سابقة وبأشواط طويلة قبل عام 2003، حصل التغيير في عام 2003 ما سمح بإدخال التطورات الإلكترونية التي كان ممنوع من دخولها العراق فيما سبق وأرتبط العراق بالتطورات التكلوجية في العالم.

اهمية البحث:

التحول الرقمي شيء مهم وضروري من أجل خدمة المواطن في أية دولة، ويمنح رؤية جديدة في أداء عمل المؤسسات الرسمية وغير الرسمية، والتخلص من الإجراءات الإدارية البطيئة والمعقدة، فلابد من معرفة ماهية التحول الرقمي وماهي الاسس والركائز التي يستند عليها لتكون عملية التحول الرقمي سليمة وصحيحة وهل يمتلك العراق ما يؤهله إلى تحول رقمي وأداء مؤسساتي إلكتروني لنصل لمرحلة الحكومة الرقمية؟.

مشكلة البحث:

على الرغم من أن العراق عرف التطورات التكنولوجية والرقمية التي تؤهله الى عملية التحول الرقمي منذ التغيير الذي حصل عام ،2003 إلا أن هناك تحديات واجهت هذا التحول وجعلته في مصاف الدول المتأخرة رقميًا.

فرضية البحث:

أن عدم استقرار الاوضاع في العراق لاسيما الأمنية والسياسية والاقتصادية منذ التغيير في عام 2003 ولحد يومنا هذا على الرغم من التحسن النسبي جعله في مرتبة الدول المتأخرة رقمياً، وهذا التأخر في التحول الرقمي جعله يستمر في الإجراءات الإدارية المعقدة والبطيئة التي لاتوفر خدمة مريحة للمواطن العراقي، وفي بعض الأحيان هذا التأخر الرقمي يحسب للعراق؛ نتيجة التحديات المصاحبة للتحولات الرقمية في الدول الأخرى وما نشاهده من عمليات الاختراقات والقرصنة الالكترونية بدافع الجريمة المنظمة او بدافع الإرهاب واستهداف المؤسسات الحكومية أو بدافع الانتقام.

مناهج البحث:

تم الاعتماد على المنهج الوصفي التحليلي لوصف صيرورة التحول الرقمي وفوائد والخصائص المصاحبة له وتحليل التحديات التي تواجه هذا التحول في العراق.

هيكلية البحث:

بعد تحديد مشكلة البحث وفرضيته تم تقسيم البحث الى محاور ثلاثة فضلاً عن مقدمة وخاتمة، نخص المحور الأول صيرورة التحول الرقمي في البيئات الداخلية للدول، ودرس المحور الثاني الأمن الإلكتروني مدخل وقائي للحفاظ على مكتسبات التحول الرقمي، وتناول المحور الثالث واقع التحول الرقمي في العراق وتحدياته.

المحور الأول: صيرورة التحول الرقمي في البيئات الداخلية للدول

أدى ظهور شبكة الويب العالمية، وأزدياد التقنيات المصاحبة مثل الإنترنت، والهواتف الذكية وWeb 2.0، SEO، والحوسبة السحابية، والتعرف على الكلام، وأنظمة الدفع عبر الإنترنت، والعملات المشفرة الحاجة إلى التحول الرقمي؛ للوصول الى خدمات كان يصعب الوصول اليها في مجالات الصحة، والتعليم، والتمويل، والاقتصاد، والخدمات والتأثير على جميع جوانب الحياة البشرية[1].

وهذه التغيرات والتحولات الإلكترونية التي شهدها العالم امتدت من الأفراد الى المنظمات حتى شملت الحكومـات مؤخراً من أجل التحول إلى مجتمع واقتصاد المعرفة، إذ

أضحت الدول تتنافس في تحفيز مؤسساتها الرسمية وغير الرسمية لمواكبة التطور، ومن بين أهم الاستجابات لتلك التطورات ظهور مفاهيم التحول الرقمي في الإدارة الحكومية.

فظهرت تعريفات متعدد للتحول الرقمي منها أنه إعتماد واستخدام الأدوات والوسائل التكنولوجية لرقمنة المنتجات أو الخدمات التي تقدمها القطاعات المختلفة بتحويل البيانات الخاصة بها إلى هيئة رقمية (صفر/ 1)، ومن ثم يمكن التعامل معها إلكترونيًا باستخدام الحواسيب، سواءً أكان بالتصنيف أم بالتخزين، ثم استدعائها وتبادلها واستنباط المعلومات المفيدة منها؛ لزيادة قيمتها وسهولة تسويقها، ومن ثم تحسين الخدمات والمنافسة وخلق الفرص[2].

ويعرف التحول الرقمي بأنه عملية الانتقال من أنموذج العمل التقليدي الى أنموذج يعتمد التقنيات التكنولوجية الرقمية في الابتكار للمنتجات والخدمات والتسويق مع توفير قنوات جديدة للعوائد عبر استراتيجية رقمية التي لا يمكن أن تحدث إلا من خلال تقييم للإمكانات الرقمية ودراسة لمتطلبات الاستثمار الرقمي في ظل انشطة التسويق الرقمي مع وجود إرادة للتغير لدى الإدارة[3].

والتحول الرقمي هو التدخلات الاستراتيجية التي تعزز القدرة الرقمية التنظيمية؛ لتحسين عمليات الدولة وخدماتها ونماذج اعمالها لإرضاء مواطنيها[4].

والتحول الرقمي هو "عملية تحول شاملة ناتجة عن مزيج من ثالث ظواهر: الأتمتة، وإزالة الطابع المادي وإعادة تنظيم أنماط الوساطة، إذ يؤثر هذا التحول على جميع الأعمال والأنشطة والعمليات الداخلية للمؤسسات، ويشير التحول الرقمي إلى العملية التي تقود المؤسسة إلى دمج التقنيات في جميع أنشطتها من لتحسين أدائها. إنه نهج يرتكز على البيانات ويعتمد بشكل كبير على استخدام مجموعة من الخوارزميات المعقدة؛ لتعزيز اكتساب آفاق جديدة، وتسهيل المعاملات مع المواطنين، وضمان ولائهم عبر الاستخدام الأمثل للوظائف المختلفة للمؤسسة[5].

وتتجلى الثورة التكنولوجيا الرقمية في الميادين المختلفة التي تشمل الآتي[6]:

1- **المجال السياسي والأمني:** التكنولوجيا محرك رئيس للفعل السياسي، فهي التي تشكل الحركات الاجتماعية، وساهمت في تغير بعض جوانب الممارسة السياسية عبر جمع وتصنيف وتحليل وتداول المعلومات والبيانات المتعلقة بممارسة قيم الديمقراطية

وآلياتها المختلفة، إذ أضحت الديمقراطية تعتمد على الحوكمة الإلكترونية والتصويت والانتخاب الإلكتروني.

2- **المجال الاقتصادي** عبر العديد من المظاهر منها الاقتصاد الرقمي والتعاطي مع التجارة الإلكترونية، والتكنولوجيا المالية عبر تطوير الخدمات المالية المقدمة والتحول من النقود بصفتها التقليدية إلى العملات الرقمية.

3- **المجال الثقافي والاجتماعي** عبر التوجه نحو مجتمع المعرفة للوصول الى المجتمع الذكي الذي هو انتاج هجين تتداخل فيه الأبعاد الاجتماعية بالتقنية وفق رؤية جديدة وقيم اساسية قوامها الانفتاح، والترويج لأجندات حقوق الإنسان والانفتاح على الثقافات الاخرى، وتزايد دور المجتمع والرأي العام في التأثير في القضايا العالمية والاقليمية، ونشر ودعم الافكار الاحتجاج والتغير بعيداً عن تحكم السلطات، وانتشار اشكال جديدة من التضليل التي تمس جماعات وأفراد أو نظم قيمية معينة، وتحدي الهوية وتعزيز المشاعر السلبية اتجاه مسألة الانتماء، واستغلال القوى الخارجية لهذه التكنولوجيا لتسويق ثقافاتها ونماذجها الثقافية، فضلًا عن المراقبة والتجسس على معلومات المواطنين.

والدوافع التي قادت الحكومات اتجاه التحول الرقمي هي لحصد ثمار وفوائد هذا التحول وفق الآتي[7]:

- زيادة التكاليف والضغوط على الموازنة لاسيما التراجع الكبير في ايرادات الدول لاسيما النفطية؛ لذلك لابد من توفير التكاليف، وتنفيذ العمليات الحكومية بأكثر فعالية.
- التحكم في الوقت والتكاليف ويحسن الكفاءة التشغيلية للمؤسسة.
- تحسين الابتكار للمؤسسة عبر مخرجات تقنية رقمية لتقديم خدمات افضل.
- تحقيق القابلية التنافسية بين مؤسسات الدولة.
- تقديم خدمات ومنتجات ذات جودة عالية وتحقيق رفاهية المواطنين.

وهذا التحول الرقمي مسار الوصول الى ما يعرف بالحكومة الالكترونية التي تعرف أنها المعرفة الإلكترونية؛ لتطوير المعرفة الإدارية وتقنياتها التطبيقية والمهارات المهنية، فهي تقوم

بإغناء الفكر الاداري بمفاهيم تتصل بالمعرفة الإلكترونية وتقنيات الاتصالات والمعلومات، كما تعرف بإنها استخدام الجهات الحكومية لتقنيات المعلومات مثل استخدام شبكات النطاق الواسع، والإنترنيت، والحوسبة المتنقلة عبر العلاقات المتبادلة بين المواطنين، والمؤسسات والجهات الحكومية، وأصحاب المصالح الأخرى التي من شأنها تحقيق مجموعة من الأهداف منها تحسين تقديم الخدمات الحكومية، وتحسين قطاع الاعمال والصناعة، وتحسين مستويات الاتاحة، والوصول الى إدارة حكومية كفؤة[8].

تعرف الحكومة الإلكترونية بأنها جعل جميع الإدارات الحكومية تتكامل مع بعضها البعض، وتقدم الخدمات فيما بينها وبين المواطنين والقطاع الخاص بشكل مباشر وإلكتروني، وبذلك فإن مفهوم الحكومة الإلكترونية أشمل من مفهوم الإدارة الإلكترونية، وتعرف ايضًا الحكومة الإلكترونية تعد الإطار الشامل والمتكامل للتطبيقات الإلكترونية في المجال الإداري على مستوى أطراف العملية الإدارية كافة، وهذا يعني أن تطبيق أسلوب الإدارة الإلكترونية هو الخطوة السابقة لتطبيق أسلوب الحكومة الإلكترونية في الجهات الحكومية[9].

واضحت كل المجتمعات تطمح الى الحكومة الإلكترونية التي تعد نموذجية في طريقة عملها عبر تقديم الخدمات الحكومية بدءًا من تحصيل الضرائب الى العلاج، عبر بوابات الانترنيت، لتوفير الخدمات للمواطنين، لإنهاء الاجراءات البيروقراطية المعقدة عبر اكتفاء المواطن بهاتف محمول مربوط بشبكة المعلومات الدولية-الانترنيت- لقضاء حاجاته اليومية من المعاملات دون عناء الذهاب الى التعامل المباشر مع الموظفين وما يقود ذلك الى الاحتكاك المباشر المفضي الى الفساد الاداري والمالي[10].

ولكن هذا التحول الرقمي للوصول الى الحكومة الالكترونية لديه متطلبات وأسس لابد من الارتكاز عليها وهي[11]:

1- التقنيات عبر منظومة من الأجهزة والبيانات والتخزين والبرمجيات التي تعمل ضمن بيئة تقنية ومراكز معلومات بكفاءة تشيلية غير منقطعة.

2- البيانات أن تقوم المؤسسات بجهود إدارة وتحليل البيانات بشكل منتظم لتوفير نوعية بيانات نوعية موثوقة وكاملة مع توفير وتطوير أدوات مناسبة للتحليل الاحصائي والبحث عن بيانات التنبؤ في المستقبل.

3- الموارد البشرية التي تشكل جانبًا حيويًا يصعب على المؤسسات التحول الرقمي بدونه ويكون مؤهل وقادر على استخدام البيانات وتحليلها.

4- العمليات بناء تقني يتضمن سياسات واجراءات تغطي نشاطات مؤسسات الدولة وعملياتها مترابطة مع التقنيات اللازمة والتطبيقات المطورة والبيانات المعالجة.

العراق اليوم في بيئتين اقليمية وعالمية اتجهت دولها منذ مدة ليست بالقصيرة نحو التحول الرقمي وتحقيق أهداف التنمية المستدامة للأمم المتحدة، وغادرت الاجراءات التقليدية والممارسات الادارية البيروقراطية البطيئة والخاطئة في بعض الأحيان، فأصبح لازمًا عليه التوجه نحو هذا التحول المهم والذي يعود بالفائدة على طرفي الدولة المواطن والحكومة.

المحور الثاني: الأمن الالكتروني مدخل وقائي للحفاظ على مكتسبات التحول الرقمي

العمل في بيئة التحول الرقمي الآمنة يتطلب مدخل واستراتيجية وقائية من التهديدات والتحديات عدة ذلك أن الفضاء الالكتروني مبني على مشاركة المعلومات عبر الوسائط الاجتماعية فهناك احتمالية النشر المهمل للمعلومات ما يقود الى مخاطر أمنية، لأن هذا الفضاء مليء بنقاط ضعف التي تحتوي على برامج نصية لتحميل وتشغيل ملفات الوسائط والتطبيقات يمكن عد معظمها برامج خبيثة يمكن أن تقود الى هجمات إلكترونية يمكن أن تكون جزء من حرب المعلومات[12].

ويمكن تشخيص مصادر الخطر على شبكات التحول الرقمي وفق الآتي[13]:

1- الخطر الداخلي: المهاجمون من داخل عمل شبكة المعلومات وهم الأفراد العاملين لنفس الدائرة الحكومية المستهدفة، وهذا النوع هو الأشد خطورة وفتكًا من خطر الأعداء الخارجين وهو التهديد الأكبر للمؤسسات الحكومية، فانتهاك الخصوصية من داخل المؤسسة الحكومية سهل الحدوث وصعب الكشف في حالات كثيرة لاسيما الاشخاص الذين يمتلكون خاصية الولوج الى نظام شبكات المعلومات، وطمس معالم الدخول واثاره وهذا متأتي من حالات منها عدم الرضا العاملين بالمؤسسة الحكومية، واثبات الذات، والاستفادة المادية.

2- الخطر الخارجي: الأشخاص-قراصنة الانترنيت- الذين يهاجمون شبكة المعلومات من خارج المؤسسات الحكومية سواء اكانوا على صلة بالمؤسسة ام لا.

3- خطر التشويش: ويقصد بها العوامل التي تؤثر على ارسال واستقبال البيانات والمعلومات عبر شبكات المعلومات، اذ تتعرض الى نوع من التشويش في الارسال او الاستقبال عبر المعدات والبرامج وقد يكون التشوش مقصوداً من جهات معينة او غير مقصود ظروف طبيعي.

4- خطر سوء التصميم: هناك بعض الأخطاء الفنية في تصميم الشبكات والأنظمة الالكترونية التي تعمل عليها الشبكات ناتج عن نقص في المعلومات وعدم تكامل الرؤية لدى مصممي البرامج في المؤسسات الحكومية.

5- خطر سوء الاستخدام: ناتج من اهمال الموظفين الحكوميين العاملين المتعمد أو غير المتعمد في مؤسسات الدولة الذي يتطلب منهم كفاءة والخبرة العملية والعلمية لقيادة هذه الشبكات والتطبيقات والأنظمة الالكترونية.

6- خطر الكوارث الطبيعية نعيش في بيئة معرضة لكوارث الزلازل والانفجارات والحرائق ونتائجها الخطرة على الانظمة والشبكات المعلوماتية.

وهذه الأخطار المشخصة للتحول الرقمي في الدول متأتية من:

1- **الهجمات الالكترونية** التي هي فعلًا يقوض من قدرات ووظائف شبكة الكمبيوتر لأهداف سياسية او قومية او شخصية عبر استغلال نقطة ضعف معينة تمكن المهاجم من التلاعب بالنظام، ويرتبط بذلك الجرائم الكترونية التي هي افعال واعمال غير قانونية تتم عبر معدات أو اجهزة الكمبيوتر أو شبكة المعلومات الدولية-انترنيت- أو تبث عبرها محتوياتها[14]. ويمكن اجمال الجرائم الالكترونية ب[15]:

أ- الهجمات الالكترونية في قطاع الخدمات المالية، الجرائم الالكترونية ضد الحكومات التي تهاجم المواقع الرسمية للحكومة، وأنظمة شبكاتها، وتركز على تدمير البنى التحتية لهذه المواقع أو الأنظمة الشبكية بشكل كامل.

ب- جريمة الاختراق والبقاء غير المشروع.

ت- جرائم الالكترونية ضد الملكية الفكرية كالتعدي على تصميم أو نموذج.

ث- جرائم الاحتيال والاعتداء على الأموال، كإدخال بيانات غير صحيحة أو تعليمات من غير المصرح بها، أو استعمال بيانات وعمليات غير مسموح الوصول إليها بغية السرقة من قبل موظفين فاسدين في الشركات والمؤسسات المالية.

ج- جرائم الابتزاز الالكتروني.
ح- جرائم الاستخدام غير المشروع لأدوات الدفع الالكتروني.
خ- اختراق المواقع التجارية الأمر الذي يسبب خسائر مادية ضخمة.
د- جرائم السطو على البطاقات الائتمانية.
ذ- جرائم النصب والاحتيال التجاري الالكتروني

2- **الإرهاب الإلكتروني** الذي يعد الوجه المتحول من الارهاب الفعلي الحقيقي وفق الآتي[16]:

أ- بنية هيكل الارهاب الالكتروني: يكمن في وجود جماعة منظمة تعمل بشكل منهجي لارتكاب عدد غير محدد من الجرائم، على هذا الأساس يعد الارهاب التكنولوجي ارهابًا من حيث الهيكل لاشتماله على العناصر الآتية: وجود عدد غير محدد من الأعضاء، الوصول الى الموارد والتمويل، القدرة على التخطيط المستدام للعمليات وتنفيذها بمور الوقت فهي جرائم الكترونية منظمة؛ لأن اعضاء الخلية على تواصل وتنسيق مستمر لتنفيذ هجمات الكترونية محددة ضد العدو الا وهو مؤسسات الدولة.

ب- مبدأ الضرر: لا يهاجم الإرهاب الإلكتروني المصالح الفردية؛ لأن غايته إظهار الوقع الحقيقي في نفوس المواطنين بالعموم واستشعارهم بقوة الكيان الإرهابي، أي زرع الخوف في نفوس أكبر عدد ممكن من الأفراد لذلك يعمل على استهداف جماعي لمصلحة جماعية هجومًا مباشرًا لمصالح وطنية ومؤسسية للدولة والمجتمع.

ت- العناصر: يتكون هذ الارهاب من عنصرين غائي ووسائلي: إلغائي أي ارتكاب جرائم ذات دوافع سياسية دائمًا عبر تغيير النظم السياسية والإطاحة بالحكومات المنتخبة شرعيًا، اما الوسائل فهي تنفيذ الاعمال الارهابية بطريقة مناسبة لغرس الإرهاب في نفوس المواطنين مع استخدام الوسائل المناسبة لترويع وبث الرعب العام عبر استخدام الادوات الرقمية الفايروسات الدودية والهجمات البرامجية الخبيثة لحجب الخدمات.

3- **القرصنة الإلكترونية** من بين التهديدات التي تشكل خطرا على التحول الرقمي وتعني الاستغلال من قبل أشخاص معينين هدفهم إلحاق الضرر بأشخاص آخرين أو لأسباب تتعلق بالفضول، ولهذا يتم إطلاق تسميات مختلفة على القراصنة في الفضاء الرقمي

حسب خلفياتهم وأهدافهم، فالقرصنة الالكترونية تعني الوصول إلى أجهزة الآخرين بطريقة غير مشروعة عبر ثغرات نظام الحماية، وأخطر أنواع القراصنة الذين يسمون بالهاكر هاكر القبعات السوداء، اذ يقومون بعمليات الاختراق لأهداف خبيثة وتخريبية، فيخترقون أجهزة وأنظمة المستخدمين؛ لسرقتها أو العبث بها أو تخريبها، وغالبا ما يكون هدفهم هو الحصول على مبلغ مالي عن طريق نشر فيروس الفدية، أو لأهداف سياسية مختلفة تقف ورائها جهات أجنبية أو عبر أطراف من الداخل مدعومين من الخارج[17].

ولحماية هذا الفضاء الالكتروني لابد من أمن الكتروني الذي هو جزء من الأمن السيبراني وهو من اهم مجالات الامن في القرن الحادي والعشرين، ويقصد به مجموع العمليات والانظمة التقنية التي تستخدمها الدول لحماية الشبكات واجهزة الحاسب الآلي وكل ما هو موجود على شبكة المعلومات الدولية-انترنيت- وهو امر ضروري في ظل انتشار الهجمات الإلكترونية ما يعرض الحواسيب والشبكات الوطنية التابعة للدولة لخطر الاتلاف والمسح أو التعطيل أو الاختراق يعرض أمن الدولة لخطر[18].

ويعرف ايضًا بأنه حماية جميع أنواع المعلومات ومصادر الأدوات التي نتعامل معها وتعالجها من منظمة وغرف تشغيل الأجهزة ووسائط التخزين والأفراد من السرقة أو التزوير أو التلف أو الضياع أو الاختراق باتباع اجراءات وسياسات وقائية، أي المحافظة على المكونات المادية وغير المادية للحاسب الآلي فضلًا عن اضفاء الشرعية على حدود وصلاحية استخدام المعلومات[19].

ومتطلبات تحقق الأمن الالكتروني والحفاظ على أمن بيئة التحول الرقمي لابد من[20]:

1- **العناصر المادية:** الأجهزة والقطع الفنية والالكترونية التي تمثل البنية التحتي الاساسية اللازمة لتشغيل نظم المعلومات.
2- **العناصر البرمجية:** المكونات غير المادية التي تشتمل على النظم البرمجية الاساسية والمطلوبة لتشغيل نظم المعلومات.
3- **القوى البشرية:** الأفراد الكفء وذوي المهارات العالية في مجال تكنولوجيا المعلومات والأمن السيبراني الذين يقع على عاتقهم تشغل النظم وادامتها في المؤسسات.

4- دعم الإدارة العليا لتطبيق نظم المعلومات.
5- إعادة تصميم الهيكل التنظيمي لتلبية متطلبات تكنولوجيا المعلومات والتحول الرقمي.
6- الشبكات والاتصالات وهي الوسيلة التي يتم عبرها نقل المعلومات ومرورها من مكان لآخر ويجب أن تكون وطنية خالصة وليس في موقعها في دول أخرى أو أقمار صناعية مستأجرة.

المحور الثالث: واقع التحول الرقمي في العراق وتحدياته

أن التحول الرقمي في الدولة العراقية لابد أن يستند على عدد من الاساسيات التي يجب أن تكون متاحة لتقييم مدى جاهزية العراق لهذا التحول وفق مؤشرات عدة هي[21]:

1- البنية التحتية للاتصال والتكنولوجية: إذ تعد ركيزة اساسية للتحول الرقمي في الدولة العراقية، كما تعد عاملًا مهما في تحقيق الشفافية وتدفق المعلومات ويمكن قياس هذا المؤشر وفق مؤشرين هما: مؤشر توفر الأجهزة والبرمجيات الإلكترونية في المؤسسات، ومؤشر الاتصال بالأنترنيت داخل المؤسسات.
2- مؤشر توظيف المعلوماتية الذي يعد أهم دعائم واسس تقدم الدول وتطورها التي تسطيع الدولة من خلالها أن تقدم للفرد العديد من الخدمات اختصارًا للهد والوقت لكن يجب أن توظف هذه التقنية وفق خطط استراتيجية لتطويرها واستثمارها في جميع المجالات وفق مؤشرات فرعية هي: مؤشر نظم البيانات والمعلومات، ومؤشر آليات مفعلة لإدارة المعلومات.
3- توفر الخبرة من الموارد البشرية المؤهلة لاستخدام تقنيات المعلومات.
4- نشر الوعي الضروري لتقبل استخدام التحول الرقمي الحكومية.
5- ربط مؤسسات الدولة المختلفة بشبكة اتصالات واحدة تخدم انشطتها ومهامها ومسؤولياتها نحو خدمة الجمهور بسهولة ويسر.
6- مرونة الهياكل المؤسسية وملاءمتها مع مهام ومسؤوليات التحول الرقمي واستحداث وحدات تنظيمية ترعي مصالح الجمهور وتقويتها باستمرار.
7- وضع القوانين والتشريعات التي تلائم اعمال التحول الرقمي ونشاطاته.

8- المحافظة على الخصوصية وعدم تهديد شبكة المعلومات الدولية-الانترنيت- لها بصورة او اخرى، لضمان ثقة الجمهور بالخدمات الالكترونية المقدمة من قبل الحكومة والاقبال عليها والتعامل معها.

9- استحداث وحدات للإجابة السريعة على تساؤلات المواطنين اتجاه الخدمات الالكترونية المقدمة في حالة وجود صعوبات امام المواطن.

ويمكن ملاحظة المؤشرات السابقة على تسلسله وفق مؤشر تطور الحكومة الالكترونية للمدة 2012-2020[22]:

1- العراق بالترتيب 137 من 193 دولة لسنة 2012.

2- العراق بالترتيب 155 لسنة 2019

3- العراق بالترتيب 143 على مستوى العالم من اصل 170دولة بمؤشر الحكومة الالكترونية لسنة2020.

كما يمكن ملاحظة تصنيف الدول العربية وفق مؤشر التحول الرقمي الى دول قائدة ودول في مرحلة التحول الرقمي ودول متأخرة والعراق يعد من الدول المتأخرة في التحول الرقمي في البيئة الاقليمية كما موضح في الجدول الآتي:

الجدول (1) يوضح مؤشرات التحول الرقمي للدول العربية لعام 2022[23].

الدول	الحكومة الرقمية	الاسس الرقمية	الاستعداد الرقمي للمواطن	الابتكار الرقمي
الامارات	85.55	71.83	74.6	63.94
البحرين	82.13	57.38	72.23	49.33
السعودية	80.24	57.55	76.97	61.37
الكويت	79.13	52.45	64.44	45.81
عمان	77.48	56.38	76.15	48.58
قطر	71.73	56.51	77.51	61.21
تونس	65.26	37.46	58.04	44.66
المغرب	57.29	41.65	51.79	46.46
مصر	55.27	39.25	59.33	48.67
الاردن	53.09	36.48	66.85	49.93
الجزائر	51.73	42.33	51.73	43.54
لبنان	49.55	35.92	66.28	45.96
اليمن	30.45	13.5	40.68	31.16
فلسطين	20.05	12.83	35.17	30.60
موريتانيا	28.2	12.83	40.71	29.76
السودان	20.05	12.883	35.17	27.34
الصومال	20.05	12.83	35.17	27.43
العراق	20.05	12.83	35.17	27.43
جزر القمر	20.05	12.83	35.17	27.43
جيبوتي	20.05	12.83	35.17	27.43
سوريا	20.05	12.83	35.17	27.43
ليبيا	20.05	12.83	35.17	27.43

فجاء العراق متذيلًا الجدول وفق مؤشرات التحول الرقمي عند مقارنته بالدول العالمية أو دول المنطقة الاقليمية نتيجة الآتي:

1- الظروف والأوضاع غير المستقرة التي عاشها العراق على الصعد المختلفة السياسية والاقتصادية والأمنية منذ التغيير عام 2003 ولحد عام 2021 جعلته متأخر في عملية التحول الرقمي.

2- البنية التحتية المحدودة والأطر التنظيمية، إلا أنّ التبني التدريجي للتكنولوجيا يحدث تأثيراً ملحوظاً في البلد. فبدلاً من توقع حدوث تغيير هائل بين عشية وضحاها، يجب أن ندرك أنّ التحول الرقمي هو عملية تدريجية، وكل تقدم صغير يساهم في تقدم البلد .

3- التطور التكنولوجي الذي شهده في مجال المعلومات والاتصالات بعد عام 2003 تزامن معه ضعف الأمننة الإلكترونية، وركاكة بنيته التحتية ما أدى الى أن يكون العراق منكشفًا أمام الكثير من الدول والجماعات الخارجة عن القانون، لأن أكثر مؤسسات الدولة تتعاقد الدول الأخرى فيما يخص الاقمار الصناعية حول معلوماته الإلكترونية، أي يقع موقع تخزين معلوماته الإلكترونية يقع خارج حدود وسلطة الدولة العراقية ما يؤدي ذلك الى مرور معلوماته الى خوادم الدول الاخرى م رجوعها الى العراق عند استدعائه لها[24].

4- سرعة الاتصال بالأنترنيت متدينة بدرجة كبيرة مع ارتفاع تكاليفه، على الرغم من أن وزارة الاتصالات العراقية أصبح لديها مشروع وطني للأنترنيت بالتعاون مع شركة ايرثلنك للاتصالات، وشركة سمفوني للاتصالات بدعم من شركة سيسكو العالمية بتزويد بمعدات وأجهزة المشروع.

5- المعوقات الادارية وتدرج تحتها غموض المفهوم ومن تنفيذ هكذا مشروع يحتاج الى عملية تغيير على صعيد المؤسسات والأقسام والشعب وإعادة توزيع المهام والصلاحيات ما يستلزم تغير في القيادات الادارية والمراكز الوظيفية في ضوء التخصصات الجديدة التي يحتاجها التحول الرقمي ما يقود ذلك الى عملية مقاومة من قبل البنى الوظيفية التقليدية في المؤسسات الحكومية.

6- التحديات المالية أن عملية التحول الرقمي في مؤسسات الدولة والمحافظة عليها من الاختراق والهجمات الالكترونية تحتاج الى بنية تحتية متطورة ومبالغ مالية ضخمة، لأن هذه

التقنيات في حالة تطور مستمر لا يفيد معه التكاسل أو الاعتماد على الانظمة المعلوماتية الالكترونية القديمة.

7- الأتمتة لا تتم بالضرورة بصورة صحيحة أو منهجية، وكان من المفترض ان تعمل على التعاون الرقمي الذي يتطلب منك أن تقوم على وفق مبادئ معينة"، واوضح صفد الشمري رئيس مجلس المسار الرقمي العراقي" حينما تتحدث عن حكومة إلكترونية، فإنها ليست نظاما رقميا ممكناً إنجازه خلال اليوم أو يومين أو سنة او سنتين، ومن ثم تعمل عليه الحكومة الرقمية من دون تشبيك رقمي بين الوزارات، ومن ثم عندما تتحدث عن حكومة إلكترونية من دون تشبيك معناه إنه لن يكون لدينا حكومة إلكترونية لمدة 50 سنة تقريبا، ومن ثم علينا أن نتحرك على التشبيك ومن ثم تنتقل إلى موضوعة الحكومة الإلكترونية"[25].

وعلى الرغم من تحديات للتحول الرقمي إلا أن العراق ماضي بعملية التحول الرقمي وهو ما أكده الأمين العام لمجلس الوزراء العراقي حميد الغزي أن التوجه الحكومي هو تحقيق التحول الرقمي الشامل، وضرورة الاسراع في استكمال مشروع الحكومة الإلكترونية وتوسعة الخدمات الالكترونية المقدمة لتحقيق التحول الرقمي الشامل وتسهيل الاجراءات الخاص بحصو المواطن على خدمة حكومية متكاملة، واستعرض فريق دائرة مركز البيانات الوطني الحكومي أبرز الانجازات المتحققة هي خدمات الكترونية بالتعاون مع المؤسسات الحكومية المستفيدة ضمن المنصة الإلكترونية- أور-، كما شملت تطبيق (راقبني)، وأنظمة (فحص العوز المناعي للوافدين الأجانب، والشهادات الجامعية، وأجندة مجلس الوزراء، والخطط المستقبلية التي تعمل عليها الدائرة تمثلت بأنظمة (فحص الأحياء، وشهادات الوفاة، وخدمات الماء والكهرباء، وإيصال التيار الكهربائي للمواطنين، وتمكين الأجيال، وفحص الجرحى، والأملاك العقارية، وحفر الآبار، والتسجيل في المدارس)، فضلا عن تخصيصه رقم الهاتف (5599) لتقديم الخدمات الإرشادية إلى المواطنين، للاستعلام عن آليات استخدام الأنظمة في المنصة الإلكترونية، واتجهت عدد كبير من الوزارات الحكومية العراقية نحو خطوات التحول الرقمي[26].

في مقابل هذا التحول الرقمي النسبي والمتواضع لنجد هناك تهديدات لهذا التحول وهو الهجمات التي تتعدد وفق الآتي[27]:

أ- حسب الاسلوب المستخدم.

1- هجمات التصيد تحفيز الضحية لفتح رابط يحتوي على برمجة خبيثة تصيب الجهاز.

2- هجمات وقف الخدمة عبر اغراق الضحية بالآلاف الرسائل والطلبات التي تؤدي في النهاية الى انقطاع الخدمة ووقفها.

3- الابواب الخلفية ثغرات موجودة على أجهزة الضحية بهدف التجسس أو جمع المعلومات.

ب- حسب القطاع والهدف المستهدف: قد يكونوا أفراد عاديين يتم اختراقهم بهدف الابتزاز أو شركات خاصة لسرقة الملكية الفكرية أو القطاع المالي والمصرفي بهدف الاضرار باقتصاد الدولة أو سرقة الاموال أو خدمات حكومية أو أجهزة أمنية لسرقة معلومات استخباراتية أو خطط عسكرية.

ت- حسب الفواعل المشاركة يقوم بهذه الهجمات قوات رسمية وغير رسمية أو مجموعات إرهابية أو إجرامية.

وهذه التهديدات للتحول الرقمي نابع من الضعف في مجال الأمن الالكتروني، التي يمكن اجملها بالآتي[28]:

- **نقص الوعي:** لا يزال الوعي بمخاطر الأمن الالكتروني محدودًا بين أفراد المجتمع والمؤسسات الحكوميَّة والخاصة، الأمر الذي يُعيق قدرتهم على اتخاذ خطوات فعّالة لحماية أنفسهم من الهجمات الإلكترونية.
- **نقص الكوادر المتخصصة:** يعاني العراق من نقصٍ حادٍ في الكوادر المتخصصة في مجال الأمن الالكتروني، ما يعيق قدرته على التصدي للهجمات الإلكترونية بكفاءة.
- **البنية التحتية الرقمية الضعيفة:** لا تزال البنية التحتية الرقمية في العراق ضعيفة، ما يجعلها عرضة للاختراقات والهجمات الإلكترونية.
- **غياب القوانين والتشريعات:** لا يوجد في العراق قوانين وتشريعات كافية لحماية الفضاء الإلكتروني من الهجمات الالكترونية، ما يعيق قدرة السلطات على ملاحقة المتورطين في هذه الهجمات.

وأعلنت شركة تريند مايكرو العالمية الرائدة في مجال الأمن السيبراني في 2023/7/17 عن نتائج تقريرها السنوي للأمن السيبراني، والذي كشف عن زيادة ملحوظة بنسبة 55٪ في عمليات اكتشاف التهديدات العالمية، وكذلك زيادة هائلة على مستوى الملفات الخبيثة المحظورة بلغت نسبة 242٪ في عام 2022، وقدر تعلق الامر بالعراق نجحت حلول الشركة

باكتشاف وحظر أكثر من 15 مليون تهديد عبر البريد الإلكتروني، وقامت بحماية أكثر من 400 ألف مستخدم من التضرر من روابط خبيثة قاموا بالضغط عليها، كما استطاعت تحديد وإيقاف أكثر من نصف مليون هجوم لبرمجيات خبيثة في الدولة، وهذا يكشف لنا حجم التهديدات الالكترونية[29].

الخاتمة

العراق في ظل السياسات العبثية للنظام السياسي قبل عام 2003 جعلته متأخرًا عن باقي دول البيئة الاستراتيجية العالمية والاقليمية تكنولوجيًا ورقميًا، وبعد دخول التكنولوجيا بعد العام 2003 وعمليات التطور المستمرة عالميًا وعلى المستوى الداخل العراقي أصبحت التكنولوجيا في متناول مواطني الدولة بعد ظهور شبكة المعلومات الدولية-الانترنيت-إلا أن هذا التطور التكنولوجي لم يكن بالمستوى المطلوب في مؤسسات الدولة الرسمية ودخولها بشكل محدود ونسبي ما جعل الدولة العراقية مستمرة بإجراءاتها البيروقراطية المعقدة في ظل ما شهدته الدولة العراقية بعد عام 2003 من ظروف استثنائية من أوضاع أمنية وسياسية غير مستقرة ثم تلاه ذلك بسيطرة عصابات داعش الارهابي على بعض المناطق العراقية ما جعل الدولة العراقية بمؤسساتها منشغلة بالقضاء على هذا التهديد الارهابي الوجودي نيابة عن دول العالم هذا الهدف الذي غطى على الأهداف الأخرى التي كانت مرسومة ضمن البرامج الحكومية للدورات المتتالية، في ظل هذا الوضع كان العراق في مراتب متأخرة في مؤشرات التحول الرقمي مقارنة مع دول البيئة الاستراتيجية الاقليمية والعالمية وهذا انعكس في سوء جودة الخدمة المقدمة للمواطن العراقي وهذا ما يلمسه المواطن عند زيارته أو قراءة للتقارير عن التحولات الرقمية في باقي دول العالم فكان على الدولة العراقية لازمًا عليها أن تلحق بركب التحول الرقمي العالمي لاسيما وأن تعاملات الدول على المستوى الرسمي وغير الرسمي مرتبط بالتكنولوجيا والتحول الرقمي مغادرين التعاملات الورقية، هذا التأخير في التحول الرقمي ليس نتاج سبب واحد بل نتاج مركب لأسباب من ضمنها أن الموظفين في بعض دوائر الدولة ذات عقليات رجعية ونقص خبرة لا ترضى بالتطور والتحول الرقمي، وضعف البينة التحتية التكنولوجية ونحن في ظل التحول الرقمي لعدد من مؤسسات الدولة نلحظ ان شبكة المعلومات الدولية-الانترنيت- التي لابد أن تزود بها مؤسسات الدولة ضعيفة لا ترقى للقيام بالعمليات الرقمية المرتبطة بالمؤسسات الحكومية كون التحول الرقمي يجعل الفساد الاداري والمالي المرتبط

بالمؤسسات الحكومية يقل مقابل ارتفاع درجة الشفافية والنزاهة وبيان حقيقي لإيرادات الدولة المالية والمتحقق منها.

وعلى الرغم من التحول الرقمي النسبي والمتواضع للدولة العراقية إلا أنه يواجه تحديات لتنعكس على الأمن الوطني العراقي منها أن التحول الرقمي يحتاج إلى أقمار أصطناعية ووسائط نقل لبيانات المواطنين خاصة بالدولة العراقية لحفظ بيانات المواطنين امنيًا، وعدم تسريبها أو اطلاع الدول الاخرى عليها وهذا مرتبط بالسيادة العراقية وهو ما لا تملكه الدولة العراقية أو اتجاهها الى شركات القطاع الخاص لتصميم برامج التحول الرقمي ما يجعل هذه الشركات مالكة لمفاتيح الولوج الى هذه البرامج ومن الممكن معرفة نقاط الضعف في هذه البرامج الالكترونية الرقمية، كما لاننسى عمليات الاستهداف المستمرة لبرامج التحول الرقمي من قبل عصابات الجريمة المنظمة أو التنظيمات الإرهابية لأغراض تخريبية أو وقف عجلة التقدم أو لأغراض سياسية. وفي نهاية مطاف هذه الرحلة العلمية نذكر أهم الاستنتاجات وهي:

1- تدريب الكوادر الوظيفية باختلاف مستوياتها على عمليات التحول الرقمي.
2- جودة شبكة المعلومات الدولية-الانترنيت- لابد أن تكون ممتازة وجيدة بالمستوى المطلوب لعمليات التحول الرقمي.
3- امتلاك أقمار اصطناعية خاصة لخزن بيانات المواطنين وعدم تسريبها لجهات أخرى أو اطلاع الدول الأخرى عليها.
4- وضع استراتيجيات استباقية ووقائية وضرورة التحديث المستمر لبوابات أمان التحول الرقمي لمؤسسات الدولة الرسمية، لمنع حالات الانتهاكات التي تستهدف مؤسسات الدولة على المستوى التكنولوجي والرقمي.
5- وضع القوانين والتشريعات اللازمة لحماية الفضاء الالكتروني والرقمي.
6- ضرورة تبسيط الاجراءات المصاحبة للعمليات الادارية الرقمية وعدم جعلها مشاها للعمليات الادارية الروتينية التقليدية.

المصادر والمراجع:

[1] هناء عفيف و هيبة خولوفي، الاتجاه نحو التحول الرقمي: حتمية او خيار؟، مجلة اقتصاد المال والاعمال، المركز الجامعي لميلة، الجزائر، العدد1، 2022، ص282.

[2] محمد سالم، اتجاهات التحول الرقمي، مجلة افاق مستقبلية، مركز المعلومات ودعم اتخاذ القرار، مصر، العدد3، 2023، ص291.

[3] خيرة شاوشي وزهرة خلوف، التحول الرقمي في الجزائر، مجلة المحاسبة التدقيق والمالية، جامعة خميس مليانة، الجزائر، العدد1، 2023، ص19.

[4] لبني سحر قاري، دراسة تحليلية لمحددات نجاح التحول الرقمي في الشركات، المجلة الجزائرية للاقتصاد والمالية، جامعة يحي فارس بالمدية، الجزائر، العدد15، 2021، ص35.

[5] رانية تقاوة وبشامة شوام، التحول الرقمي كخيار استراتيجي في ظل الانتقال نحو الاقتصاد الرقمي في الجزائر: دراسة استكشافية، مجلة الاقتصاد والبيئة، جامعة بن باديس مستغانم، الجزائر، العدد1، 2023، ص422؛ صدوقي غريسي واخرون، واقع واهمية التحول الرقمي والاتمتة، مجلة اراء للدراسات الاقتصادية والادارية، المركز الجامعي افلو، الجزائر، العدد2، 2021، ص ص101-102

[6] لمزيد من التفاصيل ينظر: موسى بن قاصي، عصر الثورة الرقمية: حبة جديدة في مسار تطور البشرية، في عبدالقادر دندن محررًا، العلاقات الدولي في عصر التكنولوجيا الرقمية : تحولات عميقة ومسارات جديدة، مركز الكتاب الاكاديمي، الجزائر، 2021، ص ص25-36.

[7] صدوقي غريسي واخرون، مصدر سبق ذكره، ص103؛ محمد بوعتلي، تنمية الحكومية الرقمية كعامل اساسي لتحقيق التحول ارقمي في الدول العربية: دراسة تحليلية وتصنيفية باستخدام تقنية التحليل العنقودي الهرمي خلال سن 2022، مجلة المنتدى للدراسات والابحاث الاقتصادية، جامعة زيان عاشور بالجفلة، الجزائر، العدد2، 2023، ص ص94-95.

[8] محمد بوعتلي، مصدر سبق ذكره، ص ص94-95.

[9] عائشة بنت احمد الحسني وشذا بنت عبدالمحسن الخيال، اثر تطبيق انظمة الادارة الالكترونية على الاداء الوظيفي: دراسة ميدانية على موظفات العمادات في جامعة الملك عبدالعزيز بجدة، المجلة العلمية لقطاع كليات التجارة، جامعة الازهر، العدد10، 2013، ص ص54-55.

[10] موسى بن قاصي، مصدر سبق ذكره، ص27.

[11] خيرة شاوشي وزهرة خلوف، مصدر سبق ذكره، ص19.

[12] حسين قوادرة، التفاعلات النزاعية في قوالب سيبرانية: الصورة الجديدة للصراع الدولي، في عبدالقادر دندن محررًا، العلاقات الدولي في عصر التكنولوجيا الرقمية : تحولات عميقة ومسارات جديدة، مركز الكتاب الاكاديمي، الجزائر، 2021، ص ص53-54.

[13] لمزيد من التفاصيل ينظر: خديجة حام، الانظمة المعلوماتية في مواجهة القرصنة والتخريب: المخاطر المحدقة والحلول الناجعة، في مجموعة مؤلفين، الأمن المعلوماتي: مهدداته وسبل الحماية، مؤتمر كلية الاداب واللغات، جامعة مولود معمري بتيزي، الجزائر، 3-2015/11/4، ص ص37-41.

[14] منى عبدالله السمحان، متطلبات تحقيق الامن السيبراني لأنظمة المعلومات الادارية بجامعة الملك سعود، مجلة كلية التربية، جامعة المنصورة، مصر، العدد 111، 2020، ص11.

[15] جميلة سلايمي ويوسف بوشي، التحول الرقمي بين الضرورة والمخاطر، مجلة العلوم القانونية والسياسية، جامعة الوادي، الجزائر، العدد2، 2019، ص ص962-963.

[16] ابراهيم بولمكاحل، تجليات الارهاب السيبراني: داعش ونهج الخلافة الرقمية، في عبدالقادر دندن محررًا، العلاقات الدولي في عصر التكنولوجيا الرقمية : تحولات عميقة ومسارات جديدة، مركز الكتاب الاكاديمي، الجزائر، 2021، ص ص141-142؛ مسيكة محمد، الفضاء السيبراني وتحديات الامن القومي للدول، مجلة العلوم القانونية والاجتماعية، جامعة زيان عاشور بالجفلة، الجزائر، العدد4، 2022، ص456.

[17] ليلى بعولي، التهديدات في الفضاء السيبراني وانعكاساتها على السيادة الرقمية: القرضنة الالكترونية نموذجًا، ستراتيجيا مجلة دراسات الدفاع والاستشراف، المعهد العسكري للوثائق والتقويم، الجزائر، العدد16، 2021، ص ص8-9، ص11.

[18] نانيس عبدالرزاق فهمي، مستقبل الامن السيبراني في عصر الميتافيرس، مجلة افاق مستقبلية، مركز المعلومات ودعم اتخاذ القرار، مصر، العدد3، 2023، ص305.

[19] عبدالقادر معبد، الشابكة والأمن المعلوماتي، في مجموعة مؤلفين، الأمن المعلوماتي: مهدداته وسبل الحماية، مؤتمر كلية الاداب واللغات، جامعة مولود معمري بتيزي، الجزائر، 3-2015/11/4، ص138.

[20] خالد مخلف الجنفاوي، التحول الرقمي للمؤسسات الوطنية وتحديات الأمن السيبراني من وجهة نظر ضباط الشرطة الاكاديميين بالكويت، المجلة العربية للآداب والدراسات الانسانية، المؤسسة العربية للتربية والعلوم والآداب، مصر، العدد19، 2021، ص ص86-87.

[21] هند عبدالمجيد حمادي ووفاء جعفر امين، سوق العمل العراقي من التقليدي الى الرقمية: تحديات ومعالجات، المجلة العراقية للعلوم الاقتصادية، العدد69، 2021، ص ص119-120؛ سمي مزغيش، وفق النموذج الاماراتي: كيف تساهم الحكومة الالكترونية في تحسين الحياة اليومية،، في عبدالقادر دندن محررًا، العلاقات الدولي في عصر التكنولوجيا الرقمية : تحولات عميقة ومسارات جديدة، مركز الكتاب الاكاديمي، الجزائر، 2021، ص ص434-435.

[22] ماد ناجي احمد، منهجية علمية للتحول الرقمي في العراق، دائرة البرامج الاستشارية الحكومية، وزارة التخطيط العراقية، 2021، ص13.

[23] محمد بوعتلي، مصدر سبق ذكره، ص97.

[24] حازم حمد موسى، الرؤية الاستراتيجية للأمن الوطني العاق في الفضاء السيبراني: مقاربة بين المعضلة الأمنية والمكنة الادائية، المجلة الجزائرية للعلوم القانونية والسياسية، جامعة الوادي، الجزائر، العدد5، 2020، ص551.

[25] ذو الفقار المحمداوي، العراق يتجه صوب التحول الرقمي، صحيفة المدى اليومية، العدد5575، 2023/12/13، شبكة المعلومات الدولية-اترنيت- https://almadapaper.net/view.php?cat=303367.

[26] موقع بغداد اليوم، العراق يقترب من تحقيق التحول الرقمي الشامل، 2021/11/9، شبكة المعلومات الدولية-انترنيت-https://baghdadtoday.news/170724-.html.

[27] مسيكة محمد، مصدر سبق ذكره، ص455.

[28] احمد الجسار، الامن السيبراني: تحد جديد يوجه العراق، جريدة الصباح اليومية، 2024/3/13، شبكة المعلومات الدولية-انترنيت--https://alsabaah.iq/93360 ..html

[29] موقع شفق نيوز، 20 مليون تهديد في العراق: تقرير الامن السيبراني يكشف حصيلة 2022، 2023/3/17، شبكة المعلومات الدولية-انترنيت- https://shafaq.com.

ملف العدد
الأمن السيبراني
درع التحول الرقمي العراقي
(بين التحديات الراهنة وضرورات المستقبل)

تحليل التحول الرقمي في العراق
بين التحديات والفرص

م.د. تمارا كاظم الاسدي
الجامعة المستنصرية/ كلية العلوم السياسية

إنَّ التحولات التي يشهدها العالم اليوم تؤكد على الحاجة الملحة للاعتماد على الوسائل الرقمية والإدارة الإلكترونية في مرحلة ما بعد البيروقراطية لاسيّما في ظل سيطرة الشركات العالمية وتقدم تكنولوجيا المعلومات والاتصالات، فالتحول الرقمي في العراق يعد تحدياً كبيراً وفرصة مهمة في آنٍ واحد، إذ يواجه العراق تحديات مثل ضعف البنية التحتية لتكنولوجيا المعلومات والاتصالات، وقلة الوعي التكنولوجي، واختراق الأمن الرقمي، ومع ذلك قد تتاح فرص جديدة مثل تحسين التواصل بين الحكومة والمواطنين، وتعزيز الشفافية والفعالية في تقديم الخدمات الحكومية، وتحسين البنية التحتية لتكنولوجيا المعلومات والاتصالات، وتعزيز تواجد الحكومة الإلكترونية فضلاً عن تعزيز بيئة الأعمال وتحفيز الابتكار والنمو الاقتصادي وتعزيز الحماية السيبرانية لضمان سلامة البيانات والتحولات الرقمية في البلاد، وعليه فإن تعزيز التحول الرقمي العراق وتحقيق هذا الهدف يتطلب إنشاء برنامج حكومي جديد يتضمن برنامجًا شاملا للتحول الرقمي، مدعوماً بنظام قانوني متكامل يهدف إلى تحقيق أهداف ترشيد الخدمة العمومية.

الكلمات المفتاحية: التحول الرقمي، العراق، الأمن الرقمي.

Digital Transformation Analysis in Iraq
Between Challenges and Opportunities

DR. TAMARA KADIM Al-Asadi
Al Mustansiriya University/College of Political Science

The transformations that the world is witnessing today underscore the urgent need to rely on digital means and post-bureaucratic e-governance, especially in the context of global corporate ownership and ICT delivery Digital transformation in Iraq is a major challenge and an important opportunity simultaneously, Iraq faces challenges such as weak ICT infrastructure new opportunities such as improved communication between the Government and citizens, enhancing transparency and effectiveness in the delivery of government services and improving ICT infrastructure,

الاستلام 2024/02/18
الارجاع 2024/04/01
القبول 2024/05/28

Enhancing the presence of e-government as well as enhancing the business environment, stimulating innovation and economic growth and enhancing cyber protection to ensure data integrity and digital transformations in the country Thus, promoting Iraq's digital transformation and achieving this goal requires the establishment of a new government program that includes a comprehensive digital transformation program, Supported by an integrated legal system aimed at achieving the objectives of streamlining the public service.

Keywords: Digital Transformation, Iraq, Digital Security.

المقدمة

أن موضوع التحول الرقمي يشغل مكانة مهمة ويتناول بشكل واسع النطاق في الوقت الحاضر، فعلى الرغم من أن العالم يتجه نحو التقنية والرقمنة بشكل متسارع، إلا أن البقاء في مجال المنافسة يتطلب من كل منظمة أو شركة أن تتبنى التحول الرقمي، إذ أن انتشار التقنيات الحديثة، لاسيّما في مجال الإلكترونيات ووسائل الإعلام والاتصالات والإنترنت، أدى إلى دخول عصر التحول الرقمي، حيث يقوم الاقتصاد على التكنولوجيا والمعرفة والمعلومات، ولم يتوقف هذا التوجه نحو الاندماج في الاقتصاد الرقمي عند التغيرات الهيكلية العالمية، بل أصبح يعد ميزة تنافسية للعديد من الدول، وفي الوقت نفسه يعد تهديدًا للدول التي ما زالت تتأخر في هذا المجال، فالتحول الرقمي يحمل العديد من الفوائد الإيجابية التي تجعله ضروريًا لاستمرارية النجاح والتميز، فبفعل التحول الرقمي شهدت الدول المتقدمة والعربية وتحديداً العراق تغييرًا كبيرًا فقد قامت بتنفيذ استراتيجيات واضحة لتعزيز هذا التحول بهدف تعزيز التنمية الاقتصادية والاجتماعية والحد من الفجوة بين الدول المتقدمة والنامية.

أهمية البحث:

وتأتي دراسة موضوع التحول الرقمي في العراق من كونه ذات أهمية كبيرة لتسليط الضوء على الأثر الإيجابي الذي يمكن أن يحققه التحول الرقمي في تطوير القطاعات المختلفة في البلاد، إذ يتيح التحول الرقمي فرصًا هائلة لتحسين الكفاءة وتسريع عمليات العمل، مما يعزز التنافسية ويدعم النمو الاقتصادي من خلال الاعتماد على الابتكار والتكنولوجيا في تعزيز التنمية الشاملة وتحقيق التقدم في العراق.

هدف البحث:

أن الهدف من البحث يتمثل في استكشاف وتحليل التحديات التي تواجه عملية التحول الرقمي في العراق كالعوائق التقنية والتنظيمية التي تعترض سبيل تبني التكنولوجيا الرقمية في البلاد، وكذلك استكشاف السبل لتجاوز هذه التحديات، فضلاً عن تحليل الفرص المتاحة في مجال التحول الرقمي بما يساهم في توجيه السياسات والاستراتيجيات اللازمة لتعزيز التحول الرقمي في العراق وتحقيق الفوائد الشاملة لهذه العملية.

فرضية البحث:

يقوم البحث على فرضية تتعلق بتوضيح تأثير التحول الرقمي على العراق عبر تحديد العوامل التي تعوق تبني التكنولوجيا الرقمية في البلاد وكيفية التغلب عليها، فضلاً عن استكشاف الفرص المتاحة لتعزيز التحول الرقمي وتحقيق النمو الاقتصادي.

اشكالية البحث:

وتأتي اشكالية البحث تتساءل عما إذا كان التحول الرقمي في العراق حتمية ناتجة عن ثورة تكنولوجيا المعلومات والاتصالات، أم هو خيار استراتيجي لمواجهة البيروقراطية وتحقيق أهداف مشروع الحوكمة الالكترونية في العراق، وتشمل هذه الإشكالية مجموعة من الأسئلة الفرعية، منها:

- ما مفهوم التحول الرقمي؟
- ما هي التحديات الرقمية الأكثر شيوعاً في العراق؟
- هل هناك فرص امام تحقيق نجاح التحول الرقمي في العراق؟
- كيف يمكن تحديد مستقبل التحول الرقمي في العراق؟

منهجية البحث:

اعتمد البحث على المنهج التحليلي وذلك لتحليل وتقييم التحديات التي تواجه التحول الرقمي في العراق وتقديم استنتاجات دقيقة حول التحديات التي تواجه عملية التحول الرقمي، فضلاً عن المنهج المستقبلي الاستشرافي للوصول إلى النتائج المطلوبة، ومن ثم سيتم تقسيم البحث إلى عدة مجالات هي:

- التحول الرقمي: تأصيل نظري لفهم شامل.

- تقييم نقدي لتحديات التحول الرقمي في العراق.
- فرص التحول الرقمي: بوابة العراق نحو التنمية الاقتصادية.
- رؤية لمستقبل التحول الرقمي في العراق.

أولاً- التحول الرقمي: تأصيل نظري لفهم شامل.

يعرف التحول الرقمي بأنه:" العملية التي تستلزم نموذج عمل وقدرات تقنية ورقمية مبتكرة، تجمع بينها الابتكار في إنتاج منتجات وخدمات إبداعية، مما يجعلها تتفوق على الطرق التقليدية في تقديم الخدمات"، ويهدف التحول الرقمي إلى تحسين الكفاءات التشغيلية وتقليل التكلفة، وزيادة نسبة امتلاك العملاء والجمهور، بهدف التفوق على المنافسين، فالتحول الرقمي يمثل عملية انتقال للمنظمات إلى نموذج عمل يعتمد على التقنيات الرقمية لابتكار منتجات وخدمات مبتكرة، وتوفير فرص جديدة لزيادة الإيرادات وتحسين قيمة منتجاتها[1].

كما تعرف عملية التحول الرقمي على أنها: استخدام التقنيات الرقمية الحديثة لتغيير نموذج الأعمال، وتوفير فرص جديدة للدخل والقيمة المضافة، والانتقال إلى الاقتصاد الرقمي عبر التحول التقني والإداري والتسويقي"[2].

كذلك يعد التحول الرقمي عمليةً أو مجموعة عمليات ديناميكية تسعى إلى التكيف مع احتياجات المستفيدين المتغيرة، من خلال بناء نماذج عمل ومنتجات جديدة تستفيد من التقنيات الرقمية لتحسين تجربة المستخدم ورفع جودة الأداء والكفاءة التشغيلية، مع التركيز على دعم الابتكار الرقمي، ففي ظل انتشار واسع لاستخدام التكنولوجيا الرقمية في العالم اليوم، أصبح التحول الرقمي أحد أهم المواضيع في الأولويات الاستراتيجية للقطاع العام والخاص، فقد أدركت دول العالم أهمية تبني برامج مبنية على استراتيجيات وخطط مدروسة لتحقيق التحول الرقمي في عصر الرقمنة، وقد اتسعت عمليات الرقمنة لتشمل جميع الوظائف والمسائل والإجراءات والعمليات الحيوية في المجتمع الرقمي، بما في ذلك الاقتصاد الرقمي والتعليم الرقمي والصحة الرقمية والتجارة الرقمية والحكومة الرقمية[3]، إلا أنه بالرغم من تلك الاهمية في ظل انتشار استخدام الإنترنت ووسائل التواصل الاجتماعي، أصبح النشاط الرقمي يتعرض لتحديات تتعلق بالحريات والخصوصية والأمان، ويتضمن ذلك رغبة بعض الدول في التحكم في الفضاء الرقمي ومراقبة مواطنيها، وتهديدات مثل التجسس والاختراقات الإلكترونية التي

قد تؤدي إلى تعريض الأفراد والمنظمات للخطر، ومن هنا نشأ مفهوم (الأمن الرقمي) الذي يهدف إلى حماية الأفراد والجماعات والمنظمات من التهديدات والمخاطر على الإنترنت، سواءً كانت تلك التهديدات تتعلق بالاختراقات الإلكترونية، أو التجسس، أو التهديدات التي تستهدف السلامة الشخصية والمعلوماتية[4].

ومن خلال مجمل التعاريف السابقة يتضح لنا التحول الرقمي يمثل استخدام جميع التقنيات الرقمية المتاحة لتحسين أداء الشركات واستبدال العمليات القديمة ببدائل رقمية جديدة، مما يؤثر على جوانب الأعمال بشكل شامل، لا يقتصر فقط على التكنولوجيا[5].

وبناءً على ذلك يمكننا استنتاج أن التحول الرقمي يمثل تغييرات جذرية في نموذج الأعمال والعمليات، سواءً في القطاع الخاص أو الحكومي، إذ يمكن أن يتضمن تغييرات شاملة في منتجات، أو خدمات المؤسسة وكذلك في طرق تقديمها، ويشمل التحول الرقمي تدخلات استراتيجية تؤثر على جميع جوانب المؤسسة من المبيعات إلى التوريد، وتكنولوجيا المعلومات وسلسلة القيمة بأكملها، ويهدف هذا التحول إلى تحقيق تحسينات كبيرة في الأداء، فضلاً عن حماية البيانات والمعلومات من الاختراقات وتعزيز هوية المؤسسة لتميزها عن المنافسين وبناء هوية فريدة لها[6].

ثانيا- تقييم نقدي لتحديات التحول الرقمي في العراق.

منذ ظهور التكنولوجيا الرقمية والثورة المعلوماتية ، بدأت المجتمعات تواجه تغيرات سريعة، فقد أدت الأهمية المتزايدة للمعرفة إلى جانب العولمة والآثار المترتبة على التطور التكنولوجي وثورة المعلومات والاتصالات في عصر الثورة الصناعية الرابعة إلى إيجاد عالم مختلف تماماً، عالم اندماج التكنولوجيات الرقمية وتغلغلها السريع في البنية التحتية لكل مؤسسة مثل المؤسسات المالية والاتصالات والنقل والتعليم والرعاية الصحية وغيرها، وساهمت في حدوث تقارب بين تلك التكنولوجيات، إذ تندمج مجموعة كبيرة من التكنولوجيات التي تشتمل على إنترنت الأشياء والحوسبة السحابية وتحليل البيانات الضخمة والذكاء الاصطناعي لتوجد نظاماً بينياً يتيح استفادة متبادلة بين مختلف أنواع التكنولوجيات بحيث تستفيد كل واحدة من الأخرى وتساهم في تطويرها. وبذلك وجدت الدول والمجتمعات على حد سواء نفسها أمام فرص وتحديات غير مسبوقة، إذ أصبحت المعلومات المنشورة عبر الإنترنت هي الأكثر

هيمنة على الحياة، لذلك من الواجب معرفة المهارات الأساسية للتعامل معها بشكل سليم، وحمايتها من المخاطر[7].

ومن هذا المنطلق واجهت الحكومة الرقمية في العراق تحديات تتمثل في محدودية الوصول إلى التكنولوجيا والبنية التحتية الرقمية، مما يؤثر على قدرتها على تقديم الخدمات للمواطنين في جميع أنحاء البلاد، بجانب ذلك من ناحية هناك نقص في المهارات والقوى العاملة الرقمية، وتعقيدات بيروقراطية في مؤسسات الدولة تعيق المشاريع الرقمية، ومن ناحية أخرى صعوبة التصدي لتهديدات الأمن الرقمي وحماية البيانات الحساسة للدولة والمواطنين، مع زيادة حالات الهجمات السيبرانية والإرهاب الإلكتروني[8]، فقد بدأ تسجيل إحصائيات رسمية حول الجرائم السيبرانية في العراق منذ عام 2006، نظراً للزيادة الكبيرة في الخدمات الإلكترونية والعمليات عبر الإنترنت، مما أدى إلى زيادة في جرائم الإنترنت والأنشطة المضرة بالمجتمع، وهنا يلاحظ أن نسبة القرصنة السيبرانية في العراق تعد الأعلى في الشرق الأوسط، إذ تنوعت حالات الجرائم السيبرانية وشملت الغش عبر الإنترنت، وغسيل الأموال، والتجارة غير المشروعة، والتطفل على الشبكات، والجنس، والإرهاب الإلكتروني، ومنذ الفترة من عام(2006 إلى 2011) زادت حالات جرائم الإنترنت في العراق بمعدل سنوي متوسط قدره (2.246%) وكانت معظم هذه الجرائم تُرتكب من قبل أشخاص حاصلين على شهادات ثانوية وبكالوريوس فأظهرت البيانات أن الشباب كانوا الأكثر ارتكابًا لهذهِ الجرائم لاسيّما الذكور الذين شكلوا نسبة كبيرة منها، وهذا يشير إلى ضرورة توجيه جهود الحماية من الجرائم الرقمية نحو فئة الشباب والمراهقين[9].

وعليه، من الواضح كذلك أن الطابع التكنولوجي ساهم في إيجاد طرق جديدة للصراع بديلة للحرب المباشرة بين الدول، إذ ساهمت الآليات التكنولوجية في مساعدة المنظمات والدول في التنسيق بين جهودها والتفاعلات فيما بينها الكترونيا بعيداً عن الاتصال المباشر، وأدت الثورة التكنولوجية الى تغير شكل الحرب وأدواتها والفاعلين فيها مما ساعد على اختلاف درجة التهديد وآثاره وطبيعته ومصادره وظهور حرب الشبكات وحروب الفضاء الإلكتروني، وأصبح الارهاب جريمة عابرة للحدود القومية من حيث النشاط والخطط والتمويل والأعضاء، وتصاعد نشاط الجماعات الارهابية عبر الفضاء الإلكتروني وتعزيز بعدها العالمي وتم استخدام المنجزات التكنولوجية في ممارسة الارهاب، والتي استطاع الارهابيون

من خلالها تحقيق أضرار غير متوقعة وهائلة تتجاوز التهديدات التي تمثلها الدول لبعضها البعض، اذ استغلت الجماعات الارهابية بكافة أشكالها وأنماطها الفكرية المزايا الالكترونية كعنصر حيوي لدعم وتحقيق أهدافها، وتحولت بعد أن كانت مجموعات قلائل من الأفراد متوزعة جغرافياً الى مجتمع افتراضي غير محدد الأبعاد الكمية، وجدير بالذكر هنا انه بالتزامن مع الحرب على تنظيم داعش الارهابي منذ العام 2014 رصدت شركات أمنية مختصة بالأمن الرقمي أن هناك حرباً رقمية في العراق يتم فيها استخدام وسائل التواصل الاجتماعي لحشد المؤيدين ونشر الدعاية وجمع المعلومات الأمنية، إذ قام تنظيم داعش باستغلال الإنترنت لتحقيق أهدافه سواءً العسكرية، أو الدعائية، ووفقاً لما أكده العديد من الخبراء بالرغم من السيطرة المحكمة على الشبكة الدولية فالكثير من العمليات الإرهابية التي يقوم بها التنظيم يؤدي فيها (Google Earth) الدور الأكبر كوسيلة إعلامية[10].

وفي سياق التحديات الرقمية تعرض العراق في 26 و 27 أيلول عام 2019 إلى هجوم سيبراني استهدف ما يقارب الـ(30) موقعًا حكوميًا، بما في ذلك مواقع وزارات الدفاع والداخلية والخارجية والأمن الوطني والصحة، وقد استغل المهاجمون ثغرات معينة لتنفيذ تغييرات في بيانات موقع البحث، مما أدى إلى توجيه المستخدمين إلى صفحات بحث مزيفة. وعلى الرغم من نجاح الجهات الحكومية في استعادة بعض المواقع بسرعة، إلا أن بعضها استغرق وقتًا أطول فتمكن المهاجمون من الوصول إلى أجهزة الحواسيب الحكومية واختراق قواعد البيانات المحمية، مما أتاح لهم الحصول على معلومات حساسة، وبعد ذلك حذرت لجنة الأمن البرلمانية من خطورة مثل هذه الهجمات في المستقبل، إذ قد تؤدي إلى تسريب معلومات أمنية مهمة وحساسة[11].

وبشكل عام من الواضح أن العراق، رغم عدم استقراره العام، يواجه صعوبات في التكيف مع تحديات الفضاء الرقمي في ظل انتقال المجتمعات إلى الفضاء الافتراضي بسرعة لاسيّما أنه يعاني من نقص البنية التحتية والموارد البشرية التي تدعم التفاعل الإيجابي مع هذه التحديات، فعلى الرغم التحسن الذي شهده موقع العراق في مؤشر الأمن السيبراني العالمي في عام 2018، اذ احتل المرتبة(107) عالمياً والمرتبة(13)عربياً، إلا أنه شهد تراجعاً كبيراً في عام 2020 فقد انخفض إلى المرتبة (129) عالمياً من بين (184) دولة، والمرتبة (17) عربياً، بدرجة تبلغ(71.20)[12].

وعند التحقيق في أسباب تراجع العراق في مجال الأمن الرقمي نجد أن الجهود الحكومية في هذا الصدد شهدت تراجعاً وذلك لعدة أسباب هي:-

1. ضعف القوانين والتشريعات الحكومية المتعلقة بالأمن المعلوماتي والرقمي، الأمر الذي يتطلب تبني تشريعات قانونية فعّالة وتطبيقها على القطاع الحكومي والخاص، ويمكن للحكومة تعزيز الأمن الرقمي من خلال تنفيذ إجراءات أمنية محددة في الوزارات والمؤسسات الحكومية فضلاً عن القطاع الخاص.
2. ضعف القدرات المهنية المحلية في مجال أمن المعلومات المتقدمة، الأمر الذي يتطلب التركيز على تدريب وتطوير كوادر مهنية محترفة في القطاعين الحكومي والخاص لتمكينهم من مواجهة التحديات الرقمية.
3. ارتباط منظومات الإنترنت في العراق بالخارج، مما يستدعي إقامة شراكات فعّالة مع شركات محلية لتعزيز الأمن الرقمي وبناء علاقات موثوقة وفعّالة لسد النقص في هذا المجال.
4. قلة إدراك الشركات المحلية لحجم المخاطر الأمنية المعاصرة في مجال تكنولوجيا المعلومات، الأمر الذي يستدعي تطوير الوعي بالتحديات الأمنية والبحث عن حلول جديدة للتطورات الأمنية، بما يضمن الابتعاد عن الوسائل التقليدية والاستفادة من تكنولوجيا المعلومات المتقدمة[13].
5. تراجع دور فريق الاستجابة للأحداث الرقمية، الذي يعمل تحت إشراف مستشارية الأمن القومي العراقي، مما أثر على حماية الشبكات ومراكز البيانات والمواقع الرسمية في الفضاء الالكتروني.
6. تأخر التصويت على قانون جرائم المعلوماتية، مما أثار مخاوف بشأن الحريات العامة.
7. قلة عدد المؤتمرات وورش العمل والندوات حول الأمن الرقمي مقارنة بالدول المجاورة مثل السعودية.
8. تقليل الاستثمار في الأمن الرقمي مقارنة بالدول المجاورة مثل إيران التي تخصص مليار دولار سنوياً لهذا القطاع.
9. غياب بنية تحتية متكاملة في مجال الأمن الرقمي وعدم وجود هيئة وطنية مسؤولة عنه.

10. عدم تأدية العراق دوراً فاعلاً في المنتديات الدولية المعنية بالأمن الرقمي[14].
11. عمومًا، يمكن تحديد بعض التحديات التي يعاني منها التحول الرقمي وشبكات الإنترنت ومن بينها:-

أ. مخاطر أمن المعلومات لاسيّما فيما يتعلق بعمليات القرصنة الإلكترونية.
ب. ضعف الكفاءة في استخدام التكنولوجيا داخل المؤسسات، وتأثير البيروقراطية.
ج. نقص الخبرة للموظفين في استخدام تكنولوجيا المعلومات والاتصالات.
د. التحديات التشريعية والقانونية التي قد تبطئ عمليات التحول الرقمي.
ه. غموض المفهوم لدى بعض القادة الإداريين، مما يتطلب توضيحاً وتوعية أكبر.
و. مقاومة التغيير من قبل بعض الموظفين والقيادات الإدارية ، إذ يقاوم بعض الموظفين في المؤسسات المالية والمصرفية التحول إلى أنظمة الدفع الإلكترونية.
ز. الحاجة المتزايدة للإمكانيات المادية لتبني التكنولوجيا الحديثة، وصعوبة مواكبة التطورات التكنولوجية[15].
ح. ضعف البنية التحتية: إذ يواجه العراق تحديات في البنية التحتية الرقمية، مثل انقطاع التيار الكهربائي ونقص الإنترنت.
ط. نقص الوعي: فلا يزال الكثير من العراقيين غير مدركين لفوائد الدفع الإلكتروني.
ي. قلة ثقافة الدفع الإلكتروني: إذ أن اغلبية الشعب العراقي يفضلون استخدام النقود بدلاً من الدفع الإلكتروني.
ك. صعوبة العثور على كوادر متخصصة: تواجه المؤسسات المالية صعوبة في العثور على موظفين مؤهلين في مجال التكنولوجيا المالية.
ل. صعوبة تسريح الموظفين: لا يوجد سند قانوني لتسريح الموظفين الحكوميين، مما يجعل من الصعب على المؤسسات المالية الحكومية التكيف مع التغييرات في مجال التكنولوجيا المالية[16].

وفي نفس الوقت مع تشكيل الحكومة الحالية برئاسة (محمد شياع السوداني) في 13 تشرين الأول 2022 واجهت تحديين ماليين عند تشكيلها سرقة القرن، وأزمة ارتفاع سعر صرف الدولار، إلا أن تضمن البرنامج الحكومي إصلاح النظام المصرفي العراقي من خلال

إلغاء الموظفين الفضائيين، والتحول نحو نظام مصرفي أساسي، فضلاً عن إصدار قرارات حكومية منذ عام 2023 لتعزيز الدفع الإلكتروني تمثلت بالآتي[17]:-

- إلزام جميع المدارس والجامعات والمحطات تجهيز الوقود بفتح حسابات مصرفية وأجهزة نقاط البيع.
- إلزام جميع المراكز والمحال التجارية والمطاعم والصيدليات والدوائر الحكومية وغير الحكومية والنقابات والجمعيات بفتح حسابات مصرفية وأجهزة نقاط البيع.
- تتولى المصارف الحكومية والخاصة توفير أجهزة نقاط البيع إلى الجهات المذكورة آنفاً وغيرهم من الزبائن لتحصيل الأموال الكترونيا.
- إيداع (20%) من أجور الساعات الإضافية الممنوحة للموظفين في حساباتهم المصرفية لاستخدامها في الدفع الإلكتروني فقط.
- إعفاء التعاقدات واستيراد أجهزة الدفع الإلكتروني من الرسوم والضرائب.
- إعفاء جميع التعاملات بالدفع الإلكتروني من الضرائب.
- تنظيم ورش عمل تضم المصارف وشركات الدفع الإلكتروني واتحاد الغرف التجارية والنقابات وذوي العلاقة لتقديم أفكارهم ومقترحاتهم في مجال تقديم الحوافز والتسهيلات التي من الممكن اعتمادها في إنجاح المشروع.
- إلزام المصارف وشركات الدفع الإلكتروني بتوفير تطبيق الكتروني (مجاني) على الهاتف النقال يتيح للزبائن الدفع بواسطة الهاتف والاستعلام عن أرصدتهم وتعاملاتهم المالية وإعداد تقارير بالفواتير المدفوعة المتعلقة بأنظمة الدفع الإلكتروني.

إلا إن تطور عمليات الدفع الإلكتروني في العراق لا يزال في مراحله الأولية، فالتحول الرقمي يتطلب توفير العديد من الخدمات المتكاملة، إذ لا يزال الدفع النقدي يسود في العديد من مجالات حياة المواطنين، مثل دفع أجور الماء والكهرباء. فضلاً عن الإجراءات الحكومية الحالية ليست كافية لتعزيز الثقافة المصرفية والدفع الإلكتروني بشكل فعّال، ولذلك يجب اتخاذ إجراءات تشجيعية مثل تقديم خصومات على الجباية وضمان استمرارية مجانية الخدمة، وبالنظر إلى المشاكل التي نتجت جراء فرض عمولة على المعاملات الإلكترونية في بداية تطبيق

الخدمة في عام 2023، فقد تم تأجيلها مرارًا لغاية آذار 2024 بناءً على رفض واستجابة المواطنين، وكل تلك العوامل تستدعي جهوداً متعددة المستويات لتخطيها وضمان نجاح عمليات التحول الرقمي[18].

وبشكل عام يتضح أن من الضروري للبلدان التي تحاول التعافي من الحروب مثل العراق فهم حالة الأمن الرقمي وتحدياته والمخاطر المحتملة التي قد تواجهها من خلال دراسة مناهج متعددة للأمن الرقمي والاطلاع على نماذج وأطر أمنية تم تطويرها وتنفيذها في العالم المتقدم، مع تعديلها وتصميمها وفقًا لاحتياجات ومتطلبات المؤسسات الاقتصادية في العراق ومدى اعتمادها على تكنولوجيا المعلومات والاتصالات، وبالتالي اتخاذ هذا الإجراء كخطوة رئيسة لتجنب أي تهديد للأمن القومي خلال عملية التحول الرقمي.

ثالثا- فرص التحول الرقمي: بوابة العراق نحو التنمية الاقتصادية.

أن تحول الحكومة الرقمية في العراق يتيح فرصًا متعددة لتحسين العمليات الحكومية وتعزيز التنمية الاقتصادية بالاعتماد على التكنولوجيا الرقمية، فيمكن تعزيز الكفاءة والإنتاجية في العمليات الحكومية، وتحسين تقديم الخدمات العامة، وتعزيز الشفافية والمساءلة، كما هو مُبين في إصدار البطاقة الموحدة والبطاقة التموينية (الغذائية)، التي تؤدي إلى زيادة الكفاءة والإنتاجية، وتقليل التكاليف واستخدام الموارد بشكل أكثر فعالية لاسيّما مع استعمال تحليلات البيانات والأتمتة، ومع ذلك، ينبغي مراعاة البعد الأخلاقي في تنفيذ واستعمال تقنيات الذكاء الاصطناعي[19].

ليس هذا فقط إنما هناك توقعات بعيدة المدى حول إمكانات العملات الرقمية التي تعمل كمنصات للمعاملات الجديدة بأن تصبح تقنية سلسة في احداث فرص نحو تحقيق التنمية الاقتصادية في البلد من خلال[20]:-

1. مستوى المجهولية أو الشفافية الذي تقدمه منصات العملات الرقمية والتبادل سيكون له عواقب على تتبع تدفق التبادلات، ففي الوقت الذي أصبحت فيه عملة البتكوين سيئة السمعة جزئيا لارتباطها بالسوق السوداء عبر الإنترنت المعروف بأسم(Silk Road) ، فإن ثبات دفتر العملات الرقمية وشفافيته قد يوفر فرصاً للحد من الاحتيال والخطأ في المدفوعات.

2. العملة الرقمية قد تيسر فهم أكبر للتدفقات النقدية فهي تمد ببيانات أفضل وأكبر حول المبلغ الإجمالي واستخدام النقود في النظام، كذلك توفير فوائد أشمل للشفافية والبحث، وقد يسهم ذلك أيضاً في تيسير إدارة استقرار الاقتصاد الكلي من جانب المصارف المركزية، وفي ايجاد صورة أوضح عن رد فعل السوق الفوري تجاه سياسات، أو تغييرات معينة في الأوضاع الاقتصادية.
3. منصات التبادل الجديدة قد توسع نطاق الأسواق المالية من خلال تغيير ممارسات المعاملة باستعمال اتصال بالإنترنت أو شبكة الهاتف؛ مما يجعل المعاملات والخدمات المالية الأخرى متاحة للسكان الذين يعتمدون حالياً على التبادل النقدي.

ونتيجة لذلك فأن إعادة تشكيل النهج التعاوني والشراكة بين الإنسان والآلة يعد أمراً حيوياً لاستفادة كاملة من إمكانيات الذكاء الاصطناعي في تحديد مخابئ الأسلحة والإرهابيين، إذ ينبغي أن يشكل النهج التعاوني هذا جسراً يجمع بين قدرات البشر والقوة التحليلية للذكاء الاصطناعي، ولا يستبدل الذكاء الاصطناعي الخبرة البشرية والحكم عبر تبني علاقة تكافلية، فيمكن تحسين تعزيز فعالية العمليات الأمنية والعسكرية من خلال استعمال مسؤول وفعال للذكاء الاصطناعي في هذا السياق[21].

ومن هنا تعد الثقافة التنظيمية جانبًا حاسمًا من النضج الرقمي كأحد أبعاد العوامل الثقافية لتحقيق أهداف التحول الرقمي بفعالية؛ لأن الثقافة تؤدي دورًا هاماً في تشكيل قدرة العراق على الخضوع للتحول الرقمي الناجح، إذ تعد مواءمة الثقافة التنظيمية مع المبادرات الرقمية أمرًا ضروريًا لقيادة التغيير وتعزيز الابتكار وضمان استدامة جهود التحول الرقمي[22]، كما يسهم التحول الالكتروني في ربط القطاعات الحكومية أو الخاصة ببعضها إذ يمكن أنجاز الأعمال المشتركة بمرونة، وقد أصبحت الضرورة أكثر الحاحاً لتحول المؤسسة رقمياً، ويرجع ذلك إلى التطور المتسارع في استعمال وسائل وأدوات تكنولوجيا المعلومات في كافة مجالات الحياة سواء كانت متعلقة بالمعاملات مع القطاع الحكومي أو القطاع الخاص أو كانت تخص الأفراد، لذا فهناك ضغوط من كافة شرائح المجتمع على المؤسسات والهيئات والشركات لتحسين خدماتها وأتاحتها على كافة القنوات الالكترونية[23]، ونتيجة لذلك أصبح التحول الرقمي من الضروريات بالنسبة لكافة المؤسسات والهيئات التي تسعى إلى التطوير وتحسين خدماتها ووصولها للمستفيدين لعدة مزايا تتمثل في[24]:-

أ. التوقعات العالية من المستفيدين: إذ يتوقع المستفيدون من خدمات الدفع الإلكتروني تجارب شخصية مصرفية سلسة ومريحة.

ب. التحول نحو النظم الإلكترونية: تسعى الحكومة العراقية إلى التحول نحو النظم الإلكترونية في جميع القطاعات، بما في ذلك القطاع المالي.

ج. الانفتاح المالي: تسعى الحكومة العراقية إلى الانفتاح على الأسواق العالمية، مما سيؤدي إلى زيادة الاستثمار في مجال التكنولوجيا المالية.

وانطلاقاً مما سبق التحول الرقمي يعد جيداً في أي منظمة، إذا طبق على أساس تقني كما يقضي التحول الرقمي على الكثير من سلبيات العمل الإداري من الواسطة ، والمحسوبية ، والمحاباة، والعمل الممنهج والبيروقراطية، وعمليات غسيل الأموال والارهاب ..الخ, ويضع آليات وتوقيتات محددة لإنجاز الأعمال , ويغلق المنافذ أمام ضعاف النفوس الذين يتاجرون بقضاء حوائج الناس التي هي جزء لا يتجزأ من صميم عملهم، إلا أنه قد يقع البعض في اخطاء التحول الالكتروني مثل التركيز على اكتساب التكنولوجيا بدلاً من استعمالها، ومطالبة كل قسم بالتحول الرقمي كل على حدة دون العمل على التحول الرقمي في إطار متكامل ومتناسق، وأخيراً التركيز على استحداث المميزات دون النظر إلى مدى رغبة العملاء أو مدى تناسبها مع خبراتهم وقدراتهم، إذ يرتبط مفهوم التحول الرقمي لدى المجتمع باستعمال التكنولوجيا، والأصل في الأمور هو القيام بضبط الإجراءات المتعلقة بأداء الخدمات الحكومية كخطوة ضرورية لنجاح عملية التحول الرقمي، فالتكنولوجيا ليست هدفًا في حد ذاتها، ولكنها وسيلة يجب استعمالها بكفاءة لتحقيق أهداف محددة[25].

خلاصة القول اعتقد أن فرص التحول الرقمي في العراق تحقق تقدم ملحوظ في مختلف القطاعات، مما يبرز نمواً كبيراً في توسع المشهد الرقمي في البلاد، فقد أتاح الرصد الفوري وجمع البيانات من خلال اعتماد الفواتير الإلكترونية والإبلاغ الضريبي الرقمي والترويج النشط لأساليب الدفع عبر الإنترنت والإيداع الضريبي الإلكتروني من قبل الحكومة تسليط الضوء على الإمكانات الكبيرة للنمو والتنمية الاقتصادية في مختلف القطاعات، واخيراً فإن الانتقال إلى العمل عن بعد، وظهور أسواق عمل جديدة ذات خصائص مميزة تؤكد المشهد الديناميكي للرقمنة في العراق.

رابعا- رؤية لمستقبل التحول الرقمي في العراق.

تعد التكنولوجيا الطريق الأسرع للقضاء على كل التعقيدات ومنها البيروقراطية، لذا من الضروري تحديث المواقع الالكترونية بشكل مستمر وطرح المزيد من الخدمات خلالها؛ لأنها تشكل إضافة كبيرة ونقلة نوعية على مستوى الخدمات المقدمة وتشكل حافزاً اكبر لإنجاز كافة المعاملات بالسرعة المطلوبة، وأن التحول الرقمي للخدمات الحكومية أصبح خياراً ضرورياً للخدمات في المؤسسات الحكومية ولم يعد من الخيارات الترفيهية، بل أصبح خياراً استراتيجياً، لهذا من الضرورة الانتهاء من تحويل جميع الخدمات المقدمة للأفراد الى خدمات الكترونية، وذلك ضماناً لسرعة انجاز المعاملات ولإزالة المعوقات التي من الممكن أن تشكل تحدياً امام انجاز المشاريع ، ومن المهم تجاوز البيروقراطية التي ربما تشكل عائق امام تسريع الخدمات، وأن اغلب دول العالم قد أحدثت نقلة نوعية على مستوى الخدمات الالكترونية المقدمة للجمهور ولاسيّما خلال انتشار جائحة كورونا، إذ تم تفعيل كافة المنصات الالكترونية التي تساهم في تخليص المعاملات بنسبة(95%) وهذا انجاز جيد، وهناك بعض الجهات الخدمية تحتاج الى المزيد من التفعيل للقضاء على البيروقراطية وتسريع الخدمات الحكومية، اذ أن البيروقراطية تشكل في معظم دول العالم عائقا امام التقدم، لذلك قد سعت معظم الدول الى انجاز بدائل سريعة وقد نجحت أكثرها عبر حكومتها الالكترونية في تقديم خدمات رائدة في معظم المجالات وما زلنا بانتظار المزيد في العراق ولاسيّما من القطاعات الحيوية التي تقدم خدمات مباشرة للجمهور[26].

وعند التفكير في سيناريوهات مستقبلية للتحول الرقمي في العراق، يمكن استكشاف عدة احتمالات تأتي بتحديات وفرص متنوعة للبلد وللمجتمع تتمثل في[27]:-

أولاً- احتمال تحول رقمي متأخر: هذا المشهد هو وضع الأمان الجزئي فيصبح الفضاء الإلكتروني مجالًا للصراعات الرقمية غير مُسيطر عليه، مما يتيح للقراصنة وجماعات الجريمة المنظمة والجيوش الإلكترونية إحداث تأثير واسع النطاق، فقد تتصاعد حدة الصراعات بين مختلف الفواعل، ويصبح الفضاء الرقمي غير آمن للاتصالات والتجارة والأعمال والخدمات، إذ يتواجد مناطق غير آمنة بينما يظل بعض المناطق آمنة للأعمال والاتصالات قادرة على مواجهة تحديات الصراع الرقمي، وطالما العراق يواجه تحديات في تبني التكنولوجيا وتطبيق

الخدمات الرقمية في القطاعات المختلفة في الاستثمار والكفاءات الرقمية يمكن أن يؤدي إلى تأخر في التحول الرقمي وتقليل التنافسية.

ثانياً- احتمال الازدهار التكنولوجي: ينطلق هذا المشهد من وضع الأمان الواسع فالعراق يشهد تطورًا سريعًا في قطاع التكنولوجيا، مع تبني تقنيات حديثة مثل الذكاء الاصطناعي والإنترنت فيصبح الفضاء الرقمي أكثر أمانًا للغاية، إذ يطغى الوضع الدفاعي على الوضع الهجومي، مما يتطلب تطوير تقنيات دفاعية متقدمة، ويتميز هذا الوضع بظهور شبكات معلومات أصغر تتبع الفاعلين المختلفين، ويمكن تجريم تجاوز الحدود فيه، الأمر الذي يجعل العراق مركزًا للابتكار وريادة الأعمال التقنية في المنطقة، وبالتالي يعزز النمو الاقتصادي ويخلق فرص عمل جديدة.

ثالثاً- احتمال الحكومة الذكية: ويقوم هذا المشهد على وضع البلقنة الإلكترونية إذ تسعى الدول والفاعلون لبناء السيادة والحدود داخل الفضاء الرقمي، فتتبنى الحكومة العراقية تكنولوجيا المعلومات بشكل كبير لتقديم الخدمات الحكومية بشكل أسرع وأكثر فعالية وتحسين جودة البنية التحتية وتعزيز الشفافية لضمان نجاح التحول الرقمي.

وبهذهِ الطريقة يمكن الوصول الى حالة الاستغناء عن المستندات الورقية والتحول الى المستندات الإلكترونية ويتحول مجتمع الموظفين من مجتمع ورقي إلى مجتمع إلكتروني، يسهل للجمهور الحصول على الخدمات التي تقدمها الإدارة التي يعمل بها دون تكبد مشقة انتقال الأفراد إلى مقر الجهة الحكومية والوقوف في صفوف ومراجعة أكثر من موقع لمتابعة معاملته، مما يوفر لديه الوقت والجهد لكي يستثمرهما في الأمور الحياتية اليومية والالتفات إلى أمور أكثر أهمية من أن يضيع وقته في هذه المراجعات الحكومية.

ونتيجة لهذا التصور يتبين أن مستقبل التحول الرقمي في العراق مثير للتفاؤل ومليء بالتحديات والفرص، إذ يتطلب نجاح هذا التحول جهوداً شاملة من الحكومة والقطاع الخاص، والمجتمع المدني لتحقيق نجاح مستدام، وباختصار يمكن للعراق أن يحقق تقدم كبير نحو التحول الرقمي من خلال اتباع احتمال مختلط يجمع بين مشهد الازدهار الالكتروني والحكومة الذكية؛ مما يعزز مكانته في الساحة العالمية ويساهم في بناء مستقبل مزدهر للأجيال القادمة.

الخاتمة:

يعد التحول الرقمي مدى مفتوح لجميع أفراد المجتمعات الذين يمتلكون قدرة الوصول إلى شبكة الإنترنت، مما يمكنهم من الوصول إلى المعلومات والتواصل وإجراء الاتصالات، بفعل التطورات التكنولوجية في مجال الاتصالات والمعلومات وتزايد الاعتماد عليها، وإن المتتبع لمختلف صور تطبيق الرقمنة في العراق، وعلى الرغم من النتائج المهمة المحققة والمساهمة في القضاء على مختلف الصور السلبية التي كانت تعاني منها الإدارة في صورتها التقليدية، إلا أنها في المقابل ما زالت تعاني الكثير من صور النقص والقصور، وباستمرار العمل على تطوير التحول الرقمي في العراق، تظهر فرص هائلة مع تحديات ملحوظة تستوجب الانتباه والتفكير العميق للتعامل مع قضايا مثل نقص البنية التحتية الرقمية ونقص الكفاءات الرقمية التي تحتاج إلى استراتيجيات فعّالة للتغلب عليها من خلال استثمارات موجهة نحو تكنولوجيا المعلومات وتطوير الكفاءات الرقمية، فيمكن للعراق الاستفادة من الفرص المتاحة لتحسين جودة الخدمات وتعزيز النمو الاقتصاد لتحقيق تفوق مستدام والوصول إلى مستوى جديد من التقدم الاقتصادي والاجتماعي.

وفي الختام، يُعد التحول الرقمي في العراق فرصة عظيمة لتحقيق التنمية والازدهار للبلد في حالة عمل الحكومة والمجتمع المدني والقطاع الخاص معًا للتغلب على التحديات وضمان نجاح التحول الرقمي.

المقترحات:

توصل البحث إلى جملة من المقترحات والطرق التي يمكن أن يكون فيها التحول الرقمي في العراق مفيدًا تتمثل بالآتي:-

1- تقييم المخاطر: وذلك عبر تقديم دورات تدريبية على استخدام الحواسيب لمكافحة الأمية الإلكترونية ورفع وعي المواطنين حول التكنولوجيا الرقمية.
2- تحديث السياسات: إنشاء بوابة حكومية إلكترونية للخدمات العامة لتبسيط الإجراءات الإدارية الرقمية، وتوفير التدريب لصناع السياسات لتعزيز قدرتهم على التنبؤ بالتغيرات وصياغة تشريعات تعزز الأمن الرقمي.
3- تخصيص الموارد: تحديد أولويات الاستثمار في التقنيات الرقمية والتدريب وتعزيز الشراكات لمواجهة تحديات الحرب السيبرانية المتوقعة.

4- تعزيز التعاون والشراكات: دعم التعاون بين أصحاب المصلحة المحليين والدوليين لبناء شراكات تستند إلى فهم مشترك للتهديدات وتعزيز القدرات الاستجابة وآليات الدفاع الجماعي.

5- الابتكار والتكيف: تحفيز المؤسسات للابتكار في تقنيات الأمن الرقمي والتكيف المستمر مع التهديدات المتطورة للبقاء في مقدمة الأمان الرقمي.

6- الاستعداد للازمات: تطوير خطط الطوارئ واستراتيجيات الاستجابة للتعامل مع الأزمات الرقمية، مما يقلل من تأثيرها ويعزز جاهزية المؤسسات لمواجهتها.

وبتنفيذ هذه المقترحات، يمكن تعزيز التحول الرقمي في العراق وتحفيز تطور مجتمع متفهم للتقدم التكنولوجي ومستعد لمواجهة التحديات الرقمية المستقبلية.

المصادر والمراجع:

[1] حمدي جليلة ايمان، دور الحوكمة الرقمية في انجاح وتفعيل التحول الرقمي نموذج دولة الامارات العربية المتحدة، مجلة الدراسات القانونية والاقتصادية، العدد3(الجزائر:2023)، ص848.

[2] غادة علي عبد المعطي محمد، التحول الرقمي في السياحة المصرية (المفهوم- التحديات-المتطلبات)، المجلة الدولية للتراث والسياحة والضيافة، العدد2(الاسكندرية: جامعة الفيوم، 2019)، ص493.

[3] حرفوش مداني، التحول الرقمي حتمية ما بعد البيروقراطية أم خيار استراتيجي في عصر الرقمنة، مجلة حوليات جامعة الجزائر1، العدد37(الجزائر:2023)،ص496.

[4] الامن الرقمي وحماية المعلومات، (مركز هردو لدعم التعبير الرقمي:2017)، ص6.

[5] معنان فتيحة، التحول الرقمي كآلية لتدعيم التسويق السياحي والفندقي، رسالة ماجستير غير منشورة، جامعة الشهيد حمه لخضر الوادي، الجزائر، 2022، ص7.

[6] علي حسين جميل الشبلي، أثر التحول الرقمي في تحقيق الرشاقة الاستراتيجية دراسة حالة دائرة الجمارك الاردنية، رسالة ماجستير غير منشورة، جامعة الزرقاء، الاردن، 2022، ص16.

[7] سالي سعد محمد، الأمن السيبراني ودور الجامعات في تعزيزه لدى الطلبة، (مركز حمورابي للبحوث والدراسات الاستراتيجية، 2022)، ص2.

[8] احمد محمود القيسي، الحكومة الرقمية في العراق: التحديات الفرص، (مركز الدراسات الاستراتيجية كربلاء، 2023)، في:
https://bit.ly/3wSX1m2

[9] مصطفى ابراهيم سلمان الشمري، الأمن السيبراني وأثره في الأمن الوطني العراقي، مجلة العلوم القانونية والسياسية، العدد1(جامعة ديالى:2021)، ص170-171.

[10] سالي سعد محمد، أثر الارهاب الالكتروني على المستوى الدولي، (شبكة النبأ المعلوماتية،2020)، في:
https://bit.ly/3PpOIER

[11] مصطفى ابراهيم سلمان الشمري، مصدر سبق ذكره، ص174-175.

[12] باسم علي خريسان، الامن السيبراني في العراق: قراءة في مؤشر الامن السيبراني العالمي 2020، (مركز البيان للدراسات والتخطيط:2021)، ص8-9.

[13] مصطفى ابراهيم سلمان الشمري، مصدر سبق ذكره، ص175.

[14] باسم علي خريسان، مصر سبق ذكره، ص10.

[15] راما حسين اسحق، التحول الرقمي وأثره على تحسين رضا المواطن عن جودة الخدمات الحكومية دراسة ميدانية مركز خدمة المواطن الالكتروني، رسالة ماجستير غير منشورة، الجامعة الافتراضية السورية، سورية، 2021،ص19-20.

[16] قضية وتحليل الدفع الالكتروني للأموال في العراق، نشرة منشورة ، العدد8(مركز المنصة للتنمية المستدامة: كانون الثاني 2024)، ص10-11.

[17] المصدر نفسه، ص5-7.

[18] قضية وتحليل الدفع الالكتروني للأموال في العراق، مصدر سبق ذكره، ص7.

[19] احمد محمود القيسي، مصدر سبق ذكره.

[20] كاثرين ستيوارت وآخرون، العملة الرقمية ومستقبل المعاملات، مؤسسة راند، (كاليفورنيا:2017)، ص5-6.

[21] ايهاب عنان سنجاري، من البايت إلى المعارك دور الذكاء الاصطناعي في جهود مكافحة الارهاب، (مركز النهرين للدراسات الاستراتيجية، 2023)، في:

https://www.alnahrain.iq/post/915

[22]Roman Teicher, DIGITAL TRANSFORMATION MATURITY: A SYSTEMATIC REVIEW OF LITERATURE,ACTA UNIVERSITATIS AGRICULTURAE ET SILVICULTURAE MENDELIANAE BRUNENSIS,Volume67,Number 6(2019),p8.

[23] أحمد حسن عمر، التحول الرقمي ضرورة في تحسين كفاءة المؤسسات ، (موقع الحوار المتمدن، 2019)، في:

https://m.ahewar.org/s.asp?aid=653310&r=0

[24] قضية وتحليل الدفع الالكتروني للأموال في العراق، مصدر سبق ذكره، ص9-10.

[25] سمية بو مروان، الحكومة الالكترونية ودورها في تحسين الادارات الحكومية : دراسة مقارنة ،(الرياض: مكتبة القانون والاقتصاد للنشر والتوزيع، 2014)، ص10.

[26] غنوه العلواني، خبراء يقترحون حلولا للتغلب على البيروقراطية، (ندوة منشور على شبكة الانترنت2020)، في: https://al-sharq.com/article

[27] سماح عبد الصبور، الصراع السيبراني طبيعة المفهوم وملامح الفاعلين، مجلة السياسة الدولية، العدد ملحق عدد نيسان(القاهرة: 2017)،ص9-10.

ملف العدد
الأمن السيبراني
درع التحول الرقمي العراقي
(بين التحديات الراهنة وضرورات المستقبل)

اليات تعزيز الوعي والتنشئة الرقمية
في العراق بعد العام 2003

م.د. هند محمد عبد الجبار
جامعة تكريت/ كلية العلوم السياسية

تعدُ موضوعات الوعي و التنشئة من اهم الموضوعات في المجتمع وأن التطور المتسارع والمذهل الذي يشهده العالم الرقمي، سوف ينعكس بالتأكيد على مواضيع التوعية والتنشئة، لان العالم الرقمي صار يتدخل في جميع مفاصل الحياة وحتى في طريقة اختيار النسق الذي سوف تستخدمه الأسرة في تنشئة أطفالها، لذلك أصبح من الضروري التوعية بإيجابيات وسلبيات هذا العالم، وأن الهدف من التوعية والتنشئة الرقمية هو ردم الفجوة ما بين سرعة التغيرات الرقمية ومواكبة عمليات التوعية لهذه التغيرات الرقمية، لذلك تم التطرق الى العديد من الآليات التي تساهم في زيادة الوعي الرقمي في المجمع العراقي بصورة خاصة.

الكلمات المفتاحية: الوعي الرقمي، التنشئة الرقمية، المواطنة الرقمية، العراق.

Mechanisms for promoting digital awareness and upbringing in Iraq after 2003

Dr. Hind Muhammad Abdel-Jabbar
Tikrit University \ College of Political Sciences

The issues of awareness and upbringing are among the most important topics in society, and the rapid and amazing development that the digital world is witnessing will certainly be reflected in the issues of awareness and upbringing, because the digital world has begun to interfere in all aspects of life and even in the method of choosing the method that the family will use in raising its children, so It has become necessary to raise awareness of the positives and negatives of this world. The goal of digital awareness and upbringing is to bridge the gap between the speed of digital changes and keeping up with awareness processes for these digital changes. Therefore, many mechanisms that contribute to increasing digital awareness in the Iraqi community in particular were discussed.

Keywords: Digital awareness, digital upbringing, digital citizenship, Iraq.

الاستلام	الارجاع	القبول
2024/03/01	2024/04/28	2024/05/19

المقدمة

إن التطورات الكبيرة التي شهدها العالم بالتوجه بسرعة فائقة الى العالم الرقمي، بمنظومات وأساليب متعددة، سواءً كان ذلك بالبحث العلمي ووسائل الاتصال والتواصل والتجارة، وحكومات إلكترونية تدار من خلالها الدولة حتى صارت الصورة بأن موضوع الرقمية يشكل الاساس في كافة مجالات الحياة.

والتغيرات التي حصلت في العراق والتغيير السياسي وفسحة الحرية والديمقراطية التي بدأ العراق يشهدها، واستخدام التقنيات في جميع مرافق الحياة، لذلك اصبح من الضروري الاهتمام بموضوع الوعي والتنشئة الرقمية، وذلك ناتج من أمرين أولهما حتى يكون هذا الجيل على إطلاع بالتطورات الحاصلة، الأمر الثاني لأجل أن يكون متسلح ضد أي اختراق يهدد الجانب الأخلاقي أو يكون صيد سهل لعمليات الابتزاز وغيرها، لأن العالم الرقمي في الوقت الحاضر بالرغم الايجابيات التي يتمتع بها بجعل العالم أسهل في إنجاز الكثير من الأعمال والسرعة في انجازها بالأخص موضوع الاتصال والتواصل ولكن بالرغم من الكثير من الايجابيات هناك الكثير من السلبيات التي أدركها صانع القرار والمجتمع بدأ يشعر بمكامن الخطر وما يشكله هذا العالم الرقمي من أضعاف الهوية الوطنية، بالإضافة الى ذلك أن هذا العالم الرقمي يوفر للشخص هروب من ضغوطات الحياة والتنصل عن المسؤوليات .

اشكالية البحث

تنطلق اشكالية الدراسة من السؤال الأساسي الآتي: هل أن التطور الكبير والسريع الذي شهده العالم في الجانب الرقمي أنعكس على مستوى الوعي من خلال التنشئة الرقمية.

فرضية البحث

هناك ضغوط كبيرة يتعرض لها الأفراد في جانب الوعي والتنشئة الرقمية، لأن حدود المسؤوليات أصبحت من الصعوبة تحديدها في ظل العالم الرقمي وصعوبة التنشئة بسبب الفجوة التي حصلت في مواكبة تلك التطورات.

اهمية البحث

تنبع الأهمية من تحديد مفهومي الوعي والتنشئة الرقمية وأهميتها للنظام السياسي وللمجتمع لأنها تعد الأساس لإنشاء جيل متسلح بالقيم والمواطنة، أن النظام السياسي يحاول استخدام الكثير من

الآليات الخاصة بالوعي والتنشئة الرقمية، وأن تلك الآليات تحاول في اكساب المواطنين المهارات والقدرات في كيفية إدارة واقعهم الرقمي، وبيان إيجابيات وسلبيات ذلك الواقع، والتعرف على أهمية تلك الآليات الخاصة بالوعي والتنشئة الرقمية ومدى فائدتها للمجتمع.

مناهج البحث

لأجل الإلمام بكل جوانب الموضوع تم أستخدام المنهج الوصفي لأجل وصف الظاهرة موضوعة البحث، وأستخدام منهج تحليل النظم والذي يمثل العالم الرقمي وتأثيراته بالمدخلات والأدوات والتوعية والتنشئة بالمخرجات وكيف تكون علاقة التأثير والتأثر وبالتأكيد أيضاً تم الإستعانة بالمنهج التاريخي.

هيكلية البحث

تم تقسيم البحث الى محوريين، الأول جاء بعنوان مفهوم الوعي والتنشئة الرقمية وبينا فيه مفهوم الوعي الرقمي وأهميته ومفهوم التنشئة الرقمية، والمحور الثاني بعنوان آليات الوعي والتنشئة الرقمية وخاتمة وتوصيات .

المحور الأول مفهوم الوعي والتنشئة الرقمية

أن المجتمعات تسعى في وجودها لتحقيق أمرين اساسيين الأول: هو الحفاظ على البقاء والاستمرارية وهذه غريزة موجودة على صعيد الأفراد والمجتمع، والأمر الثاني: محاولة البقاء بصورة متماسكة في ظل بيئة مليئة بالتجاذبات والتنافرات والتشاحنات، وأن أي نظام سياسي لا يستطيع الحفاظ على مستوى جيد من التماسك في حال عدم الحفاظ على مستوى جيد من الأخلاق، والضوابط والقيم والتي تمثل بقدر عال من الوعي وأساليب جيدة في التنشئة وهذا بالتأكيد يحتاج الى وقفة جميع سلطات ومؤسسات النظام مع المجتمع للوصول إلى مرحلة جيدة في الوعي والتنشئة .[1]

وقبل التعرض إلى المفاهيم التي تم أستخدامها في عنوان البحث من الضروري الإشارة الى مفهوم الرقمية وماذا يعنيه، وللإجابة على ذلك يمكن القول أن مفهوم الرقمية يمثل الطريقة التي تولد وتخزن وتعالج البيانات في حالتين الاولى موجبة وتمثل العدد واحد والأخرى سالبة يمثلها الرقم صفر، ويكونان رقماً ثنائياً بما يسمى نظام العد الثنائي. [2] أن المصطلح يعتبر حديث نسبياً لأنه مرتبط مع الثورة المعلوماتية التي حدثت في القرن الماضي،

تعبر الرقمية عن عملية تحويل المعلومات والعمليات التقليدية إلى صيغ رقمية، حيث يتم تخزينها ومعالجتها باستخدام الحواسيب وتكنولوجيا المعلومات، ويتم من خلالها التحول من النظام الورقي في المعاملات الى النظام الالكتروني سواء في معالجة البيانات وارشفتها بالصورة الإلكترونية، إذ تهدف الرقمية إلى زيادة الكفاءة وتسريع العمليات من خلال الاستفادة من التكنولوجيا، لذلك سنعرض في هذا المحور مفهوم الوعي الرقمي وفي الجانب الثاني مفهوم التنشئة الرقمية .

أولاً : مفهوم الوعي الرقمي والاهميته.

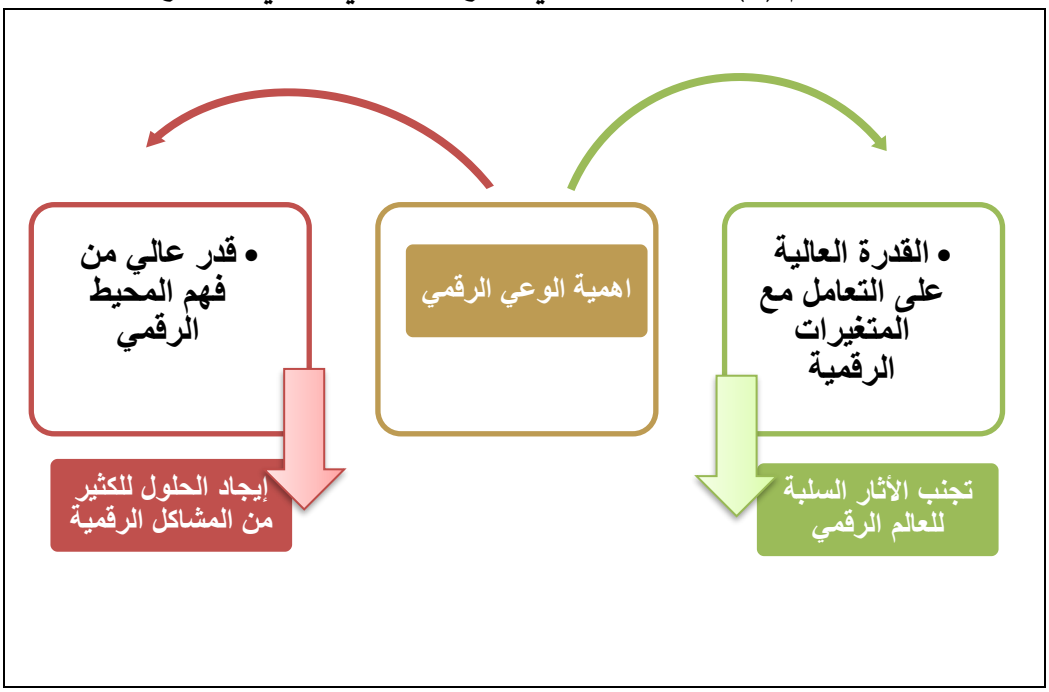
ان الوعي الرقمي هو أحد أدوات التنشئة الرقمية، وهو من المُصطلحات الحديثة التي بدأ الاهتمام بها في العالم الرقمي، ويُطلق عليها أيضاً بالثقافة المعلوماتيّة*، ومحو الأميّة المعلوماتية، ومهارات المعلومات. [3] هذه الثقافة تمكن الناشئ الحاضر والمستقبلي من استخدام المهارات التي تجعلهم مُستخدمين جيدين للتقنيات الرقمية، ومُحلّلين واعين لفاعليّة وكفاءة المعلومات التي يحصلون عليها أو يوجهونها، وأن الوعي الرقمي من الصعوبة اعطاء تعريف دقيق له، لأنه يعتمد على أسلوب المستخدم في العالم الرقمي من أجل الحفاظ على معلوماته وخصوصيته، لذلك يمكن القول ان طريقة استخدام الأفراد للعالم الرقمي تكون بنوعيين الافراد الواعيين هو الذي يلتزم بالقواعد والارشادات اثناء استخدامه للعالم الرقمي، والنوع الثاني هو الذي لا يبالي ولا يتبع القواعد والارشادات بقصد او دون قصد. لذلك يمكن القول أن الوعي الرقمي هو (مجموع المهارات التي يحتاجها الفرد ليستطيعَ العيش في عصرٍ بات يُطلَق عليه اسم العصر الرقمي لذلك، سيساعده وعيه الرقمي في البحث عن المعلومات وتنقيحها، وتقييمها، والوصول إلى النتائج الصحيحة).[4] لذلك يمكن ايضاً تعريفه بأنه إدراك الفرد للمعارف والمهارات التي تتعلق بمجال التقنية الحديثة، وكيفية استخدامها ومعرفة خفاياها، والقدرة على التعامل معها وتوظيفها في الحياة اليومية، والقدرة على حل مشكلاتها. [5]

أن جميع التعريفات التي تناولت مفهوم الوعي الرقمي تصب في توعية المستفيدين ومستخدمي العالم الرقمي، ويمكن القول أن الوعي يشتمل على المهارات التكنولوجية، ومهارات تقيم وإيجاد مصادر المعلومات.[6]

أن الوعي الرقمي يمكن وصفه بالسلاح الحقيقي لمواجهة الكثير من التطورات والتغيرات التي حدثت في العالم، و زادت تلك لأهميته في ظل العولمة وما أنتجته من تطورات في وسائل التكنولوجيا، والتي بات وجود الوعي الرقمي يشكل أهمية لأنه السبيل للخروج من مأزق هذه التغيرات وليس هذا فقط بل لملاحقتها وللتكيف معها بما يخدم الفرد والمجتمع، وتجنباً للأخطار الرقمية وآثارها.

وان الاهمية التي يتمتع بها الوعي الرقمي تنبع من الدور الذي يؤديه في مساعدة الافراد في انتقاء المعلومات الصحيحة بين ملايين المعلومات الموجودة، ومواجهة التغييرات الكبرة التي احدثتها ثورة المعلومات. [7] اما الهدف الاساسي من الوعي الرقمي هو الوصول الى المعلومات الصحيحة، وتطوير المهارات لدى الافراد في كيفية التعرف على المعلومات الحقيقية وتميزها عن المعلومات الخاطئة، والتي يمكن توضيح اهمية الوعي الرقمي من خلال المخطط التالي:

مخطط رقم (1) يبين الاهمية التي يتمتع بها الوعي الرقمي للمجتمع



المخطط من عمل الباحثة بناءً على ما ورد من معلومات في البحث

ثانيا: مفهوم التنشئة الرقمية

أن موضوع التنشئة الرقمية مرتبط باستخدام الأفراد للأنترنيت، بمجالاته المتعددة بعروضه المغرية للحياة وإدارتها بصورة أسهل، لذلك يمكن الربط ما بين التنشئة الرقمية والتنشئة الاجتماعية في أن الأولى هي جزء من الثانية، ويمكن تعريفها بأنها التنشئة التي يحصل عليها الأفراد من اللبنة الاولى وهي الأسرة، لأنها هي وحدها من يعلم الافراد في بداية حياتهم الاستخدام الأمثل لخدمات الانترنيت، مما يؤدي الى تحقيق رغباتهم ولكن دون الخروج عن دائرة الأعراف والعادات والتقاليد أو القاعدة القانونية السائدة في المجتمع. ويمكن تعريفها بأنها ايجاد السبل والطرق الصحيحة لأجل توجيه وتهيئة الأفراد الذين يكونون على تماس مع خدمات الانترنيت وبالأخص الفئة المراهقة، عن طريق تعليمهم بما هو صالح ومواجهة السلوكيات غير المرغوب فيها.[8]

إذن يمكن تعريف التنشئة الرقمية بأنها عملية تثقيف الأفراد بكل الجوانب التكنولوجية والمعلومات المرتبطة بالأنترنيت، وتوعيتهم بمخاطر الاستخدام السيء، عن طريق تسليحهم بالتنشئة الجيدة، المبنية على ثقافة تعزيز من قيم الحوار والمكاشفة.[9]

السؤال الذي يطرح كيف أثرت التحولات الرقمية على الوعي والتنشئة في المجتمع؟

وللإجابة على هذا السؤال أن التحولات الرقمية أثرت على المجتمع لأنها أصبحت مرتبطة بكل مفاصل الحياة ولكن من الضروري على الأسرة والدولة بجميع مفاصلها والاسرة بشكل خاص، تقف أمام تحدي كبير في كيفية الموائمة بين الاستفادة منها وكبح مساوئها، لذلك في كثير من الأحيان يقوم النظام السياسي والمجتمع بتطبيق آليات لتحقيق أكبر قدر من الاستفادة.

المحور الثاني آليات الوعي والتنشئة الرقمية

أن التطور الرقمي كما بينا سابقاً أصبح يغزو كل مفاصل الحياة وهذا يؤثر على النظام السياسي بكل جوانبه سواءً كانت اجتماعية أو اقتصادية أو دينية، كان تأثير التحولات الرقمية في مجال الوعي والتنشئة كبير لذلك حتم على الدولة استخدام سياسات وآليات متعددة من أجل أن يكون النظام السياسي على متابعة بالتأثيرات الرقمية من جهة وكيفية الحد من أثارها

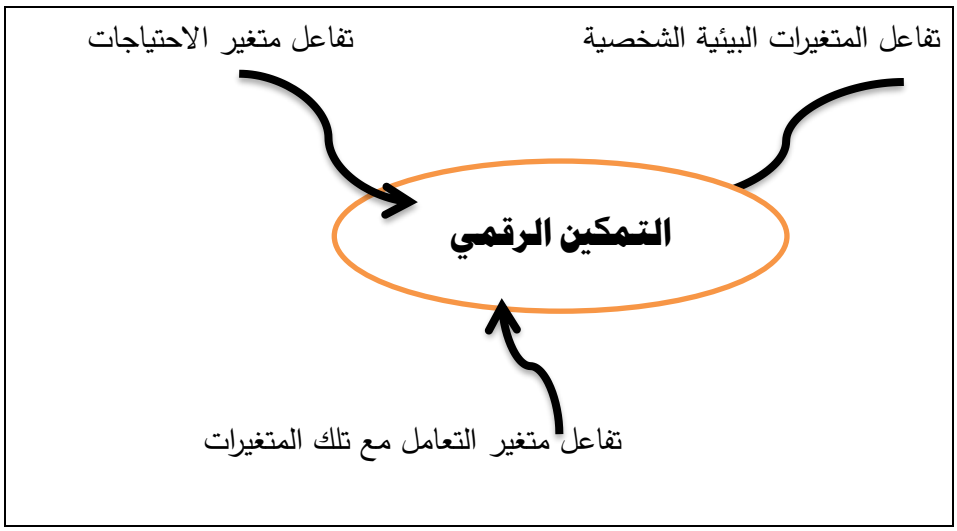
السلبية من جهة اخرى، لذلك تم في هذا المحور تناول العديد من الأليات التي تعمل من اجل السيطرة على تأثيرات العالم الرقمي.

أولاً: اليات تعزيز التمكين* واطلاقات الرقمية

مخطئ من يضن أن عدم ولوج المجتمع في العالم الرقمي هو لأجل حمايته من مخاطر هذا العالم الواسع، ولكن العكس صحيح، أن العالم ومجتمعنا من الضروري أن يكون ضمن المعترك، ولكن علينا في المقابل تمكينه من حيث قوة التنشئة الرقمية وجعله على وعي تام بالأستخدام الفعال لاحتياجات مجتمع المعلومات وقدرته على التميز بين المعلومات الصالحة من غيرها[10]، ومن الضروري أن تكون هذه التنشئة مبنية أساس الأندماج في العالم الرقمي، وتوجيههم بما هو صائب وما هو يشكل خطر.

تكمن اهمية التمكين الرقمي لأنه وسيلة للوصول الى المجتمع الرقمي، لذلك أصبح من الضروري استخدام التقنيات الرقمية من أجل تمكين الأفراد والمجتمع،[11] وأن التمكين يساهم في سرعة أنتاج المعلومات والمعرفة، يمكن القول أن التمكين لا يقتصر على أمر محدد، إنما هو عملية متعددة التوجهات عن طريق وسائل تحفيزية للفرد لزيادة انتاجه في كافة المسائل، وجعله جزء عند اتخاذ القرارات، وقدرته على الاعتماد على نفسه وتحمل المسؤوليات الموكلة إليه، ويمكن القول أن التمكين ينتج بتفاعل العديد من المتغيرات كما موضح في المخطط التالي :

مخطط رقم (2) يبين المتغيرات التي تساهم في التمكين الرقمي.



وأن هذه العملية يجب أن تكون مشتركة مع جميع المؤسسات ونابعة بدايةً من الاسرة وانتهاءً بأعلى سلطة حكومية في الدولة . [12]

ثانيا: الآليةَ الوقائيةَ المؤسساتيةَ

وهذه الالية ترتبط بجميع المؤسسات حيث تبدأ من أصغر مؤسسة في الدولة وهي الاسرة إلى أكبر مؤسسات الدولة المتمثلة بالسلطات الثلاث في الدولة وبالوزارات والمنظمات ..الخ، ان الأسرة تعد أولى الجماعات التي تساعد افرادها على توجيههم في علاقاتهم الإنسانية، لذلك تعد الاسرة المدرسة الاولى لتوجيه افراد عائلتها في مخاطر الانترنيت والعالم الرقمي وان الاسرة هي من تقوم بزرع القيم والاخلاق والسلوك، فيجيلهم من أجل تنشئتهم وادراكهم لجميع المخاطر المحيطة بهم سواءً كانت رقمية أو غير رقمية.[13] يمكن القول ان للأسرة الدور الكبير في الوعي والتنشئة الرقمية من خلال ابراز دورها في النقاط التالية :

1. الأسرة المكان الأول الذي يتم فيه غرس القيم الأساسية المتعلقة بالجانب الرقمي وهذا يتم من خلال الحوار الشامل بين افراد الاسرة ومناقشة وتوجيه الافراد في الأمور التقنية.
2. أن الأسرة تلعب الدور الكبير في تعليم الافراد على ايجابيات العالم الرقمي وعرض السلبيات. ومتابعة سلوكهم في استخدامهم للعالم الرقمي.

من بعد الأسرة تأتي المدرسة إذ تعد من أهم الحلقات المكملة للتنشئة والوعي الرقمي لأنها مؤسسة أجتماعية تربوية وتعليمية، وتتشارك مع الأسرة والنظام السياسي في الدولة لتزويد الأفراد بالمعارف والحقائق العلمية، والأسس التربوية السليمة والسلوك الاجتماعي المقبول والمهارات المهنية التي تسمح له بالتوافق مع بيئته.

لذلك من الضروري على المؤسسة التعليمية أن تُحدث وتُطور من نفسها تماشياً مع القفزات التكنولوجية في العالم الرقمي، وتقديم جميع الاجراءات الاحترازية لأجل تنشئة الجيل[14]

ثالثا: آليةَ اعتماد الاساس الأخلاقي القيمي

تكون هذه الآلية أساسها الاعتماد على مجموعة المعايير والقيم والضوابط الأخلاقية والتي من خلالها يتم تنظيم التعامل في العالم الرقمي وإعلائهِ، من مبدأ المسؤولية والاحترام،

وحتى لو كان العالم الرقمي يفتقر الى القواعد القانونية العامة. وهذا معناه ان من يحكم العالم هي الأخلاق التي أقرب الى ما يكون عملها كعمل الكوابح.

ان التقدم الرقمي الذي حصل في جميع نواحي الحياة تعد نقلة جديدة على الجيل الحالي ولم تعيشها الأجيال السابقة، وأن التطور الكبير في الجانب الرقمي، ومن الضروري اتباع قيم والأخلاقيات مثلما موجود في حياتنا الواقعية يجب أن تكون موجودة في العالم الرقمي. يمكن القول إن العالم الرقمي يكون تحت قاعدة عامة وهي (دعونا نتعامل مع الاخرين بالطريقة التي نحب أن نعامل بها) [15]

وبما أن من يدير العالم الرقمي هم الأفراد، لذلك يكون بالتأكيد هذا العالم يعكس اخلاق من يعمل به ويكون ما يحملونه من أخلاق اساس لتعاملهم.[16]

وأدى انتشار مفهوم (إدمان مواقع التواصل الاجتماعي) إلى نوع من الارتباط (النفسي والسلوكي) على منصات التواصل الاجتماعي، ونتج عنه ضرر فادح في أداء الأفراد في مختلف مجالات الحياة على المدى الطويل، مما أدى الى جعل أكثرهم عرضة لإدمانها مثل الأفراد الذين يعانون من (الخجل الاجتماعي) أو الهشاشة النفسية، فضلاً عن المراهقين.

كذلك إنعدام الخصوصية وانتحال صفة أشخاص وهميين، وسهولة الحصول على بيانات ومعلومات شخصية، مما يؤدي إلى أنتشار حيل النصب والاحتيال والأبتزاز (المادي - الجنسي - العاطفي - السياسي)، والأبتزاز هو محاولة الحصول على مكاسب (مادية أو معنوية أو جنسية بالإكراه أو التهديد)، والا يقومون بفضح أسرار الناس ومعلوماتهم الخاصة.

أن من الصعوبة السيطرة على الموضوع الاخلاقي في العالم الرقمي ولكن يمكن ان نضع بعض الامور التي من الضروري التقييد بها والتي من اهمها: [17]

1- يرتبط هذا الأمر بلوائح تنظيم المحتوى والتي يمكن تعريفها بأنها مجموعة الضوابط الأخلاقية التي تفرض محتويات أخلاقية ملائمة، عبر مختلف الوسائط والمنصات.
2- محاسبة كل من تسول له نفسه بتخريب البنى التقنية وشبكات الانترنيت .
3- الأمر الأخير هو مستوى السلوك الشخصي، القائم على احترام الذات واحترام المقابل وبالأخص المختلف سواء في (الثقافة- الدين – المعتقد – اللون – اللغة) والابتعاد عن المحتوى الذي فيه نشر للكراهية والعنصرية.

لذلك من الافضل الاعتماد على الامانة والنزاهة في التعامل مع المعلومات الرقمية، والحذر عند نقل الاخبار والمعلومات لأنه في حالة النقل غير الصحيح سيكون له أضراره وانعكاسه على المجتمع، ونشر معلومات تبين خطورة الأمر عندما يتجاوز المواطن القوانين او تسول له نفسه للأضرار بمصالحهم.

رابعًا: الآليةَ التشريعيةَ القانونيةَ

أن هذه الآلية بأبسط معنًا لها هو اعداد جيل لديه وعي بحقوقه وواجباته التي عليه، وقدرته على جلب منفعته بصورة شرعية وأن يكون على دراية بالجرائم الرقمية* وانواعها وعقابها.[18]

لذلك من الضروري على صناع القرار توعية المواطنين بأضرار من يعتدي رقمياً وهناك عقوبات مادية وجسدية تطال الشخص المعتدي.[19] وأن التزايد في استخدام العالم الرقمي، صاحبه الكثير من الجدل العلمي والقانوني، لأجل تطوير المنظومة التشريعية وتماشياً مع التطور السريع الذي شهده العالم الرقمي.

من الضروري تغير الصورة المرتبطة بحرية الأفراد باستخدام المنصات المظلمة عبر شبكات الأنترنيت وصياغة تشريعات قوانين تمنع الناس من الدخول لهذه المواقع ، ووضع تشريعات تقيد انتهاك خصوصيات الأفراد وحرياتهم، وضرورة وضع أساس تشريعي للجرائم الحديثة التي كان سببها العالم الرقمي مثل جرائم التحريض، وهتك العرض، والسب والقذف، وعمليات السرقة والنصب والاحتيال والتزوير في البيانات، وحماية الملكية الفكرية.[20]

خامسا: آليةَ تعزيز دور الإعلام لتعزيز الوعي الرقمي

يؤدي الإعلام الدور الكبير وبالأخص بالقرن الحالي ما يسمى الإعلام الرقمي* الدور الكبير في عمليات التنشئة وزرع الوعي الرقمي، واستطاع الإعلام الرقمي أن يجذب أ 8عداد كبيرة وبالأخص من جانب الشباب، والذي يطلق على ذلك العالم بالعالم الافتراضي، وأصبح الجانب الإعلامي إذا نظرنا له من ناحية نظرية بالاعتماد على درجة التأثير، حيث يقوم الأفراد بالاعتماد على الاعلام الرقمي لأجل اشباع احتياجاته، باستخدام وسيلة الإعلام وكلما كانت الوسيلة مهمة إزداد تعلق الأفراد بها.[21]

لذلك صار هناك أمر ضروري وحتمي على صناع القرار ان ينشأ عدد من المراكز الاعلامية التوعوية لأجل توجيه وتنشئة الجيل وتحصينه من الاختراقات الرقمية التي لها انعكاس على استقرار النظام السياسي.

السؤال الذي يطرح نفسه كيف يستطيع الإعلام الرقمي أن يكون آلية للوعي والتنشئة الرقمية؟ وللإجابة عن ذلك ان الإعلام الرقمي اصبح يلعب الدور الكبير في التنشئة، لان الإعلام الرقمي في الوقت الحاضر يعمل في كافة الاتجاهات وبدأ يلائم جميع اذواق وتوجهات الافراد وبدأ يأخذ كثير من الأدوار التي كانت في السابق من اختصاصات الاسرة، حيث بإمكان كل شخص بضغطة زر او لمسة واحدة ان يرى كل ما يحبه. بالإضافة أن الإعلام الرقمي أصبح مرافقاً للأفراد على مدار اربع وعشرين ساعة وبإمكان الفرد الاطلاع عليه في أي وقت وفي أي مكان.[22] لذلك يمكن حصر جزء لما يمثله الإعلام من اهمية في الوقت الحاضر وبما يقوم به من اعمال في الوقت الحاضر بما يلي:[23]

- ضرورة تعاون وسائل الإعلام المختلفة مع الأجهزة الأمنية في اعداد وصياغة الرسائل التوعوية للناس وذلك عن طريق تخصيص برامج وإعلانات منتظمة ومدروسة.
- ضرورة تحديث وسائل الإعلام بكافة أشكالها وأن تبحث دوما عن التطوير في أدائها، وأن تكون خلاقة في طرق تواصلها مع الجماهير لمد جسور الثقة فيها وبينهم، خاصة وانها تحيا في ظل منافسة قوية من وسائل الإعلام الأخرى في ظل العالم الرقمي .
- تقنين وتحجيم من حجم ما يبث من خلالها من برامج لا ترتقي الى المستوى المطلوب والتي تهدف إلى تحقيق الربح الكبير وقلة الاستفادة منها ويمكن وصفها بأنها تلويث للعقول وإثارة للغرائز .
- أن تكون الوسائل الاعلامية تحت اشراف الدولة وان تضع اللوائح القانونية لأجل تنظيم عملها.

سادسا آليةَ المواطنةَ الرقميةَ *

أن الدولة في حالة سيطرتها على الآليات سابقة الذكر، ستصل الى مواطن قادر على مواجهة أي اختراق يحاول النيل منه واسقاطه في بؤرة الجرائم الالكترونية، أن المواطنة الإلكترونية تحاول أن تبني شخصية الأفراد وتسلحهم بالأخلاق ويكونون مسؤولين أمام ما

يعتنقونه من أفكار ومعتقدات. لذلك يمكن القول إن المواطنة الرقمية بأبسط صورها هي توجيه وحماية في نفس الوقت من ناحية توجيه نقصد به نحو منافع التقنيات الحديثة، ومن ناحية حماية من أخطارها، أو باختصار أكثر دقة هي (التعامل الذكي مع التكنولوجيا)

وبات من الضروري أن يمزج المواطن بين العالم الواقعي والعالم الرقمي، ويصبح جزءًا منه، رغم أنه يفرض عليه من الخارج. لذلك صارت المواطنة الرقمية بالوقت الحاضر أن يطور الإنسان من نفسه ومن قدراته ليواكب مع هذا العالم الجديد.

أن تأثير العالم الرقمي على موضوع المواطنة يتمثل في أمرين وهما :[24]

1. يتمثل في الغزو الثقافي متعدياً على كل القيم والعادات والتقاليد والدين.
2. تكوين ثقافة جديدة والذي يؤدي إلى تشكيل مواطنة تتلاءم مع ما هو سائد من التناقضات وهجر العادات والتقاليد والعوامل التي ساهمت في تكوين المواطنة السابقة.

ولكن لا ينبغي أن نفهم من معنى المواطنة الرقمية أنها تهدف إلى وضع الحدود والعراقيل من أجل السيطرة والتحكم والمراقبة، بمعنى السيطرة من أجل التحكم، الشيء الذي من الممكن الوصول الى القمع والاستبداد ضد المستخدمين بما يتنافى مع قيم الحرية والعدالة الاجتماعية وحقوق الإنسان. فالمواطنة الرقمية

تهدف إلى العثور على الطريق الصحيح من أجل توجيه وحماية جميع المستخدمين بالأخص الأطفال والمراهقين، وذلك عن طريق تشجيع السلوكيات المرغوبة ومحاربة السلوكيات المنبوذة في التعاملات الرقمية، من أجل مواطن رقمي يحب وطنه ويجتهد من أجل تقدمه.

من هنا أصبح العالم الرقمي سلاحاً ذا حدين على المواطنة، فأما أن يتم توظيفها بشكل إيجابي لخلق الوعي، ومشاركة المعلومات، والتعبير عن الرأي بحرية، وأما أن تصبح ساحة لتداول الأمور التافهة، والشائعات دون التأكد من صحة ما يتم نشره وتداوله أو نشر المضامين التجارية التي يتكسب منها البعض والتسويق لمنتجاتها.

الخاتمة

أن العالم الرقمي بات يشكل تهديد على موضوع الوعي والتنشئة الرقمية، لذلك على صناع القرار عمل وقفه لأجل تحديث البيئة الرقمية بالأخص الوزارات التي لها ارتباط كبير في هذا الموضوع والتي نشمل منها وزارة التربية، ووزارة التعليم العالي والبحث العلمي، ووزارة العلوم والتكنولوجيا والاتصالات وهيئة الإعلام، وكشف جاهزيتهم في هذا الموضوع، وخططهم واستراتيجياتها التطورية لمواجهة التحديات الرقمية. ولأن الآليات سابقة الذكر التي بينها تواجهها تحديات عند تطبيقها في البيئة العراقية على جميع المستويات ويرجع ذلك أن العراق بعد العام 2003 عانى من تركة صعبة متمثلة في (جيل نشأ وترعرع ضمن سلسلة من الحروب والارهاب) أصبح من السهولة السيطرة على الجيل بالأخص الأطفال وحبهم للألعاب الإلكترونية وصارت تلك الالعاب تسيطر عليهم بصورة كبيرة و أن هذه الالعاب فيها من العنف التي تكون قريبة لما عاشه الجيل منذ العام 2003 الى الوقت الحالي، والتي تجعلهم مندمجين في العالم الافتراضي بعيدين عن الواقع، وهذا يؤدي الى دخولهم في عزلة اجتماعية وعدم الاندماج مع المجتمع بالإضافة أن العالم الرقمي يقلل من جعل الافراد اجتماعيون، وان الية التشريعات القانونية وفي ظل التطور الهائل نرى في كثير من الاحيان ضعف في التشريعات القانونية كثيراً ما يستخدم العالم الرقمي لترويج الافكار العنصرية والتنمر والكراهية وصعوبة ملاحقة الجناة، بالإضافة يتم استخدام هذه الشبكة للترويج عن تجارات محرمة كالدعارة وغسيل الاموال والجرائم المتعلقة بالجريمة المنظمة. وحتى موضوع الية الإعلام الرقمي صار من الصعوبة السيطرة على موضوع الإعلام ظهر الكثير من الوسائل الإعلامية الرقمية المسيسة والتي تخدم مصالحها الوصولية والشخصية بعيداً عن المصلحة العامة. وتوصل البحث الى مجموعة من **التوصيات** يمكن ايجازها بما يلي

1- أن التنشئة الرقمية موضوع حديث وأن الظروف التي تكون فيها ساهم في تشكيلهُ وبناءهُ.

2- تطوير فلسفة صناع القرار، من أجل التركيز على حماية المواطن عن طريق اقامة الدورات التثقيفية لأجل محو الامية الرقمية، وزيادة الوعي في استخدام البرامج الرقمية.

وبناء الكثير من المؤسسات التي تعمل في جانب الوعي الرقمي التي تشغل اوقات الفراغ وتوجههم نحو أعمال جيدة.

3- الاهتمام بموضوع الاعلام الرقمي وجعله يعكس صورة لما يرغب فيه مواطنو الدولة، وبناء رسالة اعلامية، تؤكد على المواطنة الصالحة، ويكون الإعلام نابع من الاحتياجات الخاصة بالمواطنين.

4- الجانب العلمي المتعلق بالجانب الرقمي يتميز بفقره في الجانب البحثي والدراسات المتعلقة بموضوع الوعي والتنشئة الرقمية .

5- في الجانب التشريعي القانوني من الضروري على صناع القرار الاهتمام بالجانب التشريعي والقانوني الذي يحمي جميع الاطراف .

6- تعزيز من دور الأسرة، لأن ما يمثله الواقع هناك ضعف وتقليص الدور الذي تقوم به الأسرة في الوعي والتنشئة، لذلك ضرورة عمل دورات وإعلانات من أجل توجيه الأسرة في تنشئة أطفالها رقمياً وتوجيههم نحو ايجابيات هذا العالم وسلبياته.

المصادر والمراجع

[1] وارم العيد وكروم محمد، تحديات التنشئة الاجتماعية في ضوء العالم الرقمي، مجلة العلوم الاجتماعية، الجزائر ، العدد 2، ايلول 2022، ص19.

[2] Harris, P. What are binary and Hexadecimal Numbers? PowerKids Press,2018,pp,3-5

[*] **الثقافة المعلوماتية** تم تعريفها من الجمعية الدولية لتكنولوجيا التعليم (ISTE) بأنها (منظومة متفاعلة من الاستراتيجيات والمعارف والمهارات والقواعد والضوابط والافكار والمبادئ المتبعة في الاستخدام الامثل للتقنيات الرقمية واستثمارها بطرق ذكية وامنة من خلال التحكم في الوصول الى المحتوى الرقمي) للمزيد انظر : سنوسي حياة، الثقافة الرقمية : قراءة تحليلية في المفهوم وعوامل اكتسابها، مجلة الحكمة للدراسات الفلسفية، المجلد 10، العدد 2، 2022، ص 311.

[3] السيد يسين، ثورة المعلوماتية في التقرير الاستراتيجي العربي، القاهرة، مركز الدراسات السياسية والاستراتيجية، 2000، ص ص 38-40

[4] فيولا مخزوم، الوعي المعلوماتي في زمن "ثورة المعلومات، مقال منشور بتاريخ 10 أيلول 2021، على الموقع : https://2u.pw/VxokJcyA تم الاطلاع بتاريخ 15\4\2024 .

[5] باسم بن نايف محمد الشريف، مدى الوعي بالتقنيات التعلمية الرقمية والذكية لأعضاء هيئة التدريس بالجامعات السعودية، مجلة كلية التربية، جامعة الازهر، العدد 179، 2018، ص 605.

[6] فكري مفتاح ابو رخيص، الوعي المعلوماتي في المجتمع الاكاديمي بجامعة الجبل الغربي في ليبيا، اطروحة دكتوراه، جامعة طنطا ، كلية الآداب، ص 33.

[7] موضة بنت ابراهيم الدبيان، تنمية اتجاهات الوعى المعلوماتي الرقمي لدى أعضاء هيئة التدريس بجامعة الامام محمد بن سعود الإسلامية وتأثيرها على تطوير البحث العلمي، مجلة دراسات المعلومات العدد 10 ،2011، ص ص101 – 16

[8] ديانا جرابر، تنشئة الإنسان في العالم الرقمي،ت: مروة عبد الفتاح شحاتة، دار نهضة مصر، 2021، ص 98.

[9] علي عبد الفتاح كنعان، الاعلام والتنشئة الاجتماعية، عمان، دار الايام للنشر والتوزيع، 2015، ص 16.

* **التمكين:** جاء من الحروف (م-ك-ن) مشتق من الفعل مكن، أي امتلك القوة والسلطان، للمزيد انظر: المعجم الوجيز، علم الكتب، 2003، 285.

ويعرفه قاموس اكسفورد بزيادة قدرة الفرد في التحكم بحياته، او في الحالة التي يتمتع بها. للمزيد انظر: Oxford Dictionary Online, Entry 'Empower'2020 http://www.oxforddictionaries.com/definition/english/empower

[10] Tekin, A., & Polat, E. Investigation of digital empowerment levels and online information searching strategies of teacher candidates. Trakya Üniversitesi Eğitim Fakültesi Dergisi7(2)pp635-658.

[11] Akkoyunlu, B., Soylu, M. Y., & Caglar, M. (2010). A study on developing "digital empowerment scale" for university students. Hacettepe University Journal of Education, (39),pp .19-10

[12] سارة غران كليمان، التعلم الرقمي، التربية والمهارات في العصر الرقمي، rand.org/pubs/conf_proceedings/CF369
اطلع عليه بتاريخ 17\4\2024

[13] عصام توفيق واخرون، المشكلات الاجتماعية المعاصرة، مداخل نظرية، تجارب عربية، اساليب المواجهة، ط4، دار الفكرة، عمان- الاردن، ص 163.

[14] وضاح محمود الحمود، نشأت مفضي المجالي، جرائم الإنترنت، التعرض للأخلاق والآداب العامة والحض على الفجور وجرائم الاستغلال الجنسي للأطفال، دار المنار للنشر والتوزيع، عمان – الأردن، ص ص30 – 32.

[15] فاطمة عبدالله الدربي، القيم الاخلاقية الرقمية، مقال منشور في جريدة البيان بتاريخ 1\2\2023 على الموقع:https://www.albayan.ae/opinions/by-the-way/2023-02-01-1.4607975 تم الاطلاع بتاريخ 20\4\2024

[16] عبدالكريم محسن ابو دلو، مستقبل الأخلاق الرقمية، مقال منشور في صحيفة الدستور الاردنية، العدد 19750، الثلاثاء 2 آب / 2022

[17] هند عليوي، اخلاقيات الانترنيت، دراسة تحليلية ميدانية من خلال منضور الاساتذة في جامعة منتوري بقسنطينة، على الموقع :
journal.cybrarians.info تم الاطلاع بتاريخ 20\4\2024

* الجرائم الرقمية: هي جميع الجرائم المتعلقة بتخريب وسرقة الانظمة والبرامج الخاصة بالمنظومات الرقمية، وجرائم الابتزاز الالكتروني والتنمر والاختلاسات المالية التي تتم عن طريق التحويلات بأرقام وحسابات وهمية .

[18] إيمان أحمد علي. الحماية التشريعية للحق في الخصوصية في العصر الرقمي؛ مجلة كلية الشريعة والقانون بطنطا، 2022، العدد 36، ص 74

[19] جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات: رؤية جديدة للجريمة الحديثة، عمان، دار البداية، 2007، ص 86

[20] سعيد بن علي بن حسن المعمري ، و رضوان أحمد الحاف : مبدأ الامن القانوني ومقومات الجودة التشريعية - مجلة البحوث القانونية والاقتصادية، كلية الحقوق ،جامعة المنصورة ، العدد 79 مارس 2022.

* **الاعلام الرقمي :** هو الاعلام الذي يتم فيه استخدام الوسائل الاتصالية الالكترونية المتاحة على شبكات الانترنيت بهدف الوصول الى اكبر عدد من الجمهور والتأثير عليهم . للمزيد انظر: وفاء حافظ عبدالسلام، الانعكاسات الاجتماعية للأنترنيت كأحد اشكال التكنولوجيا الرقمية، دراسة وصفية مطبقة على عينه من طلاب جامعة القاهرة، المؤتمر الدولي الخامس والعشرين لكلية الخدمة الاجتماعية بجامعة حلوان، مصر، ج9، 2012، ص 360.

[21] محمد عبد الحميد احمد، نظريات الاعلام واتجاهات التأثير، القاهرة، عالم الكتب، ط3، 2004،ص 237.

[22] خير ميلاد ابو بكر، التدفق الاعلامي من جانب واحد: ملامح الصورة والمخاطر السياسية والامنية على الوطن العربي، مجلة البحوث الاعلامية، طرابلس، مركز البحوث والتوثيق الاعلامي والثقافي والتعبوي، العدد 17، 1999، ص 35.

[23] شريف درويش اللبان، تكنولوجيا الاتصال، المخاطر والتحديات والتأثيرات الاجتماعية، الدار المصرية اللبنانية، القاهرة، ص.130

* **المواطنة الرقمية:** هي عمليات تفاعل الأفراد مع غيرهم باستخدام ادوات والمصادر الرقمية مثل الحاسوب بصوره المختلفة،
وشبكات المعلومات، كوسيلة للاتصال مع التخرين، باستخدام العديد من الوسائل أو البرامج مثل: البريد الإلكتروني، المدونات، ومختلف مواقع شبكات التواصل الاجتماعي. للمزيد انظر: شرف صبحي الدمرداش، معايير التربية على المواطنة الرقمية وتطبيقاتها في المناهج الدراسية، المؤتمر الدولي السادس لضمان جودة التعليم، أنماط التعليم ومعايير الرقابة على الجودة المنعقد في قطر، مسقط،2014 ص 129-147

[24] ليلى البهنساوي، الأسرة في عصر الرقمنة.. الفرص والتحديات، مقال منشور بتاريخ 2023/11/29 على الموقع :https://www.arabicmagazine.net/Arabic/articleDetails.aspx?Id=9534 تم الاطلاع بتاريخ 23\4\2024

ملف العدد
الأمن السيبراني
درع التحول الرقمي العراقي
(بين التحديات الراهنة وضرورات المستقبل)

الأمن السيبراني العراقي
مسار التطور بين المتطلبات والتحديات

أ.د. مثنى فائق مرعي
جامعة تكريت/ كلية العلوم السياسية

يعد الاهتمام بالأمن السيبراني في العراق من المسائل التي بدأت الحكومة العراقية الاهتمام بها في ظل التطورات الحاصلة في مجال الاتصالات والثورة التكنولوجية الهائلة فيه والتحول نحو الرقمنة في مختلف المجالات . وفي العراق ضمن مجال السيبرانية الامن السيبراني فقد جرى العمل على تحقيق عدة خطوات منها تبني استراتيجية للأمن السيبراني العراقي ، وانشاء فريق للاستجابة السريعة لموجهة التهديدات الإلكترونية والسيبرانية ، وكذلك وضع وثيقة سياسات ومعايير أمن المعلومات والبيانات ، وانشاء وحدات في عدد من الوزارات تختص بمشكلات ومتطلبات الامن السيبراني، وفي الوقت الذي تدرج فيه واقع الامن السيبراني العراقي من اعتماد الوثائق والسياسات الى ان شاء الوحدات والهياكل المختصة بالأمن السيبراني واهتمام المؤسسات والوزارات المعنية ، الا ان قيام نظام سيبراني يحافظ على البيانات والمعلومات من التهديدات والمخاطر يحتاج الى بذل المزيد الجود والاموال واتخاذ السياسات وامتلاك الخبرة المحلية وتعزيز التعاون الخارجي وبالشكل الذي يوفر هذه المتطلبات وبشكل مناسب.

الكلمات المفتاحية: الأمن السيبراني، العراق، التهديدات السيبرانية.

Cybersecurity in Iraq: The path of development between requirements and challenges

Prof. Dr. Muthanna Faeq Merei
Tikrit University / College of Political Sciences

Interest in cybersecurity in Iraq is one of the issues that the Iraqi government has begun to pay attention to in light of the developments taking place in the field of communications, the massive technological revolution in it, and the shift towards digitization in various fields. In Iraq, within the field of cybersecurity, several steps have been worked on, including the adoption of a strategy for Iraqi cybersecurity, the establishment of a rapid response team to address electronic and cyber threats, as well as the development of a policy document and standards for information and data security, and the establishment of units in a number of ministries concerned with

الاستلام	الارجاع	القبول
2024/03/01	2024/04/09	2024/5/25

cybersecurity problems and requirements. At a time when the reality of Iraqi cybersecurity has progressed from the adoption of documents and policies to the establishment of units and structures specialized in cybersecurity and the attention of the institutions and ministries concerned, the establishment of a cybersystem that preserves data and information from threats and risks requires more effort, money, taking policies, possessing local expertise, and enhancing External cooperation in a manner that provides these requirements in an appropriate manner.

Keywords: cybersecurity, Iraq, cyber threats.

المُقدمة

يعود انفتاح العراق في مجال اصاله وتواصله بشكل فاعل وكبير بشبكة الانترنيت الى مرحلة ما بعد عام 2003 وانهاء العزلة الاقليمية والدولية التي كان يعيشها العراق جرّاء العقوبات الدولية المفروض عليه منذ عام 1990 ، ونتيجة للازمات الأمنية والسياسية والاقتصادية المعقدة والمزمنة التي مرت بها الساحة العراقية في ظل الاحتلال الامريكي للعراق لم يكن التوجه نحو الاهتمام بالأمن السيبراني وتعزيزه والعمل به في ظل انشغال البلاد في مواجهة التحديات الأمنية والحرب على الارهاب .

واذا كان الامن السيبراني بمفهومه العام يعني جميع الاجراءات والوسائل التدابير والادوات المستخدمة من اجل توفير الحماية لشبكات الانترنيت والبرامج والبيانات من الهجوم او التلف او حصول اي ضرر او الوصول غير المصرح به اليها ، والحفاظ على سلامتها بمختلف السبل . فإن الامن السيبراني العراقي لا يختلف في مضمونه عنه من حيث كونه يمثل مجموعة الاجراءات والتدابير اللازمة للحفاظ على المعلومات والبيانات الخاصة ومواقع الانترنيت والمواقع الالكترونية الخاصة بالمؤسسات والافراد العراقيين، ومواقع على وسائل التواصل الاجتماعي ايضاً ، ووضع وتبني السياسات واصدار التشريعات الخاصة بكل ما من شأنه ايجاد نظام امن سيبراني يتناسب مع احتياجات العراق ، ويحميه من التعرض الى التهديدات السيبرانية والاختراقات التي قد تتعرض لها المؤسسات المختلفة .

اهمية البحث :

تكمن اهمية البحث في كونه يحاول دراسة موضوع في غاية الاهمية بالنسبة للعراق يتمثل بـــ "الامن السيبراني" الذي حاز على الاهتمام به في السنوات الاخيرة مواكباً للتطورات التكنولوجية في مجال الاتصالات والتحول نحو الحوكمة والرقمنة في مختلف المؤسسات ، وما

يتطلبه الامر من متابعة تطور مسار الامن السيبراني في العراق وما يحتاجه من متطلبات وما يتعرض له من تحديات وتهديدات ووضع المعالجات لها .

اشكالية البحث :

تتمثل اشكالية البحث في محاولة تفسير واقع الامن السيبراني في العراق وكيف تم الاهتمام به والخطوات التي اتخذت في شأن ترسيخه وتعزيزه في ظل ظروف معقدة مرت بها البلاد . ومن هنا يتبادر الى الذهن العديد من التساؤلات حول الموضوع لعل اهمها :

- ماذا يعني الامن السيبراني؟
- كيف تطور الامن السيبراني في العراق وما هي الخطوات التي اتخذتها الحكومة العراقية في مجال الاهتمام به؟
- ما هي متطلبات وجود نظام للأمن السيبراني في العراق؟
- ما التحديات التي تواجه الامن السيبراني العراقي؟

فرضية البحث :

يقوم البحث على فرضية مفادها ان الامن السيبراني في العراق هو موضوع في غاية الأهمية ويحتاج الى ان يوضع في مقدمة سلم اولويات الحكومة العراقية ، في الوقت الذي جاء الاهتمام به مؤخراً ولا يزال يحتاج للعديد من المتطلبات ومعالجة ما يتعرض له من تحديات عديدة .

مناهج البحث :

من اجل التحقق من فرضية البحث ودراسته بشكل علمي ومنهجي ، فقد تم الاعتماد على كل من المنهج الوصفي والمنهج التحليلي في تتبع مضامين الموضوع وتحليله .

هيكلية البحث :

تتضمن هيكلية البحث تقسيمه على : مقدمة وتمهيد ومبحثين وخاتمة ، وجاءت بالشكل التالي : سيأتي التمهيد بعنوان : "مفهوم الامن السيبراني" ، وسيكون المبحث الاول بعنوان " واقع وتطور الامن السيبراني العراقي" ، اما المبحث الثاني فسيأتي بعنوان "متطلبات الامن السيبراني في العراق وتحدياته" ، وبعدها ستأتي الخاتمة متضمنةً لأهم المقترحات التي تخص تطوير قطاع الامن السيبراني في العراق .

التمهيد: مفهوم الامن السيبراني

يُعد مصطلح الامن السيبراني من المصطلحات الحديثة التي تعددت تعريفاتها التي اختلفت بين هذه الجهة او تلك وفقاً لمنظور كل منها ازاء هذا المصطلح ، وذلك لكون هذا المصطلح حديث من حيث نشأته التي تعود الى ما بعد وكت وجود شبكة الانترنت في العقود الاخيرة السابقة .

ومن ضمن العديد من تعريفات الامن السيبراني هنالك من يُعرفه بأنه : " جميع الاجراءات والتدابير والتقنيات والادوات المستخدمة لحماية سلامة الشبكات والبرامج والبيانات من الهجوم او التلف او الوصول غير المصرح به ويشمل كل ذلك حماية الاجهزة والبيانات"[1] .

ويُعرف الامن السيبراني بأنه : "القدرة على الحماية او الدفاع عند استخدام الفضاء السيبراني من الهجمات السيبرانية ، ومعنى ذلك بشكل مبسط ان الأمن السيبراني يهتم بالتهديدات التي تقوم بها الجهات سواء داخلية أم خارجية، أو اقتصاره على نقاط ضعف الجهاز الذي يستخدمه الفرد وبالتالي، حماية الأجهزة والشبكات والخوادم والتطبيقات المتصلة بالإنترنت او الموجودة عليها والتي تتعرض للقرصنة أو الهجمات المستهدفة أو الوصول الغير قانوني"[2] .

ويُعرف الامن السيبراني ايضاً بأنه : "هو حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحتويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع. ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحو ذلك"[3] .

وفي مجال انواع الامن السيبراني ، فهنالك تقسيم مبسط له يذهب الى ان هذه الانواع تتجلى بما يلي:

- امن الشبكة ، ويركز اهتمامه على توفير الحماية لشبكة الكمبيوتر من التهديدات الالكترونية التي يكمن خلفها المهاجمين المُستهدفين أو من قبل البرامج الانتهازية الخطيرة .
- امن التطبيقات ، ويتمثل اهتمامه بإبعاد البرمجيات، والأجهزة والتطبيقات عن أي تهديدات يمكن ان حصل او تتعرض لها راهنا او مستقبلاً .
- امن المعلومات ويتركز هذا النوع من الامن على تأمين الحماية لسلامة البيانات وخصوصيتها، وذلك من خلال عملية تخزين البيانات، او حتى اثناء عملية تناقلها.

- الأمن التشغيلي ، ويتضمن مجموعة العمليات والقرارات ذات الصلة بمعالجة أصول البيانات وحمايتها ، كما تتضمن الأذونات التي يحتاج لها المستخدمين للوصول إلى الشبكة ، وكذلك الاجراءات المتلقة بكيفية ومكان تخزين البيانات او مشاركتها[4] .
- الامن السحابي ، ويتضمن امن السحابة وحماية انظمة التخزين السحابية الاساسية في مختلف الاوقات بسبب الكميات الهائلة من البيانات المخزنة عليها ، ويمكن ان يتضمن خدمات الاعمال المخزنة في مركز البيانات .
- امن البنية التحتية ، ويتمثل بكونه إجراء امني يعمل على حماية البنية التحتية الحيوية للدولة ، مثل اتصالات الشبكة او مركز البيانات او الخادم وغيرها من مفاصل تكنولوجيا المعلومات ، ويهدف هذا النوع من الامن الى الحد من نقاط ضعف الانظمة السيبرانية وحمايتها من والتخريب او الارهاب[5] .

اما فيما يخص فوائد الامن السيبراني فإنها تتلخص بـــــ[6] :

- حماية الشبكات والبيانات من الدخول غير المصرح به .
- تحسين مستوى حماية المعلومات وضمان استمرارية الاعمال .
- تعزيز ثقة المساهمين واصحاب المصلحة في الشركة .
- العمل على استرداد البيانات المسربة في اسرع وقت ممكن اذا ما حصل اي خلل في الفضاء السيبراني.

المبحث الأول: واقع وتطور الامن السيبراني العراقي

تؤشر حالة انفتاح المجتمع العراقي والمؤسسات العراقية العامة والخاصة في مجال الانترنيت الى انها قد بدأت بشكل ظاهر وفعلي بعد العام 2003 ، ولكن جاء الاهتمام بالأمن السيبراني في العراق خلال السنوات الاخيرة السابقة ولاسيما بعد تحقيق نوع الاستقرار السياسي والامني في البلاد ، وكذلك نتيجة لتوجه المؤسسات الحكومية نحو الرقمنة والتعامل الالكتروني والعمل على مواكبة التطورات التقنية في نختلف المجالات والتي يمر بها العالم ، كما لأهمية تحقيق الامن السيبراني في مواجهة تزايد التهديدات الامنية السيبرانية التي مصدرها التنظيمات الارهابية والقراصنة بمستوييها الدولي والفردي والجرائم السيبرانية وغيرها من التحديات في هذا المجال وما تتسبب به من خسائر ومشكلات كبيرة للدولة والمجتمع .

وعند نتطبع تطور الاهتمام بالامن السيبراني في العراق ، يتبين اتخاذ عدة خطوات في هذا المجال ، يمكن توضيح اهمها بشكل مختصر ، وكما يلي :

- **استراتيجية الأمن السيبراني العراقي** ، وثيقة تبنى اصدارها مستشارية الأمن الوطني عام 2017، وتمثل خريطة طريق للمضي في مجال تعزيز الامن السيبراني في العراق ، وتتركز رؤيتها في ايجاد فضاء اليكتروني آمن من اجل حماية المصالح الوطنية للدولة ، وتهدف الى الحفاظ على حقوق وقيم المجتمع العراقي الاساسية[7] . ويمثل الاعلان عن هذه الاستراتيجية بمثابة اول جهد كبير تتبناه الدولة العراقية في مجال الامن السيبراني وتعمل على تحليل مكامن الخلل في السياسة والتشريعات الإلكترونية في العراق ، مثلما السعي لتأسيس بنية تحتية إلكترونية فوقية للبلاد تواكب تطور نظيراتها في الدول الاخرى . يضاف الى ذلك ان هذه الاستراتيجية قد شخصت وجود ثغرات عديدة في السياسات الإلكترونية للعراق ، ووصفتها بأنها نقط ضعف هيكلية ذات صلة بالإهمال البشري، والتدابير غير المدروسة بشكل صحيح ، وعدم الاهتمام المجال السيبراني كأولوية متقدمة . ثم حددت الاستراتيجية جدول أعمال يستند إلى أهداف تنفيذية مدتها عام أو ثلاثة أو خمسة أعوام ، ويتضمن تأسيس وكالة إلكترونية فيدرالية، وصياغة القوانين المتعلقة بالفضاء السيبراني ، وخلق ثقافة الأمن السيبراني ، وشهادات جامعية في هذا المجال ايضاً[8] .

وحددت استراتيجية الأمن السيبراني العراقي التهديدات السيبرانية الاساسية بأنها : "الجريمة الإلكترونية، والإرهاب الإلكتروني، والصراع السيبراني، والتجسس السيبراني، الى جانب إساءة معاملة الاطفال واستغلالهم الكترونياً" . بينما وضعت هذه الاستراتيجية خريطة طريق تضم 8 محاور ، تتمثل بـ: "الحكومة الفعالة، والاطار التشريعي والتنظيمي، واطار تكنولوجيا الأمن السيبراني، وثقافة الامن السيبراني وبناء القدرات، والبحث والتطوير نحو الاعتماد على الذات، والامتثال والتنفيذ، والجاهزية لحوادث الأمن السيبراني، الى جانب التعاون الدولي"[9] .

وقد اكدت الحكومة العراقية في ايلول 2023 من خلال رئيسها السيد محمد شياع السوداني على ان البلاد ماضية في مجال تطبيق استراتيجية الأمن السيبراني التي تم اقرارها في المجلس الوزاري للأمن الوطني عام 2022 ، وان الحكومة العراقية قد شكلت "لجنة عليا

للأمن السيبراني" من أجل تنسيق وتكثيف الجهود بين مختلف الجهات المعنية بالمجال السيبراني في العراق[10] .

- **وثيقة سياسات ومعايير أمن المعلومات والبيانات** ، تم اصدار هذه الوثيقة في ايار 2019 ، من قبل اللجان المختصة في امانة مجلس الوزراء العراقي ، وجاء في نصها انها تهدف الى : "وضع اطر العمل ، ووضع السياسات والمعايير وتحديد الادوار والمسؤوليات ، وبيان الالتزام الادنى المطلوب من جميع العاملين داخل المؤسسة لضمان امن وحماية المعلومات التي يتعاملون معها على اي صورة كانت سواء صورة الكترونية او غير الكترونية، او مكتوبة او مسموعة او مرئية ، او تم تخزينها في ملفات او افلام او صور او وثائق او اقراص او اية وسائط تخزين مادية او الكترونية كانت ، منذ انشائها ، مروراً بنقلها ومعالجتها وتخزينها ، وانتهاءً بإتلافها بشكل امن وصحيح" ، وتتطلب مضامين هذه الوثيقة ان تعمل مختلف المؤسسات العراقية على تطبيق وتنفيذ بنودها وما جاء فيها من تعليمات[11] .
- **فريق الاستجابة للحوادث السيبرانية** ، تأسس هذا الفريق تحت إشراف مستشارية الأمن الوطني العراقي. ويعرف الفريق نفسه بأنه : "فريق وطني مشترك مختص بمجال الأمن السيبراني والاستجابة للحوادث السيبرانية وحماية البنية التحتية للأنترنت ونشر الوعي في مجال حماية الخصوصية والحماية الذاتية للأفراد والمؤسسات على الانترنت ، ويحمل الفريق على عاتقه مسؤولية تأمين وحماية الشبكات ومراكز البيانات الوطنية والمواقع الرسمية التي تعمل في مجال الفضاء السيبراني العراقي ويقوم بتنسيق الجهود الوطنية ودعم المؤسسات في القطاعين العام والخاص في حماية نفسها وخدماتها في الفضاء السيبراني"[12] . ويعمل الفريق من اجل تحقيق الرصانة والموثوقية للأنظمة الالكترونية، وتعزيز ثقة المواطن بالمؤسسات والارتقاء بمستوى العراق دولياً في مجال الامن السيبراني لتشجيع تطوير الخدمات الالكترونية ودعم مشروع أتمتة الخدمات والحكومة الالكترونية. مثلما يهدف الى الاستجابة للحوادث الأمنية والحد من آثارها وتوفير تدابير استباقية لتلافي هذه الحوادث، وبناء الأطر الوطنية للأمن السيبراني لتشجيع التعاون بين القطاعين العام والخاص ، وتعزيز عملية تبادل المعلومات ، وزيادة الثقة في استخدام الخدمات

الإلكترونية الحكومية، وتعزيز الوعي الأمني لمستخدمي انظمة تكنولوجيا المعلومات والإنترنت ، وتحليل التهديدات الأمنية وتأثيرها، وتوفير معلومات عن آخر الحوادث وطرق تجنبها ، وبناء مركز معتمد لتسلم البلاغات عن الحوادث السيبرانية، وتشجيع البحث والتطوير في مجال الأمن السيبراني، والتعاون المشترك مع فرق الاستجابة والمنظمات على الصعيدين الإقليمي والدولي[13] . ويقع على عاتق هذا الفريق تطبيق ما جاء في وثيقة سياسات ومعايير أمن المعلومات والبيانات .

- **المؤسسات التعليمية السيبرانية** ، اعلنت وزارة التعليم العالي والبحث العلمي العراقية عن استحداث 3 أقسام متخصصة في دراسة الأمن السيبراني في الجامعات العراقية ، وهي كل من: جامعة المستنصرية، الجامعة التقنية الشمالية، وجامعة الموصل" . كما افتتحت شبكة العراق الرقمي فروع لـ"أكاديميات عالمية" لتدريس الأمن السيبراني والحوسبة السحابية في البلاد. كما تم افتتاح أكاديمية لشركة أمازون AWS المتخصصة بالحوسبة السحابية في أربع جامعات، ثم افتتاح أكاديمية أخرى لشركة EC Council المتخصصة في الأمن السيبراني في الجامعة التكنولوجية في بغداد والجامعة التقنية الشمالية. وفي نفس الاطار تم تدريب 100 أستاذ جامعي من مختلف جامعات العراق على الحوسبة السحابية والأمن السيبراني بدعم شركات التكنولوجيا العالمية ومن خلال البرنامج الوطني لتدريب الجامعات في مجال الحوسبة السحابية وبرنامج الأمن السيبراني العراقي المدعوم من الجامعة التكنولوجية"[14] . يضاف الى كل ذلك ان العديد من مؤسسات التعليم العالي والبحث العلمي ولاسيما الجامعات العراقية قد اخذت على عاتقها عقد العديد من الندوات والمؤتمرات والقاء المحاضرات واقرار البحوث والرسائل والاطاريح الجامعية التي تخص موضوع الامن السيبراني ومجالاته المختلفة في العراق.
- **لجنة خاصة بالأمن السيبراني للانتخابات**، شكلت اللجنة العليا لتأمين الانتخابات الخصة بمجالس المحافظات في العراق "لجنة خاصة بالأمن السيبراني"، تتكون من 7 ممثلين من ذوي الاختصاص بالمعدات الفنية ، وتهدف هذه اللجنة الى تأمين إجراء انتخابات المحافظات في دورتها لعام 2023 . وان مهمة اللجنة تتمثل بفحص الأجهزة الخاصة بالعملية الانتخابية . والعمل على استكمال كل الاستعدادات اللازمة لإجراء للانتخابات

وضمان سلامتها ونزاهتها، انطلاقاً من رؤية ان الأمن السيبراني جزءاً مهما من العملية الانتخابية . ويأتي تشكيل اللجنة للأمن السيبراني كجزء من الجهود الرامية لحماية عملية الانتخابات من أي محاولات للتدخل أو التلاعب السيبراني[15].

- **جهود وزارة الداخلية ،** عملت وزارة الداخلية العراقية في مجال إرساء قواعد الأمن السيبراني في البلاد، وبخاصة جهودها فيما يتعلق بمحوري الجريمة الإلكترونية، والإرهاب الإلكتروني، ويدرج ضمن جهود وزارة الداخلية العراقية تدريب العديد من العناصر في مديريات الوزارة المختلفة على المهارات الرقمية المتقدمة لمواجهة تلك الجرائم، مثلما ووفرت متطلبات الإبلاغ السريع عن تلك الجرائم، ناهيك عن القيام بحملات توعية الشرائح العراقية المختلفة بمخاطر الامن السيبراني ، وكذلك توفير ووسائل تجنبها من قبل الأفراد العاديين، وذلك عن طريق اقامة حملات اعلامية والكترونية وندوات الحوارية وثقيفية ، وغيرها[16] .

يضاف الى كل ذلك ان جميع وزارات وتشكيلات ومؤسسات الدولة العراقية قد هيأت فرقاً إلكترونية مختصة ذات طبيعة حساسة في مجال مواجهة الجرائم السيبرانية ، ومنها استهداف المواقع الإلكترونية واختراقها ، والمواقع الإلكترونية التي يجري توظيفها في جرائم أمنية وعسكرية وإرهابية وجنائية متعددة، وكل ذلك في ظل التشريعات العراقية النافذة، التي ما زالت لا ترتقي إلى مستوى التحولات الرقمية في العراق، والمخاطر الراهنة التي تواجهها، ومنها ما يرتبط بالأمن السيبراني[17] .

ويتبين من خلال ما سبق ، ان مسيرة العراق في مجال الاهتمام بالأمن السيبراني هي وليدة الضغوطات والمتغيرات والتحديات التي مرت بها الساحة العراقية في السنوات الاخيرة المنصرمة ، فكان الاتجاه الحكومي الى تبني سياسات وجهود تعمل على حماية الفضاء السيبراني وتحقيق امنه بشكل يتناسب مع المصالح الوطنية العراقية ، ولاسيما تلك التي على صلة بالمجال الالكتروني والسيبراني .

المبحث الثاني: متطلبات الامن السيبراني في العراق وتحدياته

لقد اصبح الأمن السيبراني يشكل جزء أساسي من أي سياسة أمنية للدول ، بحيث صار معلوماً وواضحاً ان مؤسسات صنع القرار الامريكية ، والأوروبية ، الروسية ، والصينة ، الهند وغيرها من مؤسسات صنع القرار لدى الدول الاخرى ، تقوم بتصنيف مسائل الدفاع عن الأمن السيبراني كأولوية في سياساتهم الدفاعية الوطنية . وان هنالك ما يقرب من 130 دولة حول العالم عن تخصيص اقسام وتضع سيناريوهات خاصة بالحرب السيبرانية ضمن فرق الأمن الوطني . تضاف جميع هذه الجهود إلى الجهود الأمنية التقليدية لمحاربة الجرائم الالكترونية، الاحتيال الالكتروني والأوجه الأخرى للمخاطر السيبرانية[18] . وتأتي هذه الاولية والاهمية للأمن السيبراني لدى عدد من الدول من عدة جوانب ، اهمها[19] :

- يشمل الامن السيبراني جميع الأمور المتعلقة بحماية البيانات من مهاجمي المعلومات وسراقها، وبخاصة اذا كانت البيانات حساسة ومهمة ، أو معلومات حكومية وصناعية، أو شخصية، أو بيانات أو حقوق ملكية فكرية.
- يُعد وجود برامج وآليات الدفاع والأمن السيبراني وسيلة متطورة ومهمة في مجال حماية البيانات وخدمة مصلحة الجميع، في مختلف المؤسسات .
- يساهم الامن السيبراني في تقليل مخاطر الهجمات الإلكترونية على الصعيد الفردي، كونه يحميهم من مخاطر هذه الهجمات التي قد تعرض الأفراد لسرقة بياناتهم وابتزازهم، وبالتالي إحداث أضرار وخيمة في حياة الأفراد.

ومن هنا تأتي اهمية توفير متطلبات تأسيس امن سيبراني متكامل الجوانب في العراق من اجل مواجهة التحديات والتهديدات التي يتعرض لها الفرد او المجتمع او المؤسسات العراقية في المجال السيبراني :

اولاً- متطلبات الامن السيبراني في العراق :

يتطلب امتلاك اي دولة لأمن سيبراني يوائم مع ما لديها من مجال سيبراني ومعلومات وبيانات تحتاج الى حمايتها والحفاظ عليها، ان توفر كل ما يحتاجه هذا النوع من الامن من متطلبات مادية وبشرية وغيرها .

وفيما يخص متطلبات الامن السيبراني في العراق فإن استراتيجية الامن السيبراني العراقي تحددها بما يلي[20] :

- **الحكومة الفعالة :** وتعمل على التنسيق لتكوين مبادرة الامن السيبراني الوطني ، وتعزيز التعاون الفعال بين القطاع العام والقطاع الخاص ، وانشاء التبادل والمشاركة الرسمية للمعلومات والتشجيع على المشاركة غير الرسمية للمعلومات (للسرعة في تناقل المعلومات) ، وتفعيل الحكومة الالكترونية بشكل يضمن راحة المواطن .
- **الإطار التشريعي والتنظيمي** : ويتضمن مراجعة وتحسين القوانين السيبرانية العراقية الحالية – ان وجدت- من اجل معالجة الطبيعة الديناميكية للتهديدات التي تواجه الامن السيبراني العراقي ، طرح وانشاء قوانين سيبرانية جديدة لغرض تعزيز الوضع القانوني السيبراني العراقي ، انشاء برامج بناء القدرات التدريجي للجهات القانونية التنفيذية الوطنية ، التأكد من توافق التشريعات المحلية مع القوانين والمعاهدات والاتفاقيات الدولية .
- **اطار تكنولوجيا الأمن السيبراني** : ويشمل بناء وتطوير إطار تكنلوجي وطني للأمن السيبراني وفقاً لمتطلبات السيطرة على الامن السيبراني العراقي ، العمل على بناء او انشاء برنامج وطني لتقييم / إصدار شهادات للمنتجات ونظم الامن السيبراني.
- **ثقافة الأمن السيبراني وبناء القدرات** : وتتضمن العمل على : بناء وتطوير وتعزيز ثقافة الأمن السيبراني الوطني ، انشاء وتوحيد وتنسيق برامج التوعية والتثقيف في مجال الأمن السيبراني ، إنشاء وتطوير آلية فعالة لنشر المعلومات عن الأمن السيبراني على المستوى الوطني ، وتحديد الحد الأدنى من المتطلبات والمؤهلات للعاملين في مجال أمن المعلومات .
- **البحث والتطوير نحو الاعتماد على الذات** : ويكون ذلك بالعمل على : تنسيق وتحديد أولويات البحث والتطوير في مجال الأمن السيبراني ، توسعة وتعزيز مجتمع الأبحاث في مجال الأمن السيبراني ، تعزيز وتطوير وتسويق الملكية الفكرية والتكنولوجية والابتكارات من خلال البحوث المركزة والمتخصصة، تغذية ودعم السوق المحلي والصناعات في مجال الامن السيبراني ، استحداث اختصاص جامعي يختص بالأمن السيبراني وفق معايير خاصة ، استحداث تخصص يعنى بالجنائيات الرقمية وطرق التحقيق والاثبات في القضايا المتعلقة

بالجرائم المعلوماتية ، واقرار المناهج والتخصصات التي تعنى بالجرائم المعلوماتية في المؤسسات التعليمية والتطويرية المعنية بالأمر .

- **الامتثال والتنفيذ :** ويشمل توحيد أنظمة الأمن السيبراني عبر جميع مفاصل الدولة العراقية ، تقوية وتعزيز الرصد والتنفيذ للمعايير في مجال الامن السيبراني ، وضع إطار معياري لتقييم مخاطر الامن السيبراني .
- **الجاهزية لحوادث الامن السيبراني :** وتتضمن العمل على : تعزيز وتقوية فريق الاستجابة للحوادث السيبرانية العراقي ، وضع آليات فعالة للإبلاغ عن الحوادث السيبرانية ، وحث وتشجيع جميع الجهات والعاملين في مجال الامن السيبراني لمتابعة ورصد الفعاليات المتعلقة بالأمن السيبراني ، وضع معيار إطاري موحد لإدارة استمرارية الأعمال ، نشر تنبيهات انيه حول الثغرات، الضعف والتحذيرات فيما يتعلق بالأمن السيبراني ، وكذلك تشجيع جميع الجهات المتعلقة بالأمن السيبراني على تنفيذ برامج دورية لفحص وتقييم مدى احتمالية التعرض للهجمات السيبرانية في البلاد .
- **التعاون الدولي :** ويحتاج تحقيق هذا المتطلب الى : تشجيع مشاركة العراق الفعالة في جميع هيئات الأمن السيبراني الدولية والوكالات المتعددة الجنسيات ، وتعزيز المشاركة الفعالة في الفعاليات والمؤتمرات والمنتديات الدولية المتعلقة بالأمن السيبراني ، والعمل على تعزيز الموقع الاستراتيجي للعراق في مجال الأمن السيبراني من خلال استضافة مؤتمرات دولية دورية في مجال الامن السيبراني ، تنشيط التواصل مع "منظمة الاتصالات العالمية" والعمل على تحديث الملف المتعلق بالوعي الأمني السيبراني العراقي ، تأسيس شراكة واتفاقيات بين فريق الاستجابة الالكتروني العراقي وفرق الاستجابة الاليكترونية الدولية الأخرى لأجل تطوير الفريق وتوسعة آفاقه .

وبذلك يتوجب على الحكومة العراقية ان تعمل على تعزيز الوعي السيبراني لدى المواطنين والمؤسسات. والعمل على تطوير البنية التحتية التكنولوجية وتحديثها لتأمين النظام السيبراني في البلاد . وكذلك وضع تشريعات وافية لحماية النظام السيبراني ومكافحة الجرائم السيبرانية لكون العراق يفتقر الى الان لقانون الجرائم المعلوماتية. وان يكون للعراق مشاركاته في المؤتمرات والندوات العالمية التي تهتم بواقع الامن السيبراني . اذ ان تحقيق الأمن السيبراني في البلاد

يحتاج الى جهود متكاملة من الحكومة والمؤسسات والمواطنين. وايجاد كل ما يتطلبه الأمن السيبراني ليكون مساهماً في ضمان استقرار الدولة وتطورها في هذا العصر الرقمي المتقدم الذي يشهده العالم[21] . كما ينبغي ان يرتكز الأساس الرقمي في العراق إلى الأمن في مختلف مفاصله بغية تعزيز التنمية الاقتصادية طويلة الأجل. مثلما يجب أن يضمن توفير استراتيجية تحول رقمي قائمة على أساس متين للأمن السيبراني. وهذا يتطلب الاستثمار في تطوير وتنفيذ سياسات ومعايير وأطر تنظيمية فعالة للأمن السيبراني، وكذلك العناية الفائقة بتعزيز قدرات ومهارات وثقافة الأمن السيبراني بين المنظمين، والمشغلين، والموردين، وأصحاب المصلحة الآخرين في القطاعات المتخصصة . يضاف الى ذلك ان تعزيز الدفاع السيبراني في العراق يتطلب توفير نهج شامل يدمج تدابير الأمن السيبراني في جميع جوانب التحول الرقمي. وكل ذلك من دون اهمال التركيز على التعاون بين القطاعين العام والخاص[22] .

ثانيا – تحديات الامن السيبراني العراقي وتهديداته:

لا يعمل اي نظام أمن في بيئة اعتيادية ومناسبة ومن دون ان يتعرض الى تحديات او تهديدات ، وبخاصة نظام الامن السيبراني بشكل عام وفي العراق بشكل شخص ، نظراً لحداثة الاهتمام به ولاحتياجه الى المتطلبات التي يُفترض ان يبنى عليها مقارنة بالأمن السيبراني في الدول الاخرى التي يشكل لديها اولية متقدمة .

ويواجه الامن السيبراني العراقي عدة تحديات ، لعل اهمها :

- نقص الوعي السيبراني سواء لدى المواطنين او المؤسسات الحكومية المختلفة، اذ لايزال الوعي الالكتروني ضعيفاً في العراق، ومن اسباب ذلك هو عدم توفر البرامج التثقيفية والتوعوية اللازمة التي توضح للأفراد والمجتمع اهمية الأمن السيبراني وطرق الحماية من الاختراق او الاستغلال .
- ضعف البنية التحتية التكنولوجية ، اذ لا يزال العراق يعاني من نقص في البنية التحتية التكنولوجية اللازمة لتأمين النظام السيبراني لاسيما في ظل التطور المتسارع الذي يشهده العالم في هذا المجال[23]، كما يعاني من ضعف في البنية التحتية الخاصة بالحماية الإلكترونية من الهجمات السيبرانية ، مما جعل العراق مكشوفاً لدى الكثير من دول العالم التي عملت على اختراقه والتجسس عليه لاسيما استهداف المؤسسات الامنية[24] .

- ضعف القوانين والتشريعات الحكومية الخاصة بالأمن المعلوماتي والسيبراني ، الامر الذي يتطلب اقرار تشريعات وقوانين فعالة يتم تطبيقها من قبل القطاعين الحكومي والخاص .
- ضعف القدرات المهنية المحلية وقلتها في مجال امن المعلومات المتقدمة والامن السيبراني ، الامر الذي يتطلب السعي الهادف من اجل تدريب وتطوير كوادر مهنية محترفة في القطاع الحكومي والخاص تكون مؤهلة وقادرة على مواجهة التحديات السيبرانية .
- ارتباط منظومات الانترنت في العراق بالخارج مما يعني ان الامن السيبراني العراقي مرتبط بدول وشركات اجنبية ، الوضع الذي يفترض من الحكومة العراقية العمل على تأسيس شركات خاصة بها في هذا المجال او التأسيس لشراكة فعالة مع الشركات المحلية لإقامة علاقات موثوق بها وفعالة لسد النقص في هذا المجال[25] .
- عدم مواكبة الشركات المحلية لتكنولوجيا المعلومات للتطورات الحاصة في مجال السيبرانية ، بالترافق مع ضع ادراك حجم التهديدات والمخاطر الامنية التي قد يتعرض لها الامن السيبراني في العراق ، وهذا الامر يحتاج الى مواكبة التطورات التكنولوجية في مجالات الاتصال والانترنيت ، والوعي التام بخطورة التحديات الامنية المعاصرة والبحث عن حلول تتناسب معالجاتها[26] .

اما التهديدات ، فقد تعرض المواقع الالكترونية للعديد من الوزرات والمؤسسات والاشخاص في العراق الى العديد من الهجمات والتهديدات واختراق للبيانات وسرقة المعلومات الحكومية والخاصة في السنوات السابقة .

وقد تعرضت العديد من المواقع الالكترونية المهمة والتابعة للحكومة العراقية للاختراق خلال العام 2019 وما بعده ، ومنها بينها موقع جهاز الأمن الوطني ، واختراق عدد من مواقع الوزارات في مواقع التواصل الاجتماعي ، مثل مواقع وزارتي البلديات ، والشباب والرياضة ، ودائرة توزيع الطاقة[27] ، واختراق موقع وزارة التجارة العراقية في آب 2023 ونشر بيانات المواطنين الخاصة بالبطاقة التموينية على قنوات برنامج التليكرام ، وهو الامر الذي نفته وزارة التجارة في بيان لها يوم 6 آب 2023، على الرغم من ان تلك البيانات كانت بالفعل موجودة في قنوات التليكرام قبل ان تبادر وزراة الاتصالات العراقية بحجب البرنامج في العراق ، وبينت انه الامر نتيجة لمحددات تتعلق بالأمن الوطني / ومن اجل حفاظ على

البيانات الشخصية للمواطنين، التي خرق تطبيق التليكرام سلامة التعامل بها وبشكل مخالف للقانون[28]. ومن الامثلة ايضاً على الاختراقات التي تعرضت لها المواقع الحكومية في العراق هو تعرض صفحة الامانة العامة لمجلس الوزراء العراقي على موقع التواصل الاجتماعي "فيس بوك" الى الاختراق من قبل برمجيات "خبيثة" كانت قد استغلت صلاحيات للنشر على المواقع والبريد الالكتروني الخاصة بالموقع وذلك في شهر آذار 2024[29] .

ومن الجدير بالذكر ان التهديدات السيبرانية والاختراقات التي تتعرض لها المواقع الالكترونية المختلفة في العراق ولاسيما المؤسسات الامنية وذات الصلة ببيانات ومعلومات المواطن والدولة ، تستدعي اهمية سرعة القيام بإجراءات حكومية تعزز الامن السيبراني وحماية الأمن الإلكتروني والبيانات الشخصية للأفراد والمؤسسات على حد سواء في البلاد . ولاسيما ان العراق هو من اكثر الدول عرضة للهجمات الالكترونية ، اذ احتل العراق عام 2017 المرتبة 159 عالمياً ضمن تصنيف البلدان الأكثر استعدادًا للهجمات الإلكترونية وفقاً لتقرير الاتحاد الدولي للاتصالات[30].

وقد أعلنت شركة "تريند مايكرو*" في تموز 2023 عن النتائج التي تضمنها تقريرها السنوي للأمن السيبراني، وكشف عن زيادة ملحوظة بنسبة 55٪ في عمليات اكتشاف التهديدات العالمية ، وزيادة ضخمة على صعيد الملفات الخبيثة المحظورة قد بلغت نسبة 242٪ في عام 2022 . وعلى صعيد العراق فإن التقرير تضمن بأن حلول شركة "تريند مايكرو" قد نجحت باكتشاف وحظر أكثر من 15 مليون تهديد عبر البريد الإلكتروني ، مثلما استطاعت حماية أكثر من 400 ألف مستخدم من التضرر من روابط خبيثة قاموا بالضغط عليها ، وكذلك تمكنت من تحديد وإيقاف أكثر من نصف مليون هجوم لبرمجيات خبيثة على مواقع مختلفة في العراق . الامر الذي يتطلب من الجهات المعنية في العراق العمل على المحافظة على جهود الاعتماد الآمن على التكنولوجيا في العراق، من اجل تأمين المشهد الرقمي في البلاد وحمايته من الهجمات الإلكترونية والحفاظ على المعلومات والبيانات الحساسة[31] .

وهذا هذا الامر يستدعي ان تأخذ الجهات المعنية المختلفة في العراق الامر على محمل الجد وتمنح الاهتمام بالأمن السيبراني اولوية متقدمة في السياسات والبرامج الحكومية من اجل حماية المواقع الإلكترونية وبيانات ومعلومات المؤسسات والافراد في العراق .

الخاتمة :

يتبين من خلال دراسة موضوع الامن السيبراني في العراق ان انفتاح العراق في مجال الاتصالات والمجالات الإلكترونية يمكن وصفه بأنه حديث عهد مقارنة بغيره من الدول ، ولعل هذا الامر كانت نتيجةً للظروف والازمات التي مر بها العراق سياسياً وامنياً واقتصادياً فلم يحظى موضوع السيبرانية بالاهتمام المناسب الا مؤخراً .

وان قطاع الامن السيبراني في العراق يحتاج الى العديد من المتطلبات منها البنى التحتية الخاصة بتكنولوجيا الاتصال والانترنت ، والخبرات المحلية ، والتخصيصات المالية المناسبة ، ووضع التشريعات والقوانين التي تسهل العمل في هذا المجال في البلاد ، بالإضافة الى اهمية وجود مؤسسات خاصة بالأمن السيبراني بشكل مستقل من دون ربطها بمؤسسات قد تكون عائقاً او مقيداً لعملها . وفي المقابل لم يكن المجال السيبراني في العراق بعيداً عن التعرض للعديد من التحديات منها مادية واقتصادية وعلمية وسياسية وقانونية وتقنية وغيرها .

وفيما يخص الامن السيبراني العراقي ومن خلال دراسة موضوعه يمكن التوصل الى عدد من المقترحات التي تساهم في تطوير هذا القطاع المهم والضروري ، اهمها :

- مراجعة وثيقة "استراتيجية الامن السيبراني العراقي" ، ومعالجة ما أُشر عليها من ملاحظات حتى تكون بالشكل المناسب الذي يتلائم مع التطورات الكبيرة في المجال السيبراني .
- توفير التخصيصات المالية اللازمة والكافية لمتطلبات وجود نظام امن سيبراني متكامل في العراق .
- تشكيل مؤسسة او هيئة مستقلة خاصة بالأمن السيبراني العراقي .
- تأسيس وحدات تخص الامن السيبراني وامن المعلومات تلحق بالمؤسسات والوزارات العراقية المختلفة تكون مهمتها العمل على حماية بيانات ومواقع هذه المؤسسات والوزارات ، وان يعمل بها اشخاص ذوي خبرة في المجال السيبراني ويتم تدريبهم وتطويرهم مهاراتهم بشكل مستمر.

- وضع وتطوير التشريعات والقوانين الخاصة بقضايا السيبرانية مثل الجرائم الإلكترونية والابتزاز الالكتروني والاختراق وسرقة المعلومات ، وقوانين الامن السيبراني وأمن المعلومات وغيرها .
- انشاء واستحداث اقسام ومراكز علمية وتعليمية تختص بالأمن السيبراني من اجل رفد مؤسسات الدولة بمن يملكون المؤهلات العلمية في هذا المجال ، وتكون هذه الاقسام والمراكز تابعة لوزارة التعليم العالي والبحث العلمي او حتى من الممكن لباقي الوزارات المعنية بالأمر .
- الاهتمام بمسألة مشاركة العراق في المؤتمرات الدولية والعالمية المختصة بالأمن السيبراني ، وعقد الاتفاقيات مع الاطراف والدول في المجالات السيبرانية بما يعزز مكانة العراق في هذا الاطار داخلياً وخارجياً .

المصادر والمراجع:

[1]- منى عبد الله السمحان ، "متطلبات تحقيق الامن السيبراني لأنظمة المعلومات الإدارية بجامعه الملك سعود"، **مجلة كلية التربية - جامعة المنصورة** ، العدد 111 (المنصورة : يوليو 2020) ، ص 7 .

[2]- المركز الوطني للأمن السيبراني، ما هو الأمن السيبراني؟ ، الرابط : https://www.ncsc.gov.bh/ar/cyberwiser/cyber-security.html

[3]- هيئة الاتصالات والفضاء والتقنية - السعودية ، ما هو الأمن السيبراني؟، الرابط : https://www.cst.gov.sa/ar/Digitalknowledge/Pages/cyber-security.aspx

[4]- عبير الخزاعلة ، مفهوم الأمن السيبراني ، موقع موضوع ، 17 نوفمبر 2021 ، الرابط : https://mawdoo3.com/%D9%85%

[5]- الأمن السيبراني ، موقع هارفارد بزنس ريفيو ، 2020/4/5 ، الرابط : https://hbrarabic.com/%D8%A7%D9%

[6]- المصدر نفسه .

[7]- انظر : وثيقة سياسات ومعايير أمن المعلومات والبيانات ، اللجنة الفرعية لكتابة السياسات والمعايير - لجنة تنسيق وإدارة النشاط الحكومي باتجاه انشاء الحوكمة الالكترونية ، الامانة العامة لمجلس الوزراء العراقي ، بغداد ، 9 أيار 2019، ص 17 .

[8]- هاشم شبر ، تنظيم الجهد المؤسساتي والوزاري المشترك إزاء الأمن السيبراني في العراق ، (بغداد : مركز البيان للدراسات والتخطيط ، 9 أيار 2019)، ص 3 .

[9]- صفد الشمري ، ما واقع الأمن السيبراني في العراق؟، موقع صحيفة الصباح ، 2021/6/8 ، الرابط : https://alsabaah.iq/48007-.html

[10]- صحيفة الشروق، السوداني: العراق ماضٍ في تطبيق استراتيجية الأمن السيبراني ، 2023/9/3 ، الرابط : https://bit.ly/3JT0XXe

[11]- انظر : وثيقة سياسات ومعايير أمن المعلومات والبيانات ، مصدر سبق ذكره .

[12]- فريق الاستجابة للحوادث السيبرانية ، أسس عمل فريق الاستجابة للحوادث السيبرانية ، الرابط : https://cert.gov.iq/cert

[13]- صفد الشمري ، مصدر سبق ذكره .

[14]- قناة RT ، شبكة العراق الرقمي: استحداث 3 أقسام لدراسة الأمن السيبراني لأول مرة في العراق، 2022/9/6 ، الرابط : https://bit.ly/4agSpUO
[15]- هدى جاسم، العراق.. لجنة خاصة بالأمن السيبراني لتأمين الانتخابات ، صحيفة الاتحاد ، 2023/11/9، الرابط : https://bit.ly/4agSpUO
[16]- صفد الشمري ، مصدر سبق ذكره .
[17]- المصدر نفسه .
[18]- الهيئة المنظمة للاتصالات – الجمهورية اللبنانية ، لمحة عامة حول الأمن السيبراني، الرابط : http://www.tra.gov.lb/Cybersecurity-in-few-words-AR
[19]- عبير الخزاعلة ، مصدر سبق ذكره .
[20]- مستشارية الامن الوطني ، استراتيجية الامن السيبراني العراقي ، بغداد ، 2017 ، ص 8-9 .
[21]- مصطفى علي الطائي ، تحديات النظام السيبراني في العراق ، موقع جريدة ، 2023/9/21 ، الرابط : https://jaredaiq.net/News/5780
[22]- عبد العظيم محمد الصالح ، دور الأمن السيبراني في تعزيز الاقتصاد الرقمي في العراق، جريدة العالم ، 2023/12/24 ، الرابط : https://bit.ly/3ymaMKE
[23]- مصطفى علي الطائي ، مصدر سبق ذكره .
[24]- مصطفى ابراهيم سلمان ، "الامن السيبراني وثره في الامن الوطني العراقي" ، **مجلة العلوم القانونية والسياسية** ، المجلد العاشر ، العدد الاول ، (بعقوبة : 2021) ، ص 173 .
[25]- المصدر نفسه ، ص 175 .
[26]- يسرى ستار، "الأمن السيبراني في العراق" ، **تقدير موقف** ، (بغداد : مركز رواق بغداد ، تشرين الثاني 2022).
[27]- هاشم العوادي ، حماية الأمن السيبراني العراقي الاستراتيجية المفقودة ، موقع كتابات ، 2020/1/14 ، الرابط : https://bit.ly/4b6IT8c
[28]- وكالة بغداد اليوم ، تعليق من وزارة التجارة حول "اختراق ونشر بيانات التموينية" في التيليغرام، 2023/8/6 ، الرابط : https://bit.ly/4dxDats
[29]- وكالة بغداد اليوم ، اختراق الصفحة الرسمية للأمانة العامة لمجلس الوزراء ، 2024/3/17 ، الرابط : https://bit.ly/4am6Gjm
[30]- هاشم العوادي ، مصدر سبق ذكره .
* شركة "تريند مايكرو هي الشركة العالمية الرائدة في مجال الأمن السيبراني .
[31]- شفق نيوز ، 20 مليون تهديد في العراق.. تقرير الأمن السيبراني يكشف حصيلة 2022 ، 2023/7/17 ، الرابط : https://bit.ly/3UA6tTt

ملف العدد
الأمن السيبراني
درع التحول الرقمي العراقي
(بين التحديات الراهنة وضرورات المستقبل)

قراءة تحليلية
لاستراتيجية الأمن السيبراني العراقي

أ.د. حازم حمد موسى
جامعة الموصل/ كلية العلوم السياسية
hazim@uomosul.edu.iq

إنَّ القوة السيبرانية إحدى وسائل وأدوات الدول لتحقيق أهدافها والمحافظة على مكتسباتها، ويعد تحقيق الأمن السيبراني من التحديات الأمنية المعاصرة التي تمس قوة الدولة الشاملة وهذا الحال في العراق، الذي يتطلب زيادة الوعي بالمخاطر السيبرانية المتحققة، لأن من يمتلك آليات توظيف القوة السيبرانية يصبح أكثر قدرة على تحقيق أهدافه والتأثير في أداء الفاعلين في هذه البيئة، فكان لثورة المعلومات والاتصالات انعكاساتها في ربط المصالح القومية للدول بالبنى التحتية الحيوية لها، والسعي في إقامة المراكز اللازمة التي يمكن الاستفادة منها في التصدي لما يقع من حوادث لاختراق الأمن العراقي، ويشكل كذلك تقييم الخطر، وتنفيذ تدابير لتخفيف الأثر، وإدارة النتائج جزءاً من أي برنامج وطني للأمن السيبراني وركز البحث على مكنّة بناء رؤية استراتيجية للأمن الوطني العراقي في ظل تأثير الفضاء السيبراني الذي فاقم من حجم المعضلة الأمنية، والتعريف بها وبيان أسباب اعتمادها، وإ ثبات قدرتها على تحجيم المعضلات الأمنية المعلوماتية التي يتعرض لها العراق والتي أثرت عليه جيو-استراتيجياً وجيوبوليتيكياً، بعد الارتكاز على القواعد والمسلمات العلمية- التقنية للتعامل مع معضلات الأمن السيبراني، مع الإشارة إلى حقيقة تمكين القائمين على الأمن السيبراني، لطمر فجوة الانكشاف الاستراتيجي بسبب المعضلات الأمنية، وسيجيب البحث عن التساؤل الأساسي الآتي: هل يمكن للرؤية الاستراتيجية إن تفسر المعضلات الأمنية في ظل الفضاء السيبراني الذي أوجده التغيير الدولي وتحقق طفرة في الأمن السيبراني العراقي؟مع توفير خارطة طريق متماسكة ومبادرات و آليات لتنفيذ و لتحقيق الرؤية الوطنية بشأن الأمن السيبراني في سياق الرخاء الوطني، كونه ويوفر منصات وفرصا ممتازة لتأمين وتنمية اقتصاد الدولة،وتعطي تصور لصانع القرار العراقي بضرورة العمل على أعداد بيئة أمنية سليمة في المستقبل.

الكلمات المفتاحية: الاستراتيجية، الأمن، السايبر، التهديد، المعضلة الأمنية، العراق.

الاستلام	الارجاع	القبول
2024/03/28	2024/04/29	2024/5/28

An Analytical Reading of the Iraqi Cyber Strategy

Prof. Dr. Hazem Hamad Musa
University of Mosul/College of Political Sciences

Cyber power is one of the means and tools for countries to achieve their goals and preserve their gains. Achieving cyber security is one of the contemporary security challenges that affect the comprehensive power of the state. This is the case in Iraq, which requires increasing awareness of the cyber risks that are realized, because whoever possesses the mechanisms for employing cyber power becomes more capable of Achieving its goals and influencing the performance of actors in this environment. The information and communications revolution had its repercussions in linking the national interests of countries with their vital infrastructure, and striving to establish the necessary centers that can be used to confront any incidents that occur that penetrate Iraqi security. It also constitutes risk assessment and implementation. Measures to mitigate the impact and manage the results are part of any national cybersecurity program. The research focused on the mechanism of building a strategic vision for Iraqi national security in light of the influence of cyberspace, which has exacerbated the magnitude of the security dilemma, defining it, explaining the reasons for its adoption, and proving its ability to reduce the information security dilemmas that arise. Iraq is exposed to it, which affected it geo-strategically and geopolitically, after relying on scientific-technical rules and postulates to deal with cybersecurity dilemmas, with reference to the fact that those in charge of cybersecurity are empowered to cover the gap of strategic exposure due to security dilemmas, and it will respond Find the following basic question: Can the strategic vision explain the security dilemmas in light of the cyberspace created by international change and achieve a breakthrough in Iraqi cybersecurity? While providing a coherent road map, initiatives and mechanisms to implement and achieve the national vision on cybersecurity in the context of national prosperity; Because it provides excellent platforms and opportunities to secure and develop the state's economy, it gives the Iraqi decision-maker a sense of the need to work on preparing a sound security environment in the future.

Keywords: Strategy, Security, Cyber, Threat, Security Dilemma, Iraq.

المُقدمة

إن البحث في تشكيل الأمن السيبراني العراقي، وطرق تحقيقه في مرحلة ما بعد التغيير العالمي المعلوماتي المتسارع، أمراً يصعب إدراكه دون بناء تواجه التهديدات ونعالج المعضلات الأمنية في فضائه السيبراني واستخدام الوسائل التقنية لتجنب الاختراق المعلوماتي وقائياً واستباقياً، وهذا يفضي لتوصيف مجرى ظاهرة تشكيل الاستراتيجية الأمنية السيبرانية العراقية التي طالما حرص صانع القرار على تحقيقها، إذ يعد التعامل ومعالجة المعضلة الأمنية السيبرانية العامل الحاسم والجوهري لتمكين الأداء الاستراتيجي في الفضاء السيبراني من تحقيق أهدافه،

عبر دوره المهم في تحديد نوع التشكيل الأمني الذي يرسم تلك الاستراتيجية ويراقب ذلك الفضاء المحمل بالمعضلات الأمنية الرقمية، بالإضافة إلى دوره المهم بوصفه المحدد الرئيس للتعامل مع حراك التهديد الأمني ذلك التهديد الذي بدا حالة مزمنة يعاني منها الأمن العراقي.

ومن هذا المنطلق، حاولنا استقراء تشكيل الأمن العراقي في الفضاء السيبراني بعد أن طرحت استراتيجية الأمن السيبراني العراقي وتزاحم على تناولها دراسة وبحث وتطبيق الأمنيين دارسين وممارسين، في محاولة لتشخيص المعضلة الأمنية في الفضاء السيبراني والوقاية احترازاً من تفاقمها، لكن قبل الخوض في التفاصيل لا بد من ذكر بعض المفردات المهمة لتكون له دليلاً في البحث، ولعل أهم تلك المفردات، هي :

أولاً: أهمية البحث

تكمن الأهمية في المكانة التي احتلتها الاستراتيجية الأمنية السيبرانية في المدرك الاستراتيجي العراقي بحثاً بناءً واستدامة الأمن الوطني في الفضاء السيبراني؛ كون القوة السيبراني تعد الحيز الخامس لعناصر القوة الاستراتيجية التي تحقق المكانة والدور والتأثير للدولة، فالدول في النظام الدولي تحرص على تحقيق امنها سيبرانياً.

ثانيا: إشكالية البحث

وتكمن في إن هناك تطور للتهديدات والمعضلات في الفضاء السيبراني يتكيف مع الاستراتيجية السيبرانية ويتطور عنها باستمرار، فلهذا لا بد من التحديث المستمر للاستراتيجية السيبرانية، وتلك هي اشكالية حقيقية.

ثالثا: تساؤلات البحث

يحاول الباحث الإجابة عن السؤال الرئيس التالي: هل يمكن وضع استراتيجية أمنية العراقية لمواجهة التهديدات والمعضلات في الفضاء السيبراني في ضوء هيمنة القوى الكبرى على الفضاء السيبراني وظهور الفواعل من غير الدول بوصفهم مهدد حقيقي لأمن العراق؟

وينبثق من هذا السؤال الأسئلة الفرعية التالية: ماذا نعني بالاستراتيجية الأمنية السيبرانية؟ بماذ تأثر الأمن السيبراني العراقي؟ كيف أثرت التهديدات والمعضلات الأمنية السيبرانية؟ وما العلاقة بين الأمن السيبراني والتهديد السيبراني؟ متى وضعت الاستراتيجية الأمنية العراقية؟من المسؤول عن الاستراتيجية الأمنية، وأين يسير الامن الوطني العراقي في

ضوء المعضلات والتهديدات الأمنية السيبرانية الاقليمية والدولية؟ وما مستقبل الأمن الوطني العراقي في ظل الفضاء السيبراني العالمي والإقليمي؟

رابعا: أهداف البحث

يسعى الباحث عن طريق البحث إلى تحقيق جملة من الأهداف وعلى النحو الآتي : التعرف على ماهية الاستراتيجية السيبرانية والمعضلة الأمنية وطبيعتها وكم التهديدات ومصادرها، والوقوف على الأسباب المفضية إلى التهديد السيبراني، وآليات المعالجة لتلك المعضلات، وتحديد أعراض وآثار التهديد السيبراني والتعرف على أبعاده، استعراض النماذج والمقاييس الأسس المعروفة في الأدبيات الأمنية حول المعضلات، والوقوف على دور القائمين على الأمن في الوقاية والعلاج لظاهرة التهديد السيبراني .

خامسا: فرضية البحث

استندنا على فرضية مفادها: ((كلما كانت الاستراتيجية الأمنية العراقية محكمة في الفضاء السيبراني عالجت المعضلات وتصدت للتهديدات)). وسنحاول إثباتها أو تفنيدها في نتائج البحث.

سادسا: **نطاق البحث**

1. **موضوعياً:** بظاهرة بالاستراتيجية الأمنية السيبرانية من حيث طبيعتها ومسبباتها وآثارها ومعالجاتها.
2. **شكلياً:** اقتصرت على المعضلات الأمنية السيبرانية مقابل التهديد السيراني.
3. **مكانياً:** اقتصر البحث على الساحة العراقية وبالتحديد الأمن الوطني السيبراني .
4. **زمانياً:** ركز البحث على حقبة ما بعد إطلاق الاستراتيجية السيبرانية 2017.

سابعا: مصطلحات البحث

بداية لابد من توضيح بعض المفاهيم ومنها:

1. **الاستراتيجية الأمنية:** هي التخطيط لتوظيف القدرات والإمكانات الأدائية لبناء واستدامة الوسائل الأمنية لتحقيق الأمن المستدام.
2. **الأمن الوطني:** هو توفير الحماية للمواطنين، والأفراد المتواجدين على أراضي الدولة، بمعنى، بناء الخطط واستخدام الإمكانات والوسائل الأمنية للمحافظة على سير الحياة

اليومية بشكل صحيح، وبعيداً عن وقوع أية أزمات تؤدي إلى التسبب بضرر، لمكونات المجتمع البشرية والمادية.

3. **الأمن السيبراني:** بناء الخطط واستخدام الإمكانات والوسائل التقنية التي يتم استخدامها لمنع الاستخدام غير المصرح به وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني.
4. **الفضاء السيبراني**: هو حيز التعامل مع العالم عن طريق شبكة الإلكترونية لها استقلاليتها من الداخل وتقوم بنيتها الأساسية على التقنيات الحديثة وهي كذلك أنظمة التعامل مع الحاسوب.
5. **المعضلة الأمنية**: هي الحالة التي تتسبب فيها الإجراءات التي تتخذها الدولة لزيادة أمنها في ردود أفعال من دول أخرى تؤدي إلى انخفاض في أمن الدولة بدلاً من زيادته وهذا الانخفاض يفضي إلى تعقد وفوضى في الأمن يصعب معالجتة متجاوزة حالة التهديد والمشاكل الأمنية.

ثامنا: مناهج البحث

استخدم الباحث التحليلي والاستقرائي لتحليل واستقراء الاستراتيجية الأمنية السيبرانية العراقية وتأثير المعضلات الأمنية الرقمية على العراق وسبل التأهيل والتمكين الأدائي الذي يثيره موضوع البحث، والتطرق إلى اهم متطلبات بناء الاستراتيجية للأمن السيبراني لضمان استدامة الاستراتيجية الأمنية.

تاسعا: هيكلية البحث

يتكون البحث الموسوم ((قراءة تحليلية لاستراتيجية الأمن السيبراني العراقي)) من مقدمة ومبحثين رئيسيين: الأول حمل عنوان: استراتيجية الامن السيبراني العراقي، وبدوره انقسم إلى مطلبين: الأول: اختص بالمعضلة الأمنية السيبرانية، أما الثاني: اختص بالتهديدات والمعضلات الأمنية، وتناغماً

مع ما مضى، جاء العنوان الثاني بـ: الاستراتيجية الوطنية للأمن السيبراني: الدلالة والمتطلبات، لينشطر إلى: مفهوم ودلالة والثاني: ركز على: ضرورات الأمن السيبراني في ضوء التهديدات في الفضاء السيبراني، اما المبحث الثاني: التهديد والمعضلة الأمنية السيبرانية: المتطلبات والمعالجات، لينقسم الى مطلبين، الأول: التهديدات والمعضلات الامنية السيبرانية، والثاني: المعالجات الوقائية والاحترازية في الفضاء السيبراني، لنختم البحث بجملة من النتائج والتوصيات.

المبحث الأول: الاستراتيجية الوطنية للأمن السيبراني: المفهوم والدلالة

لا شك إن هناك صعوبة في فهم، أو أدرك، التهديدات والمعضلات الأمنية لسيبرانية لاكتظاظها بالمحفزات الدافعة لاختراق الأمن الوطني من الفجوات الرخوة، والذي بدا فيها التهديد في أوجه، لهذا بدت صعبة التشخيص والعلاج على الكثير من المعنين بها، لما تضمن من تداخل بين التهديد الواقعي والتهديد الافتراضي فانعكست سلباً على العراقيين ساسة وشعب لا سيما وأن العرق مر بمعضلة أمنية كبيرة (2014-2016) وهي معضلة داعش، بعد أن لم يتمكن صناع الأمن السيبراني من حرف مسار التهديد السيبراني بالاتجاه المطلوب في الحقبة السابقة وحال ما ادرك الأمنيين ذلك الخلل حتى سارعوا إلى وضع استراتيجية للأمن السيبراني.بعد التخلص من الإشكالية الأمنية الواقعية الحقيقية عام 2017.

ولعل أفضل ما يفسر ماهية وضرورات تلك الاستراتيجية، هو البحث عن مصدر المعضلات الأمنية ومعرفة سبب استفحالها وسبل معالجتها لكن قبل ذلك لا بد من تحديد المفهوم والدلالة، فسجلات الأمن العراقي، أشرت ذلك المفهوم ودلالة بعد أن حققوا الأمن على ارض الواقع، وما أدوه من دور في إعادة رسم الخارطة الجيو- سكيورتية بين حقبة وأخرى، فالواجب علينا أن نتصفح تلك السجلات ممعنين النظر بها، في محاولة منا لتقييم الوضع الأمني ووضع استراتيجية لمستقبل الأمن العراقي السيبراني، ولأجل أبانت هذا كله عمد الباحث إلى تقسيم المبحث على مطلبين وعلى النحو الآتي:

المطلب الأول: مفهوم الاستراتيجية الأمنية السيبرانية

الاستراتيجية الوطنية للأمن السيبراني هي استراتيجية الاستعداد الوطني لتوفير تدابير متماسكة وإجراءات استراتيجية لضمان أمن وحماية الوجود العراقي في الفضاء السيبراني، وحماية البنية التحتية الحيوية للمعلومات، وبناء ورعاية مجتمع إنترنت موثوق به.[1]

وتتألف استراتيجية الأمن السيبراني الوطنية من عدة استراتيجيات قصيرة ومتوسطة وطويلة الأمد تغطي جميع الأولويات الوطنية، وتعالج التعرض الوطني للمخاطر السيبرانية، هنالك تهديدات سيبرانية رئيسة في جميع أنحاء العالم التي تضر بالمصلحة الوطنية، مثل: الجريمة الإلكترونية والإرهاب الإليكتروني والصراع السيبراني والتجسس السيبراني وإساءة معاملة الأطفال واستغلالهم عبر الإنترنت والتجنيد للمنظمات المسلحة الخارجة عن القانون ونشر الكراهية والتطرف العنيف وتلك تحولت من تهديد إلى معضلات أمنية تطلب المعالجة [2].

والذي لا يمكن نكرانه إن التهديدات السيبرانية لها مخاطرها وتهديداتها على الأمن الوطني التي تعطل البنية التحتية الحيوية للمعلومات والبيانات عن طريق اختراق أجهزتها التي يتطلب بناء منظومة احترازية للوقاية منها وإلا تكون المؤسسات العراقية عرضة للتهديد والاختراق الإلكتروني عبر السايبر[3].

لهذا فإن الاستراتيجية الوطنية هي جملة من المبادرات وآليات التنفيذية والتشريعية والتنظيمية والقضائية التي تعمل على بناء قدرات الدولة وإمكاناتها ووسائلها التقنية في مجال التمكين المؤسساتي والفردي عن طريق تفعيل مراكز البحث والتطوير والتأهيل السيبراني، والعمل على تحديد وتنسيق والتوجيه الجهد اللوجستي والتقني لأخذ جميع التدابير الاحترازية ضد التهديدات السيبرانية والجاهزية للتصدي لحوادث والهجمات السيبرانية وفتح قنوات التنسيق الدولي في مجال التعاون من اجل بناء الأمن والسلام السيبراني العالمي[4].

وللاستراتيجية السيبرانية العراقية رؤية وهدف ورسالة، فرؤيتها: بناء مجتمع آمن ومضمون ونابض بالحياة ومرن وموثوق به يوفر فرصا لمواطنيه ويحمي الأصول والمصالح الوطنية ويعزز التفاعلات السلمية والمشاركة الاستباقية في الفضاء السيبراني من أجل الرخاء الوطني، أما هدفها: توفير خارطة طريق متماسكة ومبادرات وآليات لتنفيذ ولتحقيق الرؤية الوطنية بشأن الأمن السيبراني، ورسالتها: تمكين الجميع في استخدام الفضاء السيبراني[5].

وهذا ما يعتمده المؤشر العالمي للأمن السيبراني منذ عام 2015، وفي نسخة 2021 التي أصدرها الاتحاد العالمي للاتصالات جاءت أمريكا في المركز الأول وبدرجة 100% والسعودية في المركز الثاني بدرجة99.5%.، وكان ترتيب الدول العربية ضمن مركزها العالمي في الشكل التالي:

الدولة	عربيا	عالميا
السعودية	1	2
والإمارات	2	5
عُمان	3	21
مصر	4	23
قطر	5	27
تونس	6	45
المغرب	7	50
البحرين	8	60
الكويت	9	65
الأردن	10	71
السودان	11	102
الجزائر	12	104
لبنان	13	109
ليبيا	14	113
فلسطين	15	122
سوريا	16	126
العراق	17	129
موريتانيا	18	133
الصومال	19	137
جرز القمر	20	175
جيبوتي	21	179
اليمن	خارج التصنيف	

Global Cybersecurity Index

ويلاحظ إن العراق حصل المرتبة 129 عالميا في المؤشر من اصل193دولة، بينما كان في المركز107 في مؤشر عام 2020، مبيناً أن الأمن السيبراني وحماية بيانات العراقيين،جزء لا يتجزأ من الأمن القومي العراقي، وتراجع العراق عربيا، كذلك إذ حصل على المرتبة 17 متقدماً على موريتانيا والصومال، وجزر القمر، وجيبوتي، واليمن، بينما تفوقت عليه بقية الدول العربية بما فيها سوريا، وفلسطين، وليبيا، ولبنان، والسودان.

وإذا ما دققنا نجد إن سبب التراجع أن العراق لم يقدم(إجابات عن الاستبيان الذي جمعه فريق المؤشر والذي تضمن بعض المعلومات والبيانات، وهو الأمر الذي يطرح عدة أسئلة حول سبب هذا التجاهل للجهات المسؤولة عن هذا ملف الامن السيبراني في العراق).

وتشير بعض الدراسات إن هذا التراجع في الملف الأمني السيبراني إنما يعود إلى عدم وجود مؤسسة متخصصة بالأمن السيبراني في العراق(وما هو موجود عبارة عن أقسام في دوائر مختلفة تفتقد للتنسيق أو التعاون المحترف في هذا الجانب، وكل جهة منها تعمل بمفردها).

المطلب الثاني: دلالة الاستراتيجية الأمنية في الفضاء السيبراني

بداية دلالية يوصف الفضاء السيبراني بانه شبكة مترابطة من الهياكل الأساسية للمعلومات الأساسية الحرجة وغير الحرجة، والذي يعمل على تقريب موارد المعلومات والاتصالات المترابطة عن طريق استخدام تكنولوجيات المعلومات والاتصالات، وهو يشمل جميع أشكال التدخلات الرقمية، التفاعلات والتواصل الاجتماعي، التخصصات الاجتماعية، أنشطة المعاملات، المحتويات، والاتصالات، والموارد التي يتم نشرها عبر الشبكات المترابطة[6].

السؤال هنا: لماذا يجب أن يعد الفضاء الإلكتروني مهماً للعراق؟ والجواب: ثبت فاعلية العالم الرقمي على المستوى العالمي وفي شتى مجالات الأرض والبحر والجو، لذلك يعد مجال الفضاء السيبراني هو المجال الرابع لما له من تأثير فعال وواضح في قيادة المهام الوطنية الحرجة مثل التنمية الاقتصادية والتجارة والمعاملات، والتفاعلات الاجتماعية، والطبية والصحية، والعمليات الحكومية، والأمن القومي والدفاع[7].

وتحديداً للمهم هو العلاقة بين الاقتصاد والأمن السيبراني فانه الفضاء السيبراني يوفر منصات وفرصاً ممتازة لتأمين وتنمية اقتصاد البلاد، وإن كل مواطن مرتبط بالفضاء الإلكتروني عبر الإنترنت يتأثر بشكل لا يمكن تصوره ويسمح له باتخاذ الإجراءات، والعراق اقتصادياً دخل في نطاقاً الفضاء السيبراني، والفضاء السيبراني هو الاتجاه السائد لتحقيق التكامل الوطني وتمكين الاقتصاد الرقمي، وهو فضاء مدعوم بالمعرفة مع قدرة هائلة على سد الفجوات في التنقل والتجارة والابتكارات والتعليم والحد من الفقر والتمكين الاقتصادي، والعراقيون يجب أن يدركوا إن الاقتصاد الرقمي والعملة الرقمية والمؤسسات الرقمية هي من سيهيمن على الاقتصاد العالمي[8].

المبحث الثاني: التهديد والمعضلة الأمنية السيبرانية: المتطلبات والمعالجات

تبعاً لضخامة القصد من ماهية أمن الوطني العراقي، تداخلت الكثير من العلوم الاختصاصية في تفسير تلك الماهية، فاحتدم الجدل والنقاش حول ما تعنيه تلك المفردة من رؤى وأفعال وصور ناطقة، فالأنموذج المؤصل للتكتلات الأمنية وأن كان يقوم أساساً على التقارب التفاعلي بين القوى الأمنية المتعاونة تكاملاً لتحقيق الأمن، عبر نوافذ التحالف والتآلف ومسالك التناسق الأدائي، لم يعد يمثل مرجعية للتطابق والاتساق بين تلك العناصر فحسب، وإنما بدا الإطار العام الذي يتم عن طريق تحديد صلاحية الأمن التكاملي ومدى اتساقه بفلسفة صناع القرار، وعلى النحو الآتي:

المطلب الأول: التهديدات والمعضلات الامنية السيبرانية

من المعروف أن تمثل التهديدات السيبرانية بتحديات غير مرئية توثر على منظومة الأمن[9]، فالتطور التكنولوجي الذي شهده العراق في مجال المعلومات والاتصالات بعد عام 2003 تزامن معه ضعف الأمننة الإلكترونية وركاكة البنية التحتية أدى إلى أن يصبح العراق منكشفاً استراتيجياً لكثير من دول العالم، يسهل اختراقه والتجسس على مؤسساته[10]، وهذ يتطلب المعرفة بأساسيات الأمن السيبراني [11]، والقدرة على التحقيق والتشخيص والتحقيق الرقمي[12].

وازداد الاختراق اختراقاً لدرجة استخدام العراق كساحة لشنّ الهجمات الإلكترونية لضرب أمن معلومات دول أخرى واختراق منظومتها الأمنية الإلكترونية، فضلاً عن استراق أي معلومة واستخدامها لأغراض المساومة، أي: لتنفيذ عمليات هكرية وإسنادها، ومن الملاحظ أن أكثر المؤسسات العراقية تتعاقد لتجهيز معلوماتها من أقمار صناعية ذات مورد خدمة واقع خارج الحدود العراقية الذي يؤدي إلى مرور تلك المعلومات في خوادم تلك الدول، ورجوعها إلى العراق إذ يشكل هذا الإجراء خرقاً لأمن المعلومات العراقي[13].

ولتلافي مثل هذه الخروقات الكبيرة التي تتعرض لها حركة المعلومات في العراق يتوجب بناء منظومة متكاملة لأمن المعلومات، لذا يتوجب بناء منظومة للأمن الإلكتروني العراقي بهدف حماية الفضاء السيبراني الوطني، مع التركيز على ضمان توافر أنظمة المعلومات وتمتين الخصوصية، وحماية سرية المعلومات الشخصية، واتخاذ جميع الإجراءات الضرورية لحماية امن المواطنين وامن المؤسسات من مخاطر الفضاء ال ويُعَ دُ التهديد السيبراني حافزاً

لإعادة صياغة الأمن السيبراني، فالمعضلة الأمنية تفسر التفاعلات الاستراتيجية واللوجستية الأمنية [14].

والسؤال الرئيسي هو: كيف يستجيب العراق للتهديدات السيبرانية؟ والجواب: يستجيب عن طريق التحالف مع الآخرين ضد التهديد السيبراني السائد، ويمكن أن نؤكد ذلك، "بمقاربة العراق مع الدول التي تعد التهديد هو الأكثر شيوعاً من الأمن في الفضاء السيبراني، فلو تم استعرض التفاعلات الأمنية السيبرانية في الشرق الأوسط لوجدنا أنها تفاعلات محملة بالمعضلات لعدم وجود غطاء استراتيجي يؤمنها من الاختراق والعراق جزء من الشرق الأوسط ومعضلاته متقاربة، فهو متأثر بالانكشاف الاستراتيجي في الفضاء السيبراني، فالعراق دون استراتيجية امنية سيبرانية شاملة فاعلة أكثر عرضة للمعضلات الأمنية لسببين:الأول: عدم مواكبة الطفرات التقنية العالمية، والثاني: الاعتماد على القوى الإقليمية والدولية في مجال الدعم التقني- الأمن[15].

واستمراراً في الوصف ووصولاً إلى تأثير المخاطر السيبرانية على الأمن الوطني العراقي، نجد أنه:

1. يعتمد الوجود الاقتصادي الرقمي للبلد على الأداء الفعال للبنية التحتية الرقمية، وفي الفضاء السيبراني، فإن البلد ليس معزولاً ولكنه مترابط مع بلدان أخرى وجهات فاعلة في الفضاء السيبراني من خلال شبكات مترابطة للبنى التحتية للمعلومات، وبالتالي، فإن البلد معرض لمخاطر يمكن التنبؤ بها و أخرى لا يمكن التنبؤ بها.
2. هناك جهات فاعلة ذات نوايا مشروعة، وهناك جهات فاعلة أخرى ذات نوايا غير مشروعة وخبيثة، داخل الشبكة العالمية للشبكات، توجد عيوب هيكلية حرجة يمكن استغلالها لأغراض خبيثة ونوايا جنائية ضد البلد من أجل المساس بامن وسلامة الدولة لا بد من الوقاية منها.
3. نظم المعلومات الوطنية والبنية التحتية الحيوية للمعلومات وسالمتها وتوافرها وإمكانية الوصول إليها ومما ينعكس سلباً على المواطن وبالتالي على الأمن الوطني.
4. توجد مواطن ضعف في الفضاء السيبراني يمكن استخدامها الاستغلال المصالح الاقتصادية الوطنية وتشكل تهديداً لألمن القومي.

يمكن إجمال تلك الخروقات والتهديدات بالشكل الاتي[16]:

• العمليات التخريبية التي أصابت بعض المواقع الحكومية • وتزايد صناعة الجريمة السيبرانية • الممارسات الاحتيالية • وقوع الاستغلال عبر الإنترنت من شريحة الشباب من السكان • إساءة استخدام وسائل الأعلام ومواقع التواصل الاجتماعي لشن حملات خبيثة ضد الدولة • الصراع والعنف المستمر من خلال الإنترنت • التخريب الاقتصادي من خلال حرمان المواطنين من الوصول إلى الخدمات الإليكترونية الحكومية وغير الحكومية	• التجسس الإلكتروني المنسق • التدخل الخبيث في أنظمة الكمبيوتر والأجهزة الرقمية الأخرى • القرصنة الإلكترونية • سرقة الأصول الفكرية • الإرهاب الإلكتروني • الجرائم المالية عبر الإنترنت • غسل الأموال.

كل هذه الأمور لا تنسجم مع سياسة الرفاهية لأي دولة ولها الأثر الاقتصادي الذي يكون كفيل بتدمير أي دولة وعلى صعيد العراق، نجحت حلول "ترينـد مايكرو" باكتشاف وحظر أكثر من 15 مليون تهديد عبر البريد الإلكتروني، وقامت بحماية أكثر من 400 ألف مستخدم من التضرر من روابط خبيثة قاموا بالضغط عليها، كما استطاعت تحديد وإيقاف أكثر من نصف مليون هجوم لبرمجيات خبيثة في الدولة[17].

أما عواقب الهجمات السيبرانية الأمنية والاقتصادية يمكن اختصارها في الشكل الاتي:

- سرقة الهوية
- تزوير
- الابتزاز
- البرمجيات الخبيثة
- تزييف
- والتصيد
- البريد الإلكتروني غير المرغوب
- خداع
- برامج التجسس
- سرقة الملكية الفكرية
- أحصنة طروادة والفيروسات
- التلاعب بالأجهزة
- والحرمان من الخدمة
- خرق الوصول
- سرقة كلمة المرور
- نظام التسلل
- تشويه الموقع
- يستغل متصفح الويب الخاص والعام
- الرسائل الفورية وإساءة استخدام وسائل الأعلام والتواصل الاجتماعي

المطلب الثاني: المعالجات الوقائية والاحترازية في الفضاء السيبراني

يحمل الفضاء السيبراني تأثيره في مختلف المجالات الاستراتيجية ومنها المجال الأمني، إذ يساهم الفضاء السيبراني وعن طريق أدواته المختلفة في إعادة رسم البعد الأمني المحلي والعالمي، إذ يعمل على إعادة تشكيل الوعي والإدراك السياسي والأمني للعراقيين أفراد وجماعات بصورة مغايرة عما كانت عليه، إذ نجد تصورات وبنى جديدة يتم تأسيسها في المجال السياسي والأمني، إذ لم يعد الأمن يعيش في العالم الواقعي – المحدود وإنما اصبح للاواقعية واللامحدودية التي يشكلها الفضاء السيبراني حضورها المؤثر في المجال الأمني واصبح الحديث عن الحرب السيبرانية والأمن السيبراني والردع السيبراني والجيوش السيبرانية والأسلحة السيبرانية والإرهاب السيبراني والجريمة السيبرانية وغيرها واتجهت الدول نحو تأسيس مؤسسات بحثية وأمنية تهتم بدراسة الفضاء السيبراني وكيفية توظيفه بالشكل الذي يساهم في تحقيق مصالحها السياسية والأمنية والاقتصادية وغيرها، ليكون التحدي المستقبلي الذي يفرضه الفضاء السيبراني يتمثل في قدرة الدول على التكيف مع التغيير السريع والتحديات التي يفرضها الفضاء السيبراني في المجالات العامة عموماً والمجال الامني خصوصاً، إلى جانب امتلاك القدرات والبنى المادية والبشرية التي تمكنها من إن تكون مؤثرة وفاعلة فيه. وهذا التأثير الذي يحمله الفضاء السيبراني في المجال الأمني لا يقتصر على الواقع الداخلي للدول وإنما يمتد إلى المحيط الدولي الواسع ليؤثر في إعادة رسم شكل ومضمون الأمن الدولي ويحدد اطر جديدة لطبيعة العلاقات الدولية والأمن الدولي[18].

والذي لا يمكن نكرانه إن العراق من الدول العديد التي تواجه تحدي الفضاء السيبراني في مختلف مجالاته ومنها المجال الأمني،فحالة الضعف التي يعيشها تعقد المسالة اكبر فهو لايزال يعاني عدم الاستقرار العام ولا يمتلك القدرات المطلوبة للتكيف مع تلك التحديات التي يفرضها الفضاء السيبراني، فمع الانتقال السريع للمجتمعات من الفضاء الحقيقي إلى الفضاء الافتراضي وجد العراق نفسه يدخل إلى هذا الفضاء الواسع وسريع الحركة دون أن يمر بمرحلة انتقالية، فالبنى المادية والبشرية في العراق لاتزال غير قادرة على التفاعل الإيجابي مع تلك التحديات العديدة للفضاء السيبراني،وعند البحث الإمكانيات العراقية في مجال الأمني السيبراني سنجد بان العراق لايزال يحتاج الكثير من الجهد المعرفي والإداري والقانوني والتقني لكي يكون قادر على التأثير في المجال الأمني الافتراضي من جهة ومن جهة

أخرى قادر على حماية أمنه السيبراني من التهديدات السيبرانية، وعند النظر في المؤشر الأمن السيبراني العالمي وهو مؤشر يصدر عن الاتحاد العالمي للاتصالات يشمل مركب يجمع (25) مؤشراً في معيار واحد لرصد ومقارنة مستوى التزام الأمن السيبراني للبلدان فيما يتعلق بالاتفاقية الركائز الخمس لجدول أعمال الأمن السيبراني العالمي.

هذه الركائز تشكل خمسة مؤشرات فرعية من مؤشر الأمن السيبراني العالمي والتي تشمل[19]:

1. القانونية: التدابير القائمة على وجود المؤسسات والأطر القانونية التي تتعامل مع الأمن السيبراني والجريمة الإلكترونية.
2. التقنية: التدابير القائمة على وجود المؤسسات الفنية والتعامل مع الأمن السيبراني.
3. التنظيمية: التدابير القائمة على وجود مؤسسات واستراتيجيات تنسيق السياسات لتطوير الأمن السيبراني على المستوى الوطني.
4. بناء القدرات: التدابير القائمة على وجود البحث والتطوير والتعليم وبرامج التدريب والمهنيين المعتمدين ووكالات القطاع العام التي تعزز بناء القدرات.
5. التعاون: التدابير القائمة على وجود شراكات وأطر تعاونية وشبكات تبادل المعلومات.

سنجد بأن العراق وعلى االرغم من التحسن الذي حدث في موقعه في المؤشر فهو يزال في موقع متأخر، إذ نجد بأن موقع العراق في المؤشر للعام 2018 (107) عالمياً و(13) محلياً، بعد أن كان في عام 2017 في المرتبة (158) عالميا و(19) محلياً، وعند البحث عن أسباب هذا التحسن سوف هنالك جهود حكومية عديدة اتخذها العراق في هذا المجال والتي شملت الآتي[20]:

1- تأسيس فريق الاستجابة للأحداث السبرانية، وهو فريق وطني مشترك مختص بمجال الأمن السبراني والاستجابة للحوادث السبرانية وحماية البنية التحتية للأنترنت ونشر الوعي في مجال حماية الخصوصية والحماية الذاتية للأفراد والمؤسسات على الأنترنت يعمل تحت إشراف مستشارية الأمن الوطني العراقي، يحمل الفريق على عاتقه مسؤولية تأمين و حماية الشبكات ومراكز البيانات الوطنية والمواقع الرسمية التي تعمل في مجال الفضاء السبراني العراقي ويقوم بتنسيق الجهود الوطنية ودعم

المؤسسات في القطاعين العام والخاص في حماية نفسها وخدماتها في الفضاء السبراني.

2- القراءة الأولى لقانون الجرائم المعلوماتية.

3- عقد العديد من المؤتمرات وورش العمل والندوات عن الأمن السيبراني

4- كتابة العديد من البحوث والدراسات في مراكز الأبحاث والجامعات العراقية حول الأمن السيبراني.

لكن مع ذلك لايزال العراق بحاجة إلى جهد كبير للتكيف مع تحدي الفضاء السيبراني في مختلف المجالات ومنها المجال الأمني، وذلك من خلال العمل على إجراء الآتي:

1- بناء البنية المادية والبشرية المطلوبة للتعامل مع الفضاء السيبراني.

2- العمل تأسيس كليات وأقسام علمية في الجامعات العراقية المدنية والعسكرية تختص بالأمن السيبراني تمنح درجات علمية في تخصص الأمن السيبراني.

3- العمل على بناء مؤسسات أمنية تختص بمكافحة التهديدات السيبرانية في مختلف المجالات ومنها المجال الأمني.

4- قيام المؤسسات الامنية المختلفة في العراق على بناء قوات امنية سيبرانية مثل (شرطة سيبرانية، ومخابرات واستخبارات سيبرانية، وجيش سيبراني وغير ذلك) من اجل مواجهات التهديدات السيبرانية الداخلية والخارجية.

5- العمل على بناء وعي إعلامي وثقافي حول خطورة التهديدات السيبرانية.

6- بناء منظومة قانونية تتعلق بجرائم السيبرانية.

7- المشاركة في الجهود الدولية المتعلقة بالأمن السيبراني، مثل الاتفاقيات الدولية والمؤتمرات التي تعقد حول خطر التهديدات السيبراني وكيفية التعامل معها دولياً.

أما بخصوص مصادر التهديد فهي عديدة منها: الدول الأجنبية والعصابات الإلكترونية المنظمة والإرهابيين والجماعات المتطرفة، و الهاكرز، والشركات الإلكترونية المنافسة، والشركات الإلكترونية الوهمية الأجهزة الاستخبارية –السيبرانية[21]، لهذه التهديدات قدرة كبيرة على إحداث أضرار جسيمة لسلامة اقتصاد البلد، إذا ما ترك منكشف استراتيجياً.

ومسببات التهديد عديدة مثل: ضعف منظومة الأمن السيبراني وكثرت التغرات لنظم المعلومات بفعل العيوب التقنية والإهمال التقصيري والتدابير غير المدروسة التي تاتي بعد الاختراقات وتنتهي بعد انتهاء العملية، و غياب التقييم الشامل لقياس مواطن القوة وتعزيزها وتشخيص مواطن الضعف ومعالجتها، وغياب التقنيات الرقمية الاقتصادية، وعدم مواكبة النقلة النوعية الاقتصادية في العالم الرقمي، وهشاشة البنى التحتية الرقمية عدم امتلاك عملة رقمية، وغياب التشريعات القانونية الرقمية، وعدم وجود حكومة ومؤسسات الإلكترونية عدم الثقة بالاقتصاد الرقمي، وغياب آليات التجارة الإلكترونية، وغياب التدابير الاحترازية الرقمية لحماية المنتج والمستهلك الرقمي[22].

وصولاً إلى المعالجات التي من الضروري أن يتبعها صانع الاستراتيجية العراقي لضمن الأمن والسلام في الفضاء السيبراني وعلى النحو الآتي: التوجه نحو بناء منظومة استراتيجية سيبرانية، وحماية البنى التحتية الرقمية، والقدرة التنافسية الاقتصادية العالمية في الفضاء السيبراني، وتشكيل خلية الأزمة لإدارة المخاطر السيبرانية، والتعبئة الشاملة والمشاركة والتنسيق للمكونات الحاسمة لضمان وجودنا في الفضاء السيبراني وحماية البنى التحتية للمعلومات الحيوية، وتأمين الفضاء السيبراني، واستغلال فرص الفضاء الإلكتروني لأغراض الأمن القومي والأهداف الاقتصادية، والعمل على دعم مجتمع سيبراني موثوق به، وضع خارطة طريق وطنية مع آليات منسقة مختلفة؛ إطار تنفيذي؛ والإجراءات التي تضمن تحقيق الرؤية الوطنية والأهداف المتعلقة بالأمن السيبراني[23].

الخاتمة والنتائج

الخلاصة من كل ما عرض آنفاً، يمكن القول: أن الاستراتيجية السيبرانية العراقية تواجهه تهديدات كبيرة ومعضلات أمنية خطيرة بحاجة إلى تفعيل الأمن السيبراني وفق استراتيجية وطنية فاعلة في الفضاء السيبراني وهناك علاقة طردية بين الأمن والمعضلة الأمنية، فلما ازدادت المعضلة الأمنية ازداد التهديد، وكلما ازداد التهديد أزادت الحاجة لرفع الإمكانات الأدائية المعرفية والتقنية للحفاظ على الأمن وضمان استدامته، وهذا الأمر يعتمد كثيراً على امتلاك القائمين على الأمن أجهزة الحماية الإلكترونية التي تقوى كلما تطور التهديد لحصره وتحجيمه، وهذا إن دل على شيء، فإنه يدل على أهمية الاستراتيجية الأمنية للتعامل مع المعضلات المستقبلية .

عموماً الأمن هو أكثر شيوعاً من التهديد في العراق، فالأمنيين يميلون لامتلاكهم مقومات القوة وقدرات الردع ومصداقية المعالجة في الفضاء السيبراني، ويميلون إلى بناء منظومة أمنية ذكية لها القدرة على تتفكك التهديد .

ففلسفة الامننة الرقمية تعني إضفاء الطابع الأمني على معضلة رقمية ما وعدها تهديد حقيقي وجوهري، والعلاقة بين الأمن والتهديد علاقة عكسية تضادية متلازمة، فإذا كان الأمن أكثر شمولاً ضعف التهديد، وإذا كان التهديد أكثر شمولاً ضعف الأمن .

وتبعاً لهذا الفهم، اتضح الأمن السيبراني العراقي، وبات من السهل واليسر استقراء التهديد الأمني الرقمي وتحليل الأداء الاستراتيجي في الساحة العراقية ما بعد،2017 بعد إن تم استقراء الاستراتيجية العراقية في تشكيل الأمن السيبرانى، لنخرج بجملة من النتائج منها :

1. الأمن السيبراني من اهم فروع الأمن الوطني العراقي.
2. الأمن السيبرانية يتطلب بناء منظومة استراتيجية أمنية سيبرانية متكاملة.
3. العراق حاله حال دول الشرق الأوسط فهو يعاني من الانكشاف الاستراتيجي السيبراني.
4. العراق تعرض للعديد من الهجمات في الفضاء السيبراني بسبب المكنّة المتواضعة في المجال التقني.
5. هناك علاقة عكسية بين التهديد والأمن في الفضاء السيبراني تتقارب طردياً.

كما خلصت هذه الدراسة إلى التوصيات الآتية :

1. إنشاء مراكز بحثية للأمن السيبراني .
2. بناء منابر تخطابية على منصات التواصل الاجتماعي لإشاعة لغة الأمن والسلام العراقي .
3. إدانة صناع النزاع والصراع الرقمي "ومحاكمتهم.
4. بناء منظومة أمنية رقمية متكاملة.
5. تقنين الامننة وعدم اعتماد الانتقاء والتسيس لمعضلات مجتمعية القصد منها كسر أواصر النسق الأمني.
6. تطبيق الأمن السيبراني وفقاً لمبادئ الأمن السيبراني العالمي.
7. عدم الاعتماد على القوى الخارجية في حماية الامن الوطني السيبراني العراقي.

8. اعتماد "الاستراتيجية الأمنية السيبرانية العراقية "مادة تدرس في الأكاديميات العسكرية والأمنية والجامعات العراقية.
9. بناء قاعدة بيانات ذكية لجميع سكان العراق.
10. تحويل المؤسسات العراقية إلى مؤسسات ذكية عالية التقنية.
11. تفعيل الحكومة الإلكترونية العراقية بكافة تشكيلاتها.
12. نشر التخصصات الأمن السيبراني في المؤسسات الأكاديمية المدنية والأمنية

التوصيات

هناك جملة من التوصيات للقائمين على الأمن السيبراني العراقي وعلى النحو الآتي:

1. إصدار تشريعات شاملة لتعزيز الاقتصاد السيبراني ومكافحة الجريمة السيبرانية الاقتصادية والتدابير المضادة للتهديد السيبراني التي يمكن اعتمادها على الصعيد الوطني، وتواكب التشريعات الدولية ذات الصلة في سياق تأمين الفضاء السيبراني للبلاد .
2. توفير التدابير التي تحمي البنية التحتية الحيوية للمعلومات، فضالاً عن الحد من مواطن الضعف والثغرات الوطنية من خلال إطار ضمان الأمن السيبراني .
3. وضع آليات فعالة للاستجابة لحالات الطوارئ الرقمية.
4. العمل على تحسين قدرة وتطوير مهارات فريق الاستجابة لحالات الطوارئ في الفضاء السيبراني العراقي.
5. إن الآليات الوطنية لبناء القدرات والتوعية العامة وتمكين المهارات ضرورية للمساعدة في تعزيز قدرتنا على الاستجابة السريعة والفعالة للهجمات السيبرانية.
6. وضع آلية موثوقة لإشراك أصحاب المصلح المتعددين والوطنيين والدوليين من أجل التصدي بشكل جماعي للتهديدات السيبرانية .
7. بناء منظومة امنيه لردع وحماية المؤسسات الحكومية وغير الحكومية من جميع أشكال الهجمات السيبرانية .
8. تنسيق مبادرة الأمن السيبراني على جميع مستويات الحكومة في البلاد.
9. بناء منظومة اقتصادية سيبرانية متكاملة مؤمنة
10. حماية حقوق وحريات الأفراد في الفضاء السيبراني

المصادر والمراجع:

(1) Midea S Ali, A Brief Review of Cybersecurity Issues in Iraq,Technical Report ,(University Sains
Malaysia, April 2018),p.5.

(2) Sattar J. Aboud, Cybercrime in Iraq,(International Journal of Scientific and Engineering Research Vol. 5,No. 2,2018),p. 63-64

(3) Ali Ziad al-Ali,The Hidden Threats to Iraq's National Security,article in National security and
defense, 07/10/2018,pp.2-3.

(4) Tallinn, Economic Aspects of National Cyber Security Strategies, Project)Report , 2015),p7.

(5) استراتيجية الامن السيبراني العراقي، مستشارية الامن الوطني العراقي، امانة سر اللجنة الفنية العليا لأمن الاتصالات والمعلومات.، https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/00056_06_iraqi-cybersecurity-strategy.pdf

(6) علي زياد العلي، التحديات غير المرئية للأمن الوطني العراقي، مركز البيان للدراسات والتخطيط، 2018. http://www.bayancenter.org/2018/06/4565

(7) Sattar J. Aboud, An Overview of Cybercrime in Iraq, The research bulletin jordan ACM (Jordan: Center of Innovations in Computing and Engineering Machinery, Vol. 2, No. 2, April 2012,p.31.

(8) Nmi Presents ISG Report on Cybersecurity Threats in Iraq to Iraqi President, Institute for Security Governance ,Sept 13, 2023, https://instituteforsecuritygovernance.org.

(9) Ben Buchanan. The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations, New York: Oxford University Press, 2017 ,p.23.

(10) Samer M. Abdulhamza, The Iraqi Legislative Policy to Protect National Cyber Security A study in the light of the principles of public international law, Vol. 14 No. 4 ,2022 ,pp.533-534.

(11) حسن محمد الحسين، أساسيات الأمن السيبراني، الامن الالكتروني، سوريا، 2022، ص23.

(12) محمد سعيد العامري، عادل عبدالله حميد، محمد الأمين البشري، الأمن السيبراني والتحقيقات الرقمية، أبوظبي: المتحدة للطباعة والنشر، 2021، ص ص 23-23,

(13) اسراء شريف جيجان، الأمن السيبراني الصيني دراسة في الدوافع والتحديات. قضايا سياسية،جامعة النهرين العدد 65، 2021،ص 33-47.

(14) Sadek, G. Iraq: Parliament Considers New Anti-cybercrimes Bill, Global Legal Monitor, Washington D.C.: Library of Congress, Law Library(2021),. https://www.loc.gov/law/foreign-news/article/iraq-parliament-considers-new-anticybercrimes-bill

(15) 1Midea Sabah Ali, Selvakumar Manickam, A Brief Review of Cybersecurity Issues in Iraq, April 2018, p 3.

(16) Global Cybersecurity Index 2020, International Telecommunication Union Development Sector, ITUPublications,2021,P6.

[17] 20 مليون تهديد في العراق.. تقرير الأمن السيبراني يكشف حصيلة، الشفق نيوز 2022، 17-07-2023 10:16 اطلع عليه 22/ 4/ 2024، https://shafaq.com/ar

[18] Barad, M. Definitions of strategies Strategies and Techniques for Quality and Flexibility , Springer2018, pp. 3-4.

[19] Yasin Salman Saadoun Al-Wasiti, Firas Raheem Younis Alazzawi, Requirements of Formulating a National Strategy for Developing the Cybersecurity System in Iraq According to GCI.v4(2019) Index, Review of International Geographical Education , Vol. 11,No.4, Winter , 2021,p p. 50-70

[20] S.J. Aboud, An overview of cybercrime in Iraq, The Research Bulletin of Jordan ACM, No. 22021, p.p.31–34.

[21] M.S. Ali, and, S. Manickam, A Brief Review of Cyberscurity Issues in Iraq, Technical Report, Palau Pinang: Universiti Sains Malaysia, 2018,p4-7.

[22] H.M.K.Duhaidahawi, , J. Zhang, M.S. Abdulreza, M. Sebai, and S.A. Harjan, Analysing the effects of FinTech variables on cybersecurity: Evidence form Iraqi Banks. International Journal of Research in Business and Social Science,No. 9, 2020, pp.23–133.

[23] Amnesty International, Iraq: Call to withdraw the draft Cybercrime Law which would severely undermine fundamental right to freedom of expression, Amnesty International Index: MDE 14/9944/2019, London: Amnesty International,2019,p.3..

ملف العدد
الأمن السيبراني
درع التحول الرقمي العراقي
(بين التحديات الراهنة وضرورات المستقبل)

الأمن السيبراني وإدارة المخاطر
العراق انموذجا

م.د. زمن ماجد عودة
الجامعة المستنصرية/ مركز المستنصرية
للدراسات العربية والدولية
Zaman23@uomustansiriyah.edu.iq

ثمة علاقة ترابطية وثيقة ما بين تزايد حالات الهجمات والتهديدات السيبرانية بأنواعها كافة في العراق، وما بين زعزعة الأمن القومي للبلد. إذ كلما زادت الهجمات كلما تزعزع الأمن، وكلما قلت الهجمات كلما بت الاستقرار في البلاد، ومن هنا جاء دور المؤسسات الأمنية بالتعاون مع المؤسسات التعليمية بضرورة الاهتمام بالأمن السيبراني وبناء قدرات أمنية سيبرانية قادرة على إدارة المخاطر والتهديدات، و وضع حد لتزايد الهجمات والجرائم الالكترونية التي كادت تفتك بأمن الأفراد والمجتمع و مؤسسات و وزارات الدولة كافة.

الكلمات المفتاحية: الأمن، القوة السيبرانية، التهديدات السيبرانية، الإدارة، المخاطر، العراق.

Cybersecurity and Risk Management: Iraq as a Model

Dr.Zaman Majed Auda
Al-Mustansiriyah Center for Arabic and International
Studies / Al-Mustansiriyah University

is a close correlation between the increasing incidence of cyber attacks and threats of all kinds in Iraq, and the destabilization of the country's national security. The more attacks, the more security is destabilized, and the fewer attacks, the more stable the country will be. Hence the role of security institutions, in cooperation with educational institutions, of the need to pay attention to cybersecurity, build cybersecurity capabilities capable of managing risks and threats, and put an end to the increase in attacks and cybercrimes that almost killed the security of individuals, society, institutions and ministries of the state.

Keywords: Security, Cyber Force, Cyber Threats, Management, Risk, Iraq.

الاستلام 2024/04/04
الارجاع 2024/05/12
القبول 2024/06/13

المقدمة

بعد التطورات التكنولوجية المتسارعة التي شهدها العالم في النصف الثاني من القرن الحادي والعشرين ولاسيما في المجال الأمني والعسكري، ولعدم وجود قواعد ولوائح قانونية دولية تحدد من يمكن له استعمال تلك التكنولوجية من جهة، ولحيازة جهات فاعلة من غير الدول متمثلة بـالجماعات الارهابية و الحركات المتطرفة والحركات الانفصالية للوسائل والأسلحة الذكية من جهة اخرى، الأمر الذي يهدد الامن الداخلي للدول ويجعله معرض للخطر بشكل مستمر.

لذا لابد للدول ولاسيما العراق(بسبب ما يعانيه من ضعف أمني واختراقات متكررة) التوجه نحو انشاء منظومة أمنية سيبرانية تعمل على تحصين دفاعاته الالكترونية والحفاظ على البيانات والمعلومات الاستخباراتية الأمنية من القرصنة والسرقة وغيرها من عمليات الاحتيال والتزوير والانتحال والابتزاز الالكتروني.

إشكالية البحث:

يعالج البحث المشكلة الآتية:" في ظل تزايد مخاطر الجرائم السيبرانية من حيث الكم والنوع، لابد للمؤسسات الأمنية العراقية اتخاذ إجراءات فاعلة لبناء منظومة أمنية سيبرانية لديها القدرة والامكانية الكافية لإدارة المخاطر و الحد منها لمنع تفاقمها في المستقبل القريب ".

فرضية البحث :

ينطلق البحث من فرضية مفادها:" أن الأمن السيبراني ضرورة اساسية من ضروريات إدارة المخاطر والتهديدات الأمنية والمجتمعية والاقتصادية في العراق، ولاسيما بعد ان اصبحت الوسائل السيبرانية والأسلحة الذكية ووسائل التواصل الاجتماعي متاحة للأفراد والفواعل المسلحة من غير الدول وشبكات الجريمة المنظمة وغير المنظمة تستعملها لتحقيق مآربها بعيداً عن القانون ".

هيكلية البحث :

تم تقسيم البحث إلى محوريين اساسيين للتحقق من صحة الفرضية. وهما الآتي: -

المحور الأول: الأمن السيبراني في العراق "مدخل مفاهيمي تحليلي".

المحور الثاني: السيبرانية وإدارة المخاطر في العراق.

المحور الأول: الأمن السيبراني في العراق "مدخل مفاهيمي تحليلي".

شهد العالم منذ نهاية عقد القرن العشرين تطورا تكنولوجيا ملحوظا في مجال وسائل المواصلات والاتصالات وتكنولوجيا المعلوماتية الرقمية، ويعد هذا التطور نتيجة حتمية لما يمر به العالم اجمع من تطورات متسارعة في الجوانب كافة. ونلاحظ أن الدول بدأت بمواكبة هذه التطورات ولاسيما التحول نحو العالم الرقمي والعمل على تنمية البنية التحتية الرقمية، تماشياً مع تنامي قدرات المعالجة الحاسوبية وقدرات تخزين البيانات، ومن ثم القدرة والاستعداد للتعامل مع تطور تطبيقات الذكاء الاصطناعي والنانو تكنولوجي وغيرها من تحولات الثورة الرقمية[1].

كما نلاحظ ان التغييرات في القوة السيبرانية عدت حدثا مهماً في بيئة العلاقات الدولية لما لها من انعكاس على السياسات الخارجية للدول أطراف التفاعل، لاسيما في ظل اعتماد أغلب الدول على القاعدة المادية المعلوماتية[2]. ولو اتينا إلى القوة السيبرانية لرأينا أن استاذ العلوم السياسية الامريكي جوزيف ناي أوضح أن القوة السيبرانية هي نوع جديد غير تقليدي اضيف إلى انواع القوة التقليدية السابقة، وعرفها بأنها هي "القدرة على الحصول على النتائج المرجوة من خلال استعمال مصادر المعلومات المرتبطة بالفضاء السيبراني، أي أنها القدرة على استعمال الفضاء السيبراني لخلق المزايا، والتأثير في الأحداث المتعلقة بالبيئات الواقعية الأخرى، وذلك عبر الادوات الإلكترونية"[3]. كما يرى جوزيف ناي أن القوة السيبرانية تتضمن مجموعة الموارد المتعلقة بالتحكم والسيطرة على أجهزة الحاسبات والمعلومات والشبكات والبنية التحتية المعلوماتية والمهارات البشرية المدربة للتعامل مع هذه الوسائل. تعمل على تغطية كل القضايا التي تتعلق بالتفاعلات الدولية، سواءً كانت عسكرية أو اقتصادية أو سياسية أو ثقافية أو اعلامية، وهي بذلك لا تشمل الحرب السيبرانية فحسب التي تقتصر على الجانب العسكري دون غيره من الجوانب الأخرى [4].

وفق ما يرى جوزيف ناي أن القوة السيبرانية تكمن في ثلاثة فواعل تتضح في الشكل أدناه:

الشكل رقم (1)

يوضح الفواعل المتحكمة بالقوة السيبرانية

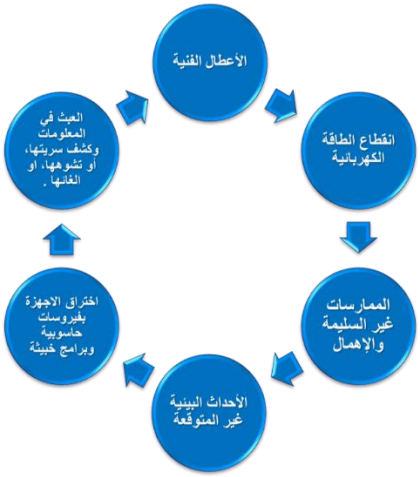
الشكل من إعداد الباحث بالاعتماد على: للمزيد ينظر: ايهاب خليفة، الحروب السيبرانية الاستعداد لقيادة المعارك العسكرية في الميدان الخامس،المستقبل للابحاث والدراسات المتقدمة،العربي للنشر والتوزيع،القاهرة،2021،ص67. كذلك ينظر:فارس محمد العمارات ابراهيم محمد الحمامصة،الأمن السيبراني المفهوم وتحديات العصر، دار الخليج للنشر والتوزيع،عمان، 2022،ص26-27.

شهد النظام الدولي منذ تسعينيات القرن الماضي بروز التهديدات الامتثالية العابرة للحدود القومية، مما أدى إلى حدوث تحولات في حقل الدراسات الأمنية والاستراتيجية والممارسة السياسية[5]. ولاسيما بعد دخول المجال الالكتروني ضمن المحددات الجديدة لمؤشرات القوة وأبعادها الجديدة من حيث طبيعتها وأنماط استخدامها، وطبيعة الفواعل فيها من جهة، وتحول الفضاء الالكتروني الى ساحة للتفاعلات الدولية لتكون بذلك السيبرانية أحد أوجه الصراعات الجديدة من بوابة امتلاك التكنلوجيا المعلوماتية من جهة اخرى، الأمر الذي كان له انعكاس على قدرات الدول وعلى تحديد طبيعة علاقاتها الدولية وسياستها الخارجية[6].

نتعرض أرصدة الفضاء السيبراني إلى عدة تهديدات و مخاطر تقف عائق أمام امكانية أطلاقها وضمان سلامة المعلومات فيها وخصوصيتها، ترجع أسباب ظهور هذه المخاطر إلى حوادث غير مقصودة تتمثل في :

الشكل رقم (2)

تهديدات أرصدة الفضاء السيبراني



الشكل من إعداد الباحث، بالاعتماد على مازن حميد شلال البكري وآخرون، الأمن في النظام الدولي مابين القوة التقليدية والقوة الجديدة،تقديم عبد الامير رشيد يار الله، دار الكلمة للطباعة والنشر والتوزيع، بغداد،2022،ص223.

لتجنب التهديدات أعلاه ولضمان حماية الأرصدة الفضاء السيبراني. يتطلب الآتي :-

الشكل رقم (3)

متطلبات حماية أرصدة الفضاء السيبراني

الشكل من إعداد الباحث.

استناداً إلى :مازن حميد شلال البكري وآخرون، الأمن في النظام الدولي مابين القوة التقليدية والقوة الجديدة،تقديم عبد الامير رشيد يار الله، دار الكلمة للطباعة والنشر والتوزيع، بغداد،2022،ص223.

ومن ثم عدت وظيفة التأمين من التهديدات السيبرانية من أكثر الوظائف صعوبة لاسيما بعد انتشار أجهزة انترنت الأشياء وأجهزة الاستشعارات بصورة كبيرة، داخل المؤسسات والشركات والمنازل والمطاعم والمقاهي. أي وجود مليارات الأجهزة ضعيفة التأمين سهلة الاختراق منتشرة في كل الأماكن، وجميعها متصل بالأنترنت، فإذا تم اختراق هذه الأجهزة والسيطرة عليها، وحقنها بالفيروسات والديدان وأحصنة طروادة، فإنها ستتحول مباشرة إلى جيش مسلح قادر على تدمير البنية التحتية للبنوك وتعطيل الخدمات المالية والمصرفية، وتدمير محطات الطاقة والسدود والمستشفيات وقطاع الاتصالات، أي تعطيل وشل حركة الخدمات الحكومية جميعها، مما يؤدي إلى التنبؤ بحدوث الحرب السيبرانية في أي وقت[7].

من هنا يأتي دور الأمن السيبراني كعنصر أساسي ومطلب ضروريا لكل الدول دون استثناء، للحماية من المخاطر والتهديدات المحتملة عن طريق مصادر خارجية من خلال الإنترنت[8]، والأمن السيبراني هو أمن الشبكات والأنظمة المعلوماتية والاجهزة المتصلة بالأنترنت والبيانات والمعلومات بمعنى اخر هو المجال الذي يتعلق بمعايير الحماية التي يجب اتباعها لمواجهة التهديدات أو الحد من أثارها. وهي الاجراءات التي يتم اتخاذها من قبل الدول، أو بعض المنظمات الحكومية او غير الحكومية للمحافظة على سرية المعلومات الالكترونية، من الاختراق والقرصنة والسرقة ومنع وصولها إلى الجهات المعادية، ولاسيما في الوقت الحاضر الذي أصبحت فيه الثورة المعلوماتية وانتشار الاتصالات على نطاق واسع من العالم الأمر الذي جعل منها هاجساً استراتيجياً لأغلب دول العالم[9].

عرف ريتشارد كمرر الأمن السيبراني بأنه : "عبارة عن وسائل دفاعية من شأنها كشف واحباط المحاولات التي يقوم بها القراصنة" [10]. بينما جاء في تقرير الاتحاد الدولي للاتصالات لعام (٢٠١٠- ٢٠١١) بأنّه "مجموعة من المهمات مثل تجميع وسائل وسياسات واجراءات أمنية ومبادئ توجيهية ومقاربات لإدارة المخاطر وتدريبات و ممارسات فضلى وتقنيات يمكن استعمالها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين ". أما إدوارد أمورس عرف الأمن السيبراني هو : "وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو

أجهزة الحاسوب أو الشبكات وتشمل تلك الوسائل الأدوات المستعملة في مواجهة القرصنة وكشف الفيروسات ووقفها وتوفير الاتصالات المشفرة ". كما نرى أن وزارة الدفاع الأمريكية "البنتاغون" وضعت تعريفاً دقيقاً للأمن السيبراني: "يعد جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والالكترونية من مختلف الجرائم وهجمات التخريب والتجسس والحوادث"[11]. كما يرى المعهد الوطني للمعايير والتقنية في الولايات المتحدة أن الأمن السيبراني هو "النشاط أو العملية أو القدرة أو الإمكانية أو الحالة التي يتم بموجبها حماية نظم المعلومات والاتصالات والمعلومات الواردة اليها والدفاع عنها ضد الضرر أو الاستخدام أو التعديل غير المصرح به أو الاستغلال"[12]

ويتمثل الأمن السيبراني في مجموعة من الآليات والإجراءات والوسائل والأطر التي تهدف إلى حماية البرمجيات وأجهزة الكمبيوتر والفضاء السيبراني بصفة عامة من مختلف الهجمات الاختراقات التهديدات السيبرانية التي قد تهدد الأمن القومي للدول. ويعد سلاح استراتيجي بيد الحكومات والإفراد لا سيما أن الحرب السيبرانية أصبحت جزءاً لا يتجزأ من التكتيكات الحديثة للحروب والهجمات بين الدول[13].

يهدف الأمن السيبراني إلى تحقيق مجموعة من الاهداف متمثلة بالآتي[14]:-

1. **الخصوصية:** توفير الحماية الفائقة لخصوصية المعلومات والإبقاء على سريتها، وذلك بعدم السماح لغير المخولين بالوصول إليها واستعمالها.
2. **الحفاظ:** الحفاظ على المعلومات وسلامتها وتجانسها، وذلك بكف الأيادي من العبث بها، وتحقيق وفرة البيانات وجاهزيتها عند الحاجة إليها.
3. **الحماية:** حماية الأجهزة والشبكات ككل من الاختراقات لتكون درع واق للبيانات والمعلومات استكشاف نقاط الضعف والثغرات في الأنظمة ومعالجتها.
4. **التطوير:** استعمال الأدوات الخاصة بالمصادر المفتوحة وتطويرها لتحقيق مبادئ الأمن السيبراني عن طريق توفير بيئة عمل آمنة عن طريق العمل عبر الشبكة العنكبوتية.

فضلاً عن ذلك، أن الهدف الأسمى للأمن السيبراني هو القدرة على مقاومة التهديدات المتعمدة وغير المتعمدة والاستجابة والتعافي، و التحرر من الخطر أو الأضرار الناجمة عن تعطيل أو اتلاف تكنولوجيا المعلومات والاتصالات[15].

يعتمد الأمن السيبراني على عدد من الركائز لمواجهة التهديدات السيبرانية وهي موضحة في الشكل رقم (4).

شكل رقم (5)

ركائز الأمن السيبراني في مواجهة التهديدات

الشكل من إعداد الباحث. استنادا إلى: مازن حميد شلال البكري وآخرون، الأمن في النظام الدولي مابين القوة التقليدية والقوة الجديدة،تقديم عبد الامير رشيد يار الله، دار الكلمة للطباعة والنشر والتوزيع، بغداد،2022،ص239 - ص241.

نلاحظ أن الأمن السيبراني يستفيد بشكل كبير من تقنيات الذكاء الاصطناعي، في مجال تحسين الأداء الأمني العام في الأماكن التي يمكن أن تكون فيها أنظمة الأمان التقليدية بطيئة وغير كافية، لغرض الحماية من التهديدات السيبرانية المعقدة والمتزايدة[16].

نستخلص مما تقدم :أن التطورات التكنولوجية الحديثة أدت إلى تغييرات في اشكال القوة والتحول نحو القوة غير التقليدية السيبرانية، وبروز تهديدات جديدة سيبرانية على الساحة العالمية. ومن ثم ظهور نوع جديد من انواع الأمن وهو **الأمن السيبراني**.كما موضح في الشكل رقم (5).

شكل رقم (5)

التحولات المعاصرة في مفهوم الأمن وبزوغ الأمن السيبراني

الشكل من إعداد الباحث.

الأمن السيبراني في العراق.

يُعدُ الأمن السيبراني الركيزة الرئيسة في مجال تطوير وصيانة البنية التحتية لتكنولوجيا المعلومات في أي بلد من بلدان العالم ولاسيما العراق، لذا تولدت ضرورة ملحة لتعزيز إطار شامل للأمن السيبراني، والعمل على إعادة تنظيم البنية التحتية الصناعية والأمنية بأكملها بمساعدة التكنولوجيا المتقدمة من اجل التوصل إلى سياسة متكاملة للأمن السيبراني قادرة على التعامل مع التهديدات الداخلية والخارجية كافة في العراق[17]، هناك عدة معايير يقاس على اساسها مستوى الأمن السيبراني في كل بلد. كما موضحة في الشكل رقم (6).

شكل رقم (6)

معايير قياس مستوى الأمن السيبراني للدولة

الشكل من اعداد الباحث.استنادا إلى : باسم علي خريسان، الأمن السيبراني في العراق: قراءة في مؤشر الأمن السيبراني العالمي 2020،مركز البيان للدراسات والتخطيط،بغداد،2021 ص9.

وفق المعايير اعلاه شغل العراق في المؤشر العالمي عام 2020 المركز 129عالمياً من اصل 184 دولة، والمركز 17 عربياً بدرجة 71,20%[18].

من هنا اتخذت الحكومات العراقية عدة إجراءات لزيادة الاهتمام بالأمن السيبراني. نلاحظ من هذه الاجراءات هي الآتي: -

اولاً: تأسيس فريق الاستجابة لحوادث الأمن السيبراني في عام ٢٠١٧

يمثل الفريق سلطة موثوقة تعزز من قدرة العراق على الاستجابة للحوادث. اذ يتولى مسؤولية إدارة ومراقبة العملية السيبرانية لجميع مؤسسات القطاع الحكومي والاستجابة لها. يضم الفريق "المركز الوطني للأمن السيبراني" والذي تقع على عاتقه مهمة مراقبة نشاط الجهات الحكومية وشبه الحكومية، ووكالات وقطاعات عدة منها القطاعات المالية والصناعية والنقل والصحة والشؤون القانونية. و الاستجابة للحوادث السيبرانية من خلال الرصد المبكر، وحماية المؤسسات عن طريق تحليل التهديدات السيبرانية المعروفة بشكل استباقي ومنع تكرارها من خلال التحليل السيبراني للمسببات الجذرية لحدوثها[19].

الشكل رقم (7)

مهام فريق الاستجابة لحوادث الأمن السيبراني

الشكل من إعداد الباحث استنادا إلى : فريق الاستجابة لحوادث الأمن السيبراني، 2024. https://cert.gov.iq/cert/sample-page2024

الخدمات التي يقدمها فريق الاستجابة لحوادث الأمن السيبراني في العراق تكمن في الآتي[20]:-

1. **الاستشارات الأمنية:** يقدم الفريق المشورة والمساعدة الأمنية من خلال استقباله المشاكل الفنية والأمنية كافة على البريد الالكتروني (info@cert.gov.iq).
2. **اختبار اختراق الشبكة الداخلية :**قيام الفريق بتطوير الاجراءات الدفاعية الفاعلة وتطبيق أسلوب تفكير استراتيجي للتحري عن عمليات القرصنة والاختراق على المستويات كافة.
3. **تدقيق أمن تطبيقات الويب :**تحديد نقاط الضعف القابلة للاستغلال في التطبيقات قبل أن يتمكن المتسللون من اكتشافها واستغلالها.
4. **التدقيق الأمني لتطبيقات الهاتف المحمول** : إجراء اختبار الاختراق ومراجعة التعليمات البرمجية على جميع الأنظمة الأساسية لتطبيقات الهاتف المحمول، وانشاء بيئة اختبار مخصصة ومجهزة بالكامل في تطبيقاتAndroid ، .iOS.
5. **الطب الشرعي والتحقيقات** :القيام بتحديد التهديدات القادمة من الداخل، للكشف عن ما سرقه المخترق للنظام، وإجراء تحقيق كامل في دفاع الأمن السيبراني لتحديد حجم الخسائر،وتوفير تحقيقات الطب الشرعي المتعمقة واليدوية والآلية التي يقوم بها مختبرو ومحققو الاختراق ذوو الخبرة.
6. **تدقيق أمنWIFI** :تعمل الشبكات اللاسلكية على توسيع البيئة الداخلية لتشمل المهاجمين الخارجيين المحتملين ضمن النطاق. كما تقوم اختبارات الاختراق اللاسلكي بتقييم مدى كفاية ضوابط الأمان المتعددة المصممة لحماية الوصول غير المصرح به إلى الخدمات اللاسلكية.
7. **التدريب على المؤسسات** :القيام بعدد من الدورات التدريبية الأمنية في مجال اختبار الاختراق، وأمن المعلومات.

ثانيا: إنشاء قاعدة واسعة من مسودات التشريعات السيبرانية

تم وضعها من قبل مختلف المؤسسات الحكومية ذات العلاقة، واللجنة العليا للحوكمة الالكترونية، والتي تتعلق بالجرائم السيبرانية وحماية البيانات ذات الطابع الشخصي، على سبيل المثال قانون الجرائم المعلوماتية، قانون الاتصالات والمعلوماتية، وقانون حماية الخصوصية، واقرار قانون التوقيع الالكتروني والمعاملات الالكترونية. وتم وضع مسودة وثيقة "سياسات ومعايير أمن المعلومات ومشاركة البيانات" في عام ٢٠١٩، لغرض تحديد قواعد السلوك

اللازمة لتوفير الحد الادنى من ضوابط الأمن السيبراني بناءاً على المعايير العالمية والتوصيات الدولية التي تم اقرارها بموجب قرار الأمن الوطني[21].

ثالثا-تطوير استراتيجية للأمن السيبراني في العراق

في هذا الصدد أنعقد في العاصمة العراقية بغداد عام٢٠١٩ مؤتمر العراق" **الإلكتروني والأمن السيبراني**" بالتعاون مع المجلس الدولي للاستشارة الالكترونية (EC-Council) التابع لمفوضية الاتحاد الأوربي وهو مجلس معني بمتابعة قضايا الأمن السيبراني وله ادوار عالمية في هذا المجال، وكان الهدف من المؤتمر تحديث وابتكار عمليات الأمن السيبراني الاستراتيجية والتكتيكية للحكومة العراقية، ومستقبل الحكومة الالكترونية، والتهديدات السيبرانية التي قد يتعرض لها العراق وسبل الدفاع عنها، وزيادة الوعي لمنع الجريمة السيبرانية في العراق، فضلا عن حماية البيانات والتعامل مع الحوادث واستعادة القدرة السيبرانية على العمل بعد الحوادث، ودور (EC-Council) في تقديم الدعم للعراق، ويأتي هذا المؤتمر في سياق خطط الحكومة العراقية للاستثمار في الحكومة الالكترونية وتعزيز الأمن السيبراني العراقي[22]. كما أقر مجلس الوزراء في عام ٢٠٢٠ وثيقة "الإستراتيجية الوطنية لأمن البنى التحتية الحرجة الحساسة"، بتعريف البنى التحتية الحساسة والمخاطر والتهديدات وآليات إدارة المخاطر والمراقبة [23]. انطلاقاً من أهمية الأمن السيبراني، وجهت رئاسة الوزراء من خلال مجلس الأمن الوطني بتشكيل فريق وطني مشترك بعضوية الجهات والمؤسسات ذات العلاقة وهي كل من مجلس النواب، مجلس القضاء الاعلى، وزارة الدفاع، وزارة الداخلية، وزراة العدل، وزارة الاتصالات، وزارة التعليم العالي والبحث العلمي، وزارة الكهرباء، وزارة النفط، جهاز المخابرات الوطني العراقي، جهاز الأمن الوطني، جهاز مكافحة الارهاب، هيأة الحشد الشعبي، هيأة الاعلام والاتصالات، فريق الاستجابة لحوادث الأمن السيبراني، مستشار مدير مكتب رئيس مجلس الوزراء، الشركات الاهلية لغرض وضع إستراتيجية العراق في مجال الأمن السيبراني وبالتعاون مع المختصين الدوليين من منظمة أسكوا، للمدة من عام 2022 - 2025 لرفع مستوى الأداء وتذليل التحديات وتقليل المخاطر المتعلقة بالأمن السيبراني على المستوى الوطني والإقليمي والدولي[24].

رابعا: دور وزارة التعليم العالي والبحث العلمي

أعلنت وزارة التعليم العالي والبحث العلمي العراقية في عام 2022 ولأول مرة عن استحداث ثلاثة أقسام متخصصة في دراسة الأمن السيبراني في ثلاث جامعات (الجامعة المستنصرية، الجامعة التقنية الشمالية، وجامعة الموصل). وافتتاح أكاديمية لشركة أمازون AWS المتخصصة بالحوسبة السحابية في أربع جامعات وأكاديمية أخرى لشركة EC Council المتخصصة في الأمن السيبراني في (الجامعة التكنولوجية، الجامعة التقنية الشمالية) لغرض تسهيل دراسة الأمن الرقمي وتطوير الخبرات المحلية ومن ثم لدعم الجهود الوطنية لحماية الفضاء السيبراني في العراق [25].

المحور الثاني: السيبرانية وإدارة المخاطر في العراق.

هناك علاقة وثيقة ما بين الأمن السيبراني وإدارة المخاطر والتهديدات السيبرانية في العراق، تكمن الإدارة في سياق الأمن السيبراني في كيفية إدارة أمن المعلومات وتحليل مستوى جاهزية منظومة الأمن من حيث التكامل الاستراتيجي، وتوسيع استراتيجية الأمن السيبراني، وكيفية إدارة المخاطر ومواجهة الهجمات الإلكترونية والعمل على التقليل منها قدر الإمكان[26].

وعلى الرغم من ضعف الامكانيات السيبرانية في العراق، إلا اننا نلاحظ أن الأمن السيبراني تمكن من إدارة عدد من المخاطر. وهي الآتي :-

اولاً: الحد من الجرائم الالكترونية

للأمن السيبراني دوراً مهماً في حماية وضمان أمن الفضاء السيبراني العراقي، وحماية بنية معلوماته الحيوية وبناء مجتمع انترنت، والتعامل مع بعض التحديات السيبرانية التي تهدد أمن العراق الوطني وسلامته. فلو دققنا النظر للاحظنا أن عدد الجرائم السيبرانية بدا بالانتشار والتزايد منذ عام 2006 في العراق ؛ وذلك بسبب الانتشار السريع للخدمات والعمليات عبر الإنترنت والتي ارتفعت معها نسبة جرائم الإنترنت، وارتفاع نسب القرصنة السيبرانية والانشطة المضرة بالنظام والمجتمع العراقي[27]. فضلاً عن ذلك يرجع انتشار إلى إن قطاع الإنترنت في العراق غير منظم، ومن بين أكثر القطاعات حرية على مستوى العالم، مما جعله أكثر عرضة للخطر. كما نلاحظ أن البيانات المتعلقة بأنواع الجرائم الإلكترونية في العراق نادرة، ونادرا ما تنشرها الحكومة العراقية في هذا الجانب أوضحت وزارة التخطيط العراقية أن الغالبية العظمى

من الجرائم الإلكترونية تتم عبر منصات التواصل الاجتماعي، في المقام الأول على الفيسبوك، وضد الأشخاص أو الشركات أو الحكومات. تشمل الهجمات السيبرانية الأكثر شيوعا الاحتيال عبر الإنترنت، وسرقة الهوية، والمواد الإباحية عن الأطفال، والمطاردة السيبرانية، وانتهاك حقوق الطبع والنشر، وقرصنة الأقمار الصناعية، والإرهاب السيبراني. الغش الإنترنت، وغسيل الأموال والتجارة السيبرانية غير المشروعة، والاختطاف والتهديد واختراق المعلومات الشخصية والمخدرات والاحتيال والتطفل على الشبكات[28]. وجرائم الاحتيال والخداع الالكتروني عن طريق محاولة خداع العملاء بالكشف عن معلوماتهم الأمنية الشخصية مثلا أرقام بطاقات الائتمان الخاصة بهم أو تفاصيل الحساب المصرفي أو أي معلومات حساسة اخرى. وجريمة البريد الدعائي المزعج عن طريق القيام بارسال اعداد كبيرة من الرسائل الالكترونية لغرض تجاري وفرضها على الناس رغم عدم رغبتهم باستلامها. وجريمة الاختراق والقرصنة الإلكترونية عن طريق قيام مجموعة من الاشخاص أو شخص واحد إعادة انتاج أو نشر مواد محمية بحقوق الطبع والنشر بشكل غير قانوني مثلاً برامج الكمبيوتر والكتب والموسيقى والافلام بواسطة أجهزة الكومبيوتر الشخصية عبر شبكة الإنترنت[29].

ثانيا: رصد الشبكات الارهابية

للأمن السيبراني دور في إدارة المخاطر الأمنية واحباط العديد من العمليات الارهابية للحد من انتشار التنظيمات والشبكات الارهابية ففي عام 2014 تمكنت شركات امنية مختصة بالأمن السيبراني من مراقبة ورصد حركات تنظيم داعش الارهابي عن طريق الاقمار الاصطناعية واجهزة GPS، ومراقبة استعمالهم لمواقع التواصل الاجتماعي عند القيام بعمليات تجنيد المزيد من الارهابين والدعاية للتنظيم[30]. ونلاحظ استعمال الجماعات الإرهابية أحدث تقنيات تكنولوجية الرقمية للحصول على الدعم اللوجستي، واستعمال الأسلحة المتطورة الذكية الأمنية والعسكرية في اغلب الاعمال الارهابية لزعزعة الأمن القومي العراقي. هنا جاء دور محللي الأمن السيبراني في رصد تحركات تنظيم داعش الارهابي بشن هجمات عبر الإنترنت، ومعرفة أماكن تواجدهم والعمل على اختراق منظومتهم الأمنية وتفكيكها للقضاء تدريجياً على التنظيم[31].

ثالثا: إدارة مخاطر الابتزاز الالكتروني

أدى الانتشار الواسع لوسائل التواصل الاجتماعي في العراق في الاعوام الأخيرة إلى ارتفاع نسب الابتزاز الإلكتروني وفق ما ذكرت الشرطة المجتمعية ارتفعت حالات الابتزاز من ١٠ الى٢٠ حالة يومياً خلال عام ٢٠٢١ عن طريق قيام اشخاص بشكل منفرد أو مجموعة على شكل شبكات من نشر الصور ومقاطع الفيديو أو وثائق لابتزاز الضحية[32] . تتمثل أنواع الفئات المعرضة للابتزاز الالكتروني. في الآتي[33]:

النوع الأول: يوجه ضد الأشخاص والمستخدمين بشكل شخصي (الشباب، النساء)، من خلال أنماط وصور مختلفة.

النوع الثاني :يستهدف مسؤولين كبار في الدولة، أو أصحاب الشركات ومنظمات الأعمال بشكل ممنهج، عبر تبني هجمات تستهدف أجهزة وخوادم حكومية حيوية، عن طريق تسريب المعلومات والبيانات،مقابل الحصول على مبالغ مالية أو لغرض التسقيط.

كما بلغ عدد الحاسبات الالكترونية المسربة 116،398, ١٧ مليون حساب في العراق وهذا مؤشر خطير يدل على ضعف إمكانيات الأمن السيبراني في العراق وعدم توفر عناصر حماية البيانات في المواقع الالكترونية [34]. وللحد من جريمة الابتزاز الالكترونية عمل فريق الأمن السيبراني في العراق باستعمال أحدث التقنيات الحديثة لرصد أصحاب المواقع الوهمية، وانشاء وزارة الداخلية ضمن مديرية مكافحة الجريمة المنظمة قسم التقنيات في وكالة الاستخبارات ومراكز الشرطة ووضع خطوط ساخنة لاستقبال الشكاوى في هذه المجال بالتعاون مع الشرطة المجتمعية وجهاز الأمن الوطني، ووكالة الاستخبارات والتحقيقات الاتحادية، ومديرية الجرائم الالكترونية.

رابعا: منع مضايقة وابتزاز عملاء المصارف

في الآونة الاخيرة تحولت أغلب التعاملات المالية والمصرفية في العراق إلى تعاملات الالكترونية رقمية عبر بطاقات الخصم والائتمان والدفع الالكتروني. اذ يواجه العملاء مضايقات وتهديدات بدرجة طفيفة أثناء القيام بالخدمات المصرفية عبر الكمبيوتر الشخصي أو الهاتف المحمول .كما كان هناك في بعض الأحيان تهديد بتحويل أموال عبر حساب مصرفي أو بطاقة ائتمان أو تسوية مسألة ابتزاز إلكتروني. من هنا بذلت البنوك العراقية قصارى جهدها

لتحديث و بناء أنظمة أمن سيبراني خاصة بها،لتتولى مهمة لحماية بيانات اعتماد عملائها وخوادم النظام الداخلي من الاختراق، وتحقيق خصوصية المستخدم [35].

خامسا : ضمان أمن المعلومات والبيانات من الاختراق

للأمن السيبراني دور في الحفاظ على سرية المعلومات ودقتها، و تحديد المعلومات والبيانات المفيدة وتميزها عن غير المفيدة. وكيفية جمع كميات كبيرة من المعلومات غير المتجانسة والتعامل معها، وتقييم وحماية خصوصية الأجزاء الحساسة من المعلومات، الحفاظ على خصوصية تبادل المعلومات الشخصية والسياقية بين سياقات مستقلة ومختلفة. وضمان عدم تغيير البيانات أو إتلافها بواسطة مستخدمين ضارين أو أخطاء في النظام. أي الحفاظ على صحة المعلومات الموجودة في النظام، و وضع الاعتبارات المطلوبة لأنظمة الكترونية آمنة [36] نلاحظ أن سهولة اختراق بيانات ومعلومات في اغلب المواقع الالكترونية الرسمية للوزارات والمؤسسات الحكومية العراقية دليل على ضعف العلاقة أو ربما انعدامها بين وزارة الاتصالات والوزارات الأخرى، وعدم التعاون فيما بينهم مما يجعل الفضاء السيبراني للعراق أكثر عرضة للخطر[37] .وفي هذا المجال اقترحت الحكومة العراقية العمل على تشريع قانون يعاقب كل من يقوم باختراق البيانات ومحو وتغيير المعلومات ولاسيما المعلومات الأمنية التي تمس الأمن القومي للبلد بعقوبة السجن لمدة تتراوح بين سبع وعشر سنوات وغرامة من 5 ملايين إلى 10 ملايين دينار[38].

سادس : حماية خصوصية مستخدمي الموقع

يعمل الأمن السيبراني على ضمان حماية خصوصية معلومات المستخدمين للموقع عن طريق أجهزة الكمبيوتر والهواتف الذكية والأجهزة اللوحية والساعات الذكية. ويوفر للمستخدمين خدمات اضافية ذات قيمة كـ (خدمات الشبكات الاجتماعية، وأنظمة الملاحة، وانظمة السيارات، وأنظمة التوصية). أن حماية كميات كبيرة من المعلومات غير المتجانسة المتعلقة بموقع المستخدمين عملية معقدة تتطلب آلية تلقائية لمعالجتها. تعد سياسات الموقع طريقة واعدة لتحقيق الحماية في الوقت الفعلي وبشكل ديناميكي. تمنح سياسات الموقع للمستخدمين عدة مميزات منها الآتي[39]:-

1. إخفاء الموقع عن طريق إنشاء موقع وهمي واحد أو أكثر لمستخدم معين. لضمان عدم قدرة المستخدمون الآخرون تمييز الموقع الحقيقي للهدف.
2. إخفاء الموقع عندما لا يريد نشره للآخرين. لعدم معرفة موضع الهدف.
3. تحديد الحد الأقصى من الدقة للموقع اعتماداً على البيئة التي يتواجد فيها المستخدمون، يمكن تحديد مستويات متعددة من التفصيل مثل البلد والمدينة والمبنى والطابق. أو تحديد الحد الأدنى لمستوى القرب الذي يريد المستخدمون التواجد فيه.

الخاتمة :

على الرغم من ضعف القدرات الأمنية السيبرانية في العراق، وعدم وجود فرق عديدة متدربة بشكل كامل في هذا المجال، غياب وضعف القوانين والتشريعيات في الجانب المعلوماتي السيبراني، ومعارضة البعض من منظمات المجتمع المدني والمنظمات الاعلام والصحافة لتشريع قانون لتجريم الجرائم الالكترونية ظناً منهم أن تشريع مثل تلك القوانين يعد مهدد لحرية التعبير عن الرأي. قلة الوعي بأهمية تشريع مثل هكذا قوانين تعمل على حماية الافراد والشركات والمنظمات والمؤسسات الحكومية الرسمية وغير الرسمية من عمليات النصب والابتزاز والانتحال والاختراق لأمن المعلومات والبيانات والحسابات المالية والمصرفية والتي من الممكن أن تهدد الأمن القومي للبلد.

إضافة إلى استعمال الشبكات الارهابية وشبكات تجارة المخدرات والاتجار بالبشر الوسائل التقنية الحديثة لتحقيق اهدافهم وضرب المواقع الحيوية في الدولة بأقل التكاليف وبأقصى سرعة والتي بدورها تزعزع أمن البلد.

إلا أن العراق تمكن من إدارة العديد من المخاطر والتهديدات الأمنية السيبرانية باستعمال احدث التقنيات وشكل عدة فرق مختصة وتدريب الالاف خارج البلد، للاطلاع على تجارب وخبرات الدول الاخرى وكيفية تعاملهم مع مثل تلك المخاطر والعمل على مواجهتها والحد منها قدر الإمكان.

مع ذلك هناك عدة مقترحات لبناء منظومة أمنية سيبرانية قادرة على مواجهة التحديات الأمنية ولاسيما بعد انتشارها وارتفاع نسبها بشكل كبير في الآونة الاخيرة. وتتمثل المقترحات في الآتي :-

1- توفير الأجهزة الأمنية الذكية "أجهزة الرصد والمراقبة والتصوير، أجهزة التنصت، أجهزة التحليل الاستخباراتي، الاقمار الاصطناعية" والوسائل السيبرانية كافة للجهات الأمنية المختصة، والتدريب على كيفية استعمالها بالشكل الصحيح وبالوقت المناسب.
2- أرسال 1000 شخص للتدريب في كل عام إلى مختلف دول العالم للتدريب على الأمن السيبراني وتقنيات الذكاء الاصطناعي لغرض إعداد كوادر مهنية كفؤة متخصصة قادرة على مواجهة وإدارة الأزمات.
3- عقد اتفاقيات ومذكرات تفاهم مع الدول الأوروبية لغرض التعاون في المجال السيبراني والاستفادة من تجاربهم وتدريب كوادرنا الأمنية.
4- تعاون المؤسسات و الوزارات الأمنية مع المؤسسات التعليمية ومراكز الابحاث المتخصصة بالأمن السيبراني لتزويدهم بالبحوث العلمية في هذا المجال، وحث وزارة التعليم العالي والبحث العلمي على افتتاح اقسام وكليات متخصصة بالأمن السيبراني والذكاء الاصطناعي والنانو تكنولوجي في الجامعات العراقية.
5- تشريع قوانين تجرم الجرائم الالكترونية كافة وتفرض غرامات مالية وعقوبات صارمة على مرتكبيها.
6- استعمال وسائل التواصل الاجتماعي ووسائل الاعلام لنشر الثقافة السيبرانية وتوعية المواطنين بمخاطر تلك الجرائم ولاسيما الاطفال والنساء والشباب لغرض عدم استغلالهم من قبل ضعاف النفوس في تلك الوسائل.
7- إنشاء منظومة سيبرانية متخصصة لحماية المواقع الحيوية في الدولة " المنشآت العسكرية، والمنشآت النفطية وأنابيب نقل الطاقة، ومحطات الكهرباء والمياه، المطارات، والبنوك المالية وغيرها ".

المصادر والمراجع:

[1]فرح يحيى زعاترة، التهديدات السيبرانية على الأمن القومي الأمريكي، العربي للنشر والتوزيع، القاهرة،2023، ص11.
[2]فرح يحيى زعاترة، المصدر نفسه،ص48.
[3]ايهاب خليفة، الحروب السيبرانية الاستعداد لقيادة المعارك العسكرية في الميدان الخامس، المستقبل للأبحاث والدراسات المتقدمة، العربي للنشر والتوزيع، القاهرة،2021، ص66.
[4] ايهاب خليفة، المصدر نفسه،ص67.
[5] فارس محمد العمارات، ابراهيم محمد الحمامصة، مصدر سبق ذكره، ص20.

[6] مازن حميد شلال البكري وآخرون، مصدر سبق ذكره،ص221.
[7] ايهاب خليفة، الخوارزميات القاتلة العلاقات الدولية في عصر الذكاء الاصطناعي، ط1، العربي للنشر والتوزيع، القاهرة،2024، ص١٦٧.
[8] فارس محمد العمارات، ابراهيم محمد الحمامصة، مصدر سبق ذكره، ص20.
[9] منى الأشقر جبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية،2016، ص25.
[10] نقلا عن: محمد مختار، هل يمكن ان تتجنب الدول مخاطر الهجمات الالكترونية؟ مجلة اتجاهات الاحداث –ملحق العدد(6)،مركز المستقبل للابحاث والدراسات المتقدمة، يناير،2015،ص5.
[11] محمد محمود العمري، مدخل الى الامن السيبراني، دار زهران،عمان، 2020 ،ص18-ص19. للمزيد ينظر : لورنس م.اوليفا، امن تقنية المعلومات نصائح من خبراء، ترجمة محمد مراياتي،المنظمة العربية للترجمة،ط1، الرياض،2011.
[12] مصطفى ابراهيم سلمان الشمري،الأمن السيبراني وأثره في الأمن الوطني العراقي،مجلة العلوم القانونية والسياسية،المجلد (10)،العدد(1)،كلية القانون والعلوم السياسية، جامعة ديالى،2021،ص156.
[13] ، مازن حميد شلال البكري وآخرون، مصدر سبق ذكره، ص474،ص475.
[14] محمد محمود العمري،المصدر السابق،ص30.
[15] فارس محمد العمارات،ابراهيم محمد الحمامصة، مصدر سبق ذكره،ص19
[16] رانيا فوزي، تطبيقات الذكاء الاصطناعي في الحروب الافتراضية الاسرائيلية،ط1،العربي للنشر والتوزيع،القاهرة،2023،ص60.
[17] Khadija Hassan Shihan، Mustafa Jawad Radif, Internal and External Factors to Adopt a Cyber Security Strategy in Iraqi Organisations، Webology, Volume 19, Number 1, January, 2022،p5181.
[18] باسم علي خريسان،مصدر سبق ذكره، ص9.
[19] فريق الاستجابة لحوادث الأمن السيبراني، 2024. https://cert.gov.iq/cert/sample-page2024
[20] Cyber Security Services in Iraq ,2024. https://ctdefense.com/cyber-security-services-in-iraq
[21] استراتيجية الامن السيبراني العراقي 2022-2025، فريق الاستجابة للأحداث السيبرانية،ص14،ص15 .
[22] مصطفى ابراهيم سلمان الشمري،الأمن السيبراني وأثره في الأمن الوطني العراقي،مصدر سبق ذكره،ص174.
[23] استراتيجية الامن السيبراني العراقي 2022-2025،المصدر السابق،ص15.
[24] المصدر نفسه،ص4،ص8 .
[25] ماجد صدام سالم، الأمن السيبراني العراقي واثره في قوة الدولة،مجلة العلوم التربوية والانسانية،العدد (18)، كلية الامارات للعلوم التربوية،الامارات العربية المتحدة،2022، ص78.
[26] مصطفى ابراهيم سلمان الشمري،الأمن السيبراني وأثره في الأمن الوطني العراقي، مصدر سبق ذكره،159.
[27] مصطفى ابراهيم سلمان الشمري،المصدر نفسه،ص170.
[28] Haydar Jawad, Aro Omar, Cybercrime Legislation in Iraq, September 2017,p1. https://www.lexology.com
[29] مصطفى ابراهيم سلمان الشمري، الجرائم الإلكترونية وتأثيرها في العراق، وقائع المؤتمر العلمي الدولي التاسع، "العراق بعد عام ٢٠٠٣ الدولة،المجتمع ,الاقتصاد ,القانون، العلاقات الخارجية: التحديات والفرص"، مركز الدراسات الإقليمية جامعة الموصل، تحرير: لقمان عمر محمود النعيمي، دار نون للطباعة والنشر والتوزيع،٢٠٢١،ص122-ص123.
[30] مصطفى ابراهيم سلمان الشمري،الأمن السيبراني وأثره في الأمن الوطني العراقي،مصدر سبق ذكره،ص171-ص173.
[31] op.cit.p5185., Mustafa Jawad Radif، Khadija Hassan Shihan

[32] مصطفى ابراهيم سلمان الشمري، الجرائم الإلكترونية وتأثيرها في العراق، مصدر سبق ذكره،ص125-ص126.

[33]رشا عادل لطفي، جرائم الاتصال عبر الإنترنت وضبط أخلاقياته في ضوء الاتجاهات البحثية الحديثة (رؤية تحليلية ونقدية)، مجلة البحوث الإعلامية،العدد 58،ج2، كلية الاعلام، جامعة الأزهر،القاهرة،2021،ص567.

[34] مصطفى ابراهيم سلمان الشمري، الجرائم الإلكترونية وتأثيرها في العراق،مصدر سبق ذكره،ص127.

[35] Mohammed Faez Hasan, Noor Salah Al-Ramadan, Cyber-attacks and Cyber Security Readiness: Iraqi Private Banks Case, Social Science and Humanities Journal, Vol - 05, Issue - 08, 2021,p2316 -p2322.

[36] Maurizio Martellini ,Cyber Security Deterrence and IT Protection for Critical Infrastructures،Springer Briefs In Computer Science Springer،2013,p5-p8.

[37] Asmaa Khalid Jarjees Al-Tae, et al, Relationship of Cybersecurity and the National Security of the Country: Iraq Case Study, A multifaceted review journal in the field of pharmacy Systematic Reviews in Pharmacy Vol 11, Issue 12, Dec 2020,p473.

[38] Khadija Hassan Shihan، Mustafa Jawad Radif, op.cit.p5185- p5186.

[39] Maurizio Martellini, op.cit,p7.

ملف العدد
الأمن السيبراني
درع التحول الرقمي العراقي
(بين التحديات الراهنة وضرورات المستقبل)

الذكاء الاصطناعي
كآلية لتحقيق الأمن السيبراني العراقي

م.د. زيد احمد بيدر

مديرية تربية صلاح الدين

يهدف البحث الى تسليط الضوء على الذكاء الاصطناعي وامكانية استخدامه كآلية في تعزيز الامن السيبراني العراقي، اذ اصبحت كثير من الدول اليوم ومنها العراق امام تحدٍ كبيرٍ، نتيجة لاعتماد مؤسسات الدولة بشكل متزايد على التكنولوجيا في تسيير اعمالها ونظرا للترابط والاتصال بين هذه المؤسسات من خلال شبكة المعلومات، فان خطر الاختراق السيبراني سوف تكون نتائجه كبيرة على الدولة، مما جعل الدول تتجه نحو ادوات جديدة لتعزيز امنها السيبراني، والذكاء الاصطناعي يعد من بين ابرز هذه الادوات، وقد توصلت في البحث أنه بإمكان تقنيات الذكاء الاصطناعي تحقيق نتائج كبيرة في مجال تعزيز الامن السيبراني العراقي من خلال قدرتها في الكشف عن التهديدات فضلا عن قدرتها على التبوء ويتم ذلك بواسطة القيام بعملية مسح شامل للبيانات واجراء تنبؤات من خلال عمليات تدريب النظام على تلك الخطوات، مما يجعلها قادرة على التبوء بالهجمات واكتشاف مناطق الضعف التي يمكن استهدافها، وكذلك تستطيع تقنيات الذكاء الاصطناعي توفير القدرة على الاستجابة الفعالة للتهديدات بشكل آلي والقدرة على تطوير وسائل حماية جديدة لها.

الكلمات المفتاحية: الذكاء الاصطناعي، الامن السيبراني، الامن العراقي.

Artificial intelligence
as a mechanism for achieving Iraqi cybersecurity

Dr. Zaid Ahmed Bader

Salah al-Din Education Directorate

The study aims to shed light on artificial intelligence and the possibility of using it as a mechanism to enhance cybersecurity in Iraq, as many countries today, including Iraq, are facing a major challenge, as a result of state institutions' reliance on technology in conducting their work and due to the interconnection and communication between these institutions through the information network. The risk of cyber penetration will have great consequences for the country, which has made countries turn towards new tools to enhance their cyber security, and artificial intelligence is among the most prominent of these tools. The study found that artificial intelligence techniques can achieve great results in the field of enhancing Iraq's cyber security through its ability In detecting threats as well as its ability to predict, this is done by conducting a comprehensive data scanning process and

الاستلام	الارجاع	القبول
2024/04/04	2024/05/12	2024/06/13

making predictions through training the system on these steps, which makes it able to anticipate attacks and discover weak areas that can be targeted, and artificial intelligence techniques can also provide the ability to respond. Effective detection of threats automatically and the ability to develop new means of protection for them.

Keywords: artificial intelligence, Cyber security, Iraqi security.

المُقدمة

لم تعد تقنية الذكاء الاصطناعي تقتصر على جانب معين بل أتسع استخدامها ليشمل جميع المجالات، ويمكن اعتبار العقد الثاني من القرن العشرين اشبه بسباق بين الدول، لكن هذه المرة اختلف شكله ومضمونه عما كان يجري في السابق، وذلك لترابط الذكاء الاصطناعي بجميع المجالات سواءً كانت اقتصادية أو عسكرية أو اجتماعية، إذ تعد بمثابة مفتاح تطور العلوم الأخرى ومحاولة كل طرف الوصول الى درجة متقدمة تجعله في مقدمة الدول المتنافسة الأخرى، أو تكون قادرة على مواجهة التحديات والمخاطر القادمة من أي طرف آخر.

ونتيجة لاعتماد الدول بصورة كبيرة على التكنولوجيا في عمل مؤسساتها ونتيجة لترابط هذه المؤسسات في شبكة واحدة، أصبحت الهجمات السيبرانية التي تتعرض لها هذه المؤسسات لها آثار اقتصادية وأمنية واجتماعية كبيرة، مما أصبحت الدول والمؤسسات الدولية الكبرى تبحث عن وسائل متطورة لتعزيز أمنها السيبراني من خلال القدرة على مواجهة التهديدات السيبرانية، وظهرت تقنيات الذكاء الاصطناعي من بين الحلول التي حاولت الدول والمؤسسات تطويرها ودمجها بالأمن السيبراني، مما جعل الدول تدخل في سباق لمحاولة تطوير الذكاء الاصطناعي لدرجة يجعلها تمتلك ميزة تنافسية على الدول الاخرى.

أهمية البحث

يمكن إيجاز أهمية البحث بالنقاط الآتية:

1- توضيح أهمية وأهداف الذكاء الاصطناعي والأمن السيبراني.
2- بيان العلاقة بين الذكاء الاصطناعي والأمن السيبراني.
3- التعرف على الذكاء الاصطناعي ودوره في تعزيز الأمن السيبراني العراقي.

اشكالية البحث

تنطلق اشكالية البحث من السؤال الاساسي الآتي: هل تعد تقنيات الذكاء الاصطناعي من الأدوات الفعالة في تعزيز وحماية الأمن السيبراني العراقي.

فرضية البحث

ومن خلال الإجابة على التساؤل الأساسي، فإن فرضية البحث تذهب الى أن العراق قادر على تعزيز أمنه السيبراني من خلال توظيف الذكاء الاصطناعي بطريقة فعالة وامنة تمكنه بذلك من تحقيق الأمن السيبراني وحماية المعلومات والبيانات.

هيكلية البحث

وتضمنت هيكلية البحث محورين، الأول: تطريق للذكاء الاصطناعي والأمن السيبراني (العلاقة والاهداف)، في حين تضمن الثاني: دور الذكاء الاصطناعي في حماية الأمن السيبراني العراقي

المحور الأول: الذكاء الاصطناعي والأمن السيبراني (العلاقة والأهداف)

اولاً- علاقة الذكاء الاصطناعي بالأمن السيبراني

توجد مجموعة من النقاط التي تمثل حلقة اتصال بين الذكاء الاصطناعي والأمن السيبراني ، ومن أهم هذه النقاط هو التنبؤ، ويكون من خلال عمل الذكاء الاصطناعي على لعب دور يعد مكملا للأمن السيبراني بواسطة قدرته على القيام بتحليل المعلومات والوصول الى مصدرها وعددها مما يساعد على توفير الوقت والجهد على العاملين بهذا المجال، اذ يمكنه ذلك من كشف وإيقاف الهجمات السيبرانية بوقت قياسي ويساهم ايضًا في إظهار الأضرار التي تخلفها هذه الهجمات بالاعتماد على خاصية التنبؤ بعد حدوث الهجمات، وهذا ما ساهم بجعل الدول والشركات تدخل في سباق من أجل تطوير تقنيات الذكاء الاصطناعي والاستفادة منها في التنبؤ بحدوث الاختراق والتهيؤ لمواجهة هذه الهجمات قبل حدوثها، وتتيح لنا إضافة للوقت القدرة على اجراء مسح البيانات وتدريب النظام فضلًا عن تحديد أهم نقاط الضعف والعمل على تعزيز الأنظمة الدفاعية وجعلها قادرة على تحسين هذه الدفاعات بصورة مستمرة لمواجهة أي هجوم سيبراني في المستقبل[1].

اعتمدت الدول والشركات الكبرى في السابق على العنصر البشري بشكل أساسي في تعزيز الأمن السيبراني من خلال مواجهة التهديدات وسد الثغرات ولكن منذ تطوير تقنيات الذكاء الاصطناعي بدأ اهتمام الدول بشكل كبير باستخدامه في مجالات عدة ومنها الأمن السيبراني وهو ما حقق نتيجة للدفاع السيبراني من خلال التشغيل الآلي للعناصر الاساسية في العمل وهي الحاسوب والأجهزة التي تعتمد على المعالجات والبرمجيات، وتحويل ذلك الى عملية مستقلة تعمل على زيادة مواجهة التهديدات التي تطال الامن القومي للدول، وقدمت تقنيات الذكاء الاصطناعي مزايا كبيرة للدول لمواجهة التهديدات السيبرانية من خلال توفير حماية من خصومها ومن يحاول تهديد أمنها السيبراني، وذلك من خلال قياس مستوى الخطر التي تشكله الهجمات الإلكترونية والتعرف على أهم نقاط الضعف وتعزيز الأمن وطريقة الاستجابة للهجمات الالكترونية المحتملة، وهو ما يجعل اتخاذ القرار المناسب في فترة البحث والتحليل تكون دقيقة وشاملة[2].

ومن بين الأمور التي تشكل نقطة التقاء أو يكون الذكاء الاصطناعي بمثابة المكمل للأمن السيبراني، هو إمكانية تلافي الإخطاء إذ يتميز الذكاء الاصطناعي في هذا الجانب بالدقة وهو بذلك يعالج الأخطاء البشرية التي تحدث عند القيام بمهام متكررة وهذا ما يساهم بجعل القرارات الصادرة منه لا تتضمن العنصرية أو تميل لطرف على حساب الآخر، ودائما ما يكون الخطأ البشري من ابرز الاسباب في حدوث اختراق للبيانات، وهذا الأمر يستطيع الذكاء الاصطناعي التعامل معه وتجنبه، وهذا لا يعني أن الذكاء الاصطناعي يعد بديل للعاملين في مجال الامن السيبراني، بل يساهم في زيادة القدرات البشرية، وتحديدًا عندما تصل الفرق المكلفة بحماية الأمن السيبراني الى الإرهاق نتيجة لساعات العمل الطويلة أو مراقبة أزمة أو اختراق، فضلا عن التكلفة المالية التي يتطلبها إيجاد الخبراء وعملهم وكذلك الوقت الذي يستغرقه ذلك فضلا عن صعوبة إيجاد خبراء متدربين بشكل كافي بهذا المجال[3].

نتيجة للتطور السريع في تقنيات الذكاء الاصطناعي فإن ذلك جعل من إدارة التغيير في المجتمعات البشرية أكثر صعوبة وتعقيد، وأصبحت القوانين والسياسات التي يتم تشريعها لمواجهة هذه التحديات غير قادرة على مواجهة التطورات المتسارعة في عالم التكنولوجيا، وهذا ما جعل الدول والمؤسسات تواجه تحديًا كبيرًا وصعوبة في مواجهة هذا الواقع، وأن الاعتماد على الانترنيت بشكل كبير في جميع مجالات الحياة أصبح يفاقم من التحديات الامنية والقدرة

على مواجهتها في المستقبل، لاسيما أن كثير من المؤسسات والمراكز الحساسة أصبحت تعتمد بشكل متزايد على الانترنيت لاسيما أنظمة المراقبة ومحطات الطاقة والمواصلات، وأن البنية التحتية للأنترنيت التي تتحكم بهذه التفاعلات تعاني هي ايضًا من نقاط ضعف عدة، وحتى النظام الثنائي الذي يتم استخدامه في الأجهزة والبرامج، والذي حقق نجاحا طيلة العقود السابقة يمكن أن لا يكون قادرًا على مواجهة هذه التحديات في المستقبل، وهذا ما يتطلب البحث عن أدوات جديدة لضمان الأمن القومي للدول[4].

ومن بين الأمور التي تعد بمثابة علاقة بين الأمن السيبراني والذكاء الاصطناعي هو قدرة الأخيرة على الاستجابة للتهديدات السيبرانية بشكل فعال ومستمر، وهو ما جعل كثير من الأطراف الى التوجه نحو تطوير تقنيات الذكاء الاصطناعي من أجل مواجهة التهديدات السيبرانية بواسطة القيام بكشف هذه الهجمات ومن ثم التصدي لها وهذا ما يؤدي الى تطوير آليات جديدة، اذ بإمكان الذكاء الاصطناعي توفير الوقت وخفض تكلفة التصدي لهذه التهديدات سواءً كان مصدرها جهات حكومية أو جماعات إرهابية، وبغض النظر عن الأساليب والأدوات المحددة التي يستم استخدامها[5].

ويمكن القول ان علاقة الذكاء الاصطناعي بالأمن السيبراني مرت بثلاثة مراحل هي[6]:

المرحلة الأولى (2000-2010) في هذه المرحلة كانت اغلب الشركات والمؤسسات تعمل في بيئة تقنية مسيطر عليها بأحكام تعتمد على الكومبيوتر المكتبي واللابتوب ومراكز للبيانات توجد داخل المؤسسات، وكانت أغلب الهجمات في هذه المرحلة هدفها الفوضى والمال، واستخدمت فيها برمجيات خبيثة، وكانت المؤسسات تستخدم في الدفاع عن نفسها ادوات عادية مثل برامج مقاومة الفيروسات فضلا عن تبني نظام المصادقة الثنائية.

وظهر الذكاء الاصطناعي كوسيلة متميزة للحماية من خلال إثبات فاعلية غير معهودة في الكشف وعزل الرسائل الضارة، مما جعل الانظار تتجه نحو الذكاء الاصطناعي لقدرته على مواجهة التهديدات.

المرحلة الثانية (2010 - 2020): في هذا المرحلة عاش العالم نقلة نوعية نتيجة ازدياد تطبيقات البرمجيات والحوسبة السحابية، مما جعل التهديدات أكثر تعقيدًا، وتعرضت مؤسسات عدة لهجمات سيبرانية بواسطة برامج الفدية وافراغ اقراص التخزين وهذا ما جعل من تطوير تقنيات الذكاء الاصطناعي مسألة ملحة للتصدي لهذه الهجمات، وكانت أولى الخطوات نحو

هذا الهدف هو قيام شركة البرمجيات سيكلاني التي تأسست عام 2012 الى إضافة تقنية الذكاء الاصطناعي في أمنها السيبراني من خلال استبدال برامج مقاومة الفيروسات بنماذج للتعلم الآلي، وبعدها شهد هذا المجال تطور أكبر من خلال رصد العيوب والتحليل السلوكي وتطوير الآليات الدفاعية للتصدي لهذه الهجمات.

المرحلة الثالثة (2020 - الوقت الحاضر): في هذه المرحلة أصبح للذكاء الاصطناعي دورًا كبيرًا في الأمن السيبراني نتيجة للأطراف التي تعمل في كل مكان، وتطور انظمة المعلومات والاتصال التي أدت الى اضعاف الحدود الأمنية التقليدية وزيادة مساحة الهجمات، وبعد مراحل من العمل به بوصفه وسيلة دفاعية خالصة، أصبح الذكاء الاصطناعي اليوم سيف ذو حدين، يستخدم من قبل المهاجمين والمدافعين على حدٍ سواء، فمثلا تعمل أدوات الذكاء الاصطناعي الشائعة مثل (تشات جي بي تي) على تجنّب سوء استخدام الذكاء الاصطناعي، إلّا إنّ أدوات مثل (وورم جي بي تي) تبرز لمساعدة المهاجمين وتفتح المجال لمزيد من التحديات في الأمن السيبراني

ثانيا- أهداف الذكاء الاصطناعي وأدواره

يعمل الذكاء الاصطناعي دورا كبيرا في إدارة الحياة البشرية ولا يقتصر ذلك على المجالات العملياتية لكن مساره يشمل السياقات الفكرية المحركة للتوجهات، وللذكاء الاصطناعي مجموعة من الأهداف التي تتمثل بتطوير وظائف العمليات بواسطة إجراء التحليل المتقدم التلقائي للبيانات وهو يوفر بذلك الوقت والجهد، وكذلك يساهم الذكاء الاصطناعي بالوصول الى دقة عالية وفاعلية كبيرة في اتخاذ القرارات، معتمدة في ذلك على البيانات والتنبؤات، وكذلك بمرور الوقت تجعل تقنيات الذكاء الاصطناعي الطرق الخاصة بالتعلم الآلي قادرة على تحسين مهام عملها، ومن أهداف الذكاء الاصطناعي الأخرى هو تحسين التطبيقات الذكية وتطوير تطبيقات وطريق عمل تتفاعل مع المستخدمين وقادرة على توفير متطلباتهم، وتطوير مستوى الأمان واكتشاف ومواجهة التهديدات الأمنية وأيضا كشف آليات وطرق الاحتيال، فضلا عن تطوير البحث العلمي من خلال تقديم أدوات تحليل بيانات تمكن الباحثين من كشف الاشياء المعقدة والوصول الى نتائج متقدمة، وكذلك أن استخدام تقنيات الذكاء الاصطناعي يهدف الى الوصول الى التنمية المستدامة من خلال تحسين الآليات التكنولوجية المتطورة والوصول الى طرق تساعد في تحقيق الاستدامة وحماية الموارد الطبيعية،

وكذلك تحسين طرق التفاعل البشري مع الآلات من خلال تعزيز التفاعل السلس بين البشر والأنظمة الذكية[7] .

ومن أهداف الذكاء الاصطناعي هو معرفة العمليات الذهنية المعقدة التي يقوم بها العقل البشري من خلال القيام بالتفكير وبعدها تتم ترجمة هذه العمليات الى ما يوازيها من عمليات محاسبية تمنح الكومبيوتر القدرة على معالجة المشاكل المعقدة، ومعرفة شكل الذكاء الانساني من خلال آلية عمل الكومبيوتر التي تستطيع محاكاة السلوك الإنساني المتسم بالذكاء، وتعني إمكانية الحاسب على حل المسائل ، أو من خلال اتخاذ قرارات في موقف ما بواسطة وصف هذا الموقف ويمتلك البرنامج نفسه القدرة على حل المسائل والتعامل معها، أو من خلال العودة الى العديد من العمليات الاستدلالية التي تضمنها البرنامج[8].

المحور الثاني- دور الذكاء الاصطناعي في حماية الأمن السيبراني العراقي

أصبح الوصول إلى تقنيات الذكاء الاصطناعي وتطويرها من بين الاهداف الملحة التي تسعى إليها الدول لتعزيز امنها القومي، ولم تقتصر استخدامات هذه التقنيات على مجال معين إذ تعددت مجالات استخدامها لتشمل مختلف جوانب الأمن القومي للدولة، وللإحاطة بهذا الموضوع بشكل علمي كان لا بد من دراسته في قسمين الأول يتطرق لاستخدام تقنيات الذكاء الاصطناعي في المجال الأمني والعسكري والجانب الثاني يتضمن دراسة استخدام تقنيات الذكاء الاصطناعي في حماية الأمن السيبراني.

اولاً-استخدامه كآلية للكشف عن التهديدات

بدأت الدول تعتمد على تقنيات الذكاء الاصطناعي بشكل كبير وذلك لاستخدامه في الكشف عن التهديدات السيبرانية وذلك وفقا لدراسة اجرتها شركة Capgemini العالمية والتي جاءت نتائجها بان (50%) من المؤسسات التي اعتمدت على تقنيات الذكاء الاصطناعي لتعزيز أمنها السيبراني ، كانت تستخدمها من أجل عملية الكشف عن التهديدات والسبب في ذلك يرجع الى القدرة الكبيرة التي تمتع بها تقنيات الذكاء الاصطناعي على تحديد حركة المرور غير المنتظمة من خلال التعلم الآلي والتعلم العميق[9].

وهناك فرص عديدة للذكاء الاصطناعي تستعمل فيها أنظمة تعلم الآلة بصفة عامة من أجل المساعدة في التعامل مع المشاكل الكبيرة للفضاء السيبراني، وتكون بمثابة عامل مساعد

في اتخاذ القرار البشري الفعال في سبيل الاستجابة لهذه التهديدات، ويمكن أن تساهم تقنيات الذكاء الاصطناعي في المستقبل بتقديم تحليلات تنبؤيه من أجل توقع التهديدات، ويمكن أن يكون الذكاء الاصطناعي مدخلا للإلكترونيات من خلال تكوين نماذج ديناميكية من مصادر البيانات الموجودة التي ربما تكون ضخمة وغير مكتملة، وتحتوي هذه البيانات أقسام الشبكة ووصلات أكثر كفاءة لتوضيح هذه البيانات وإيجاد نقاط الضعف الكامنة قبل وقوع المشكلة، فضلا عن إمكانية ايقاف التهديدات في التصرف أو الرسائل المعنية أو يمكن تكون هناك إمكانية كبيرة للحد من آثارها، وكذلك تم تطوير الذكاء الاصطناعي وجعله قادرًا على اكتشاف الرسائل والتصرفات التي يكون هدفها الغش والخداع والفساد، والتي تحاول الدخول الى التطبيقات والنظم القائمة وكذلك محاولة انتحال شخصية مستخدم آخر فضلا عن استخدامه من أجل الكشف عن رسائل البريد الالكتروني غير المرغوب فيها والكشف عن الهجمات التي تحاول الحاق الضرر المتعمد ومنعه[10].

وأما ما يتعلق بالعراق فإن التقرير السنوي الخاص بالأمن السيبراني لعام 2022، والذي تصدره شركة شركة ترينـد مايكرو، قد أشار الى اكتشاف ومنع وحظر اكثر من (15) مليون تهديد عبر البريد الالكتروني، وقامت بتوفير الحماية الى ما يقارب من (400) الف مستخدم من التضرر بواسطة الروابط الخبيثة وتمكنت من إيقاف أكثر (500) الف هجوم لبرمجيات ضارة في العراق، وبحسب التقرير فإن التكنلوجيا ساهمت بتقديم الكثير من الفرص لمؤسسات الدولة، لكنها في الوقت ذاته شكلت تحديات أمنية جديدة، لذلك من الضروري المحافظة على جهود الاعتماد الآمن على التكنلوجيا في العراق لحماية الفضاء السيبراني للدولة من التهديدات الإلكترونية وحماية البيانات المهمة والحساسة، وأعلنت هذه الشركة التزامها بتقديم الدعم والمساعدة للعراق لتحقيق أهداف التحول الرقمي ودعمهم بالحلول الأمنية متعددة الطبقات والمراحل الدفاعية، وذكر التقرير ايضًا زيادة نسبة الهجمات الضارة بنسبة (103%)، وتنصح العراق باتباع طرق استباقية بواسطة القيام بتقييمات شاملة لحماية البنية التحتية الرقمية ومواكبة أحدث التقنيات الإلكترونية لمواجهة التحديات السيبرانية[11].

ويعد التهديد السيبراني من أكبر التحديات التي تواجه المنظومة الأمنية العراقية، لا سيما التهديدات السيبرانية المرتبطة بالتنظيمات الإرهابية والتي تعد من بين أكبر الجهات التي تهدد الأمن السيبراني العراقي، إذ تعتمد التنظيمات الإرهابية في اتصالها بالعالم الخارجي على

وسائل متقدمة وتستخدم الدعاية من خلال وسائل التواصل الاجتماعي منطلقا للدعاية والترويج لأفكارها وأعمالها مع العالم الخارجي، وتصنف نشاطات الدعاية والترويج للأفكار المتطرفة التي تصدر من التنظيمات الارهابية او أي جهات داخلية او خارجية اخرى من بين التهديدات السيبرانية [12].

وذكرت جمعية الانترنيت والتي تتخذ من الولايات المتحدة مقراً لها بان هناك أربعة مبادئ للأمن السيبراني، يتمثل أولها في الوعي، وذلك من خلال قيام الجهات المختلفة بإدراك المخاطر ومدى تأثيرها عليها وعلى الآخرين في النظام البيئي الذي يهتم بالبنى التحتية لشبكة الانترنيت واستعمالها، ويجب على جميع الأطراف الالتزام بمبدأ مواجهة التحديات الأمنية التي تهدد أمنها، والآثار المترتبة عليها، أو التقاعس عنها والتعاون باشراك جميع الأطراف حتى المتواجدة خارج الحدود المحلية في حوار دائمي يدور حول الأمن السيبراني لمواجهة التحديدات الرقمية، وتم التأكيد ايضًا على ما أطلق عليه مبدأ الحقوق الاساسية وخصائص الانترنيت، والتي تعني الالتزام بالحقوق الرئيسة والالتزام بالشفافية وعدم المساس بخصائص الانترنيت التي تهتم بالمشاركة التطوعية التي يجب على جميع الأطراف المعنية عند اتخاذ أي قرار او إجراء معين[13].

ورغم الجهود التي يبذلها العراق لتعزيز أمنه السيبراني لكن ما زالت هناك مجموعة من المؤشرات التي تؤكد تأثيرها على الأمن الوطني العراقي وتحديداً في مجال البنى التحتية الرقمية لا سيما في مسألة التبويب الرقمي الاقتصادي، فالعراق في الفضاء المعلوماتي لا يعيش العزلة إذ يرتبط مع دول العالم في الفضاء المعلوماتي، ويؤدي ضعف البنى التحتية للأمن الالكتروني الى انكماش استراتيجي أمام الدول الأخرى، وتسهل بالتالي عملية الأضرار به من خلال الاختراق والتجسس على البيانات والمعلومات التي تتعلق بالأمن السيبراني، أو ربما تعمل بعض الجهات على جعل دولة ما منطلقا لشن الهجمات الإلكترونية على الأمن المعلوماتي للدول الأخرى ومحاولة اختراقه وسرقة معلوماته وجعلها إدارة للمساومة في تنفيذ اعمال عدائية[14].

وفي إطار الجهود التي يبذلها العراق لتعزيز أمنه السيبراني فقد تم الإعلان عن استراتيجية الأمن السيبراني في عام 2017 من أجل وضع الإجراءات اللازمة لحماية الأمن السيبراني العراقي، من خلال حماية البنى التحتية المعلوماتية وإنشاء مجتمع انترنيت موثوق فيه،

وتضمنت هذه الإستراتيجية أبرز التهديدات السيبرانية التي تواجه العراق تتمثل في الجريمة والإرهاب الإلكترونية، والصراع السيبراني والتجسس والاختراق السيبراني، فضلًا عن إساءة معاملة الاطفال، وتضمنت الاستراتيجية ايضاً أبرز نقاط الضعف والآثار والفرص المتاحة في هذا الجانب، من أجل القيام بإجراءات تشريعية تهدف لحماية الأمن السيبراني وتوفر التدابير اللازمة لذلك، وتضمنت هذه الإستراتيجية خطة عمل من ثمانية محاور متمثلة بالحكومة الفعالة، والإطار التشريعي والتنظيمي، وإطار تكنولوجيا الأمن السيبراني، وثقافة الأمن السيبراني وبناء القدرات، والبحث والتطوير نحو الاعتماد على الذات، والامتثال والتنفيذ، والجاهزية لحوادث الأمن السيبراني، الى جانب التعاون الدولي، وكذلك تشكيل فريق وطني للاستجابة السريعة للتهديدات السيبرانية يكون عمله تحت أشراف واستشارة الأمن الوطني، ويكون عمله مكرس لحماية مراكز الشبكات ومراكز البيانات الوطنية والمواقع الرسمية التي تعمل في الفضاء المعلوماتي، فضلًا عن تنسيق الجهود الوطنية وتوفير الدعم للمؤسسات العامة والخاصة لتوفير الحماية لنفسها وتعزيز ثقة المواطن بالمؤسسات والارتقاء بمستوى العراق دولياً في مجال الأمن السيبراني لتشجيع تطوير الخدمات الإلكترونية ودعم مشروع الخدمات والحكومة الإلكترونية[15].

وفي العقد الثاني من القرن الحادي وظفت كثير من الدول والمؤسسات في عملها متطلبات أمن المعلومات، وذلك من خلال إدخال تقنيات الذكاء الاصطناعي في أدارة الحوادث من أجل مراقبة مخاطر شبكات المعلومات وبياناتها التي تحتاج الى مبالغ كبيرة ووقت وجهد أيضا، وفي هذا المجال قام الخبراء بمحاولات عديدة في تطوير وسائل من أجل التغلب على المخاطر المعقدة التي تستعمل وسائل تقليدية من خلال القيام بأعمال يدوية تستغرق وقتا طويلا من أجل الحد من آثارها وتبعاتها بصورة كاملة وفعالة، وتم إحراز تقدم في هذا المجال باستخدام الذكاء الاصطناعي من خلال عمليات التحليل للأحداث المختلفة وفرز نتائج التهديدات السابقة مما ساهم في تحقيق نتائج صائبة لتجنب هذه التهديدات، وينبغي على العراق أن يكثف جهوده في الاستفادة من تجارب الدول الصديقة في تكوين ما يشبه بالدرع المعلوماتي الحصين من أجل حماية وتعزيز أمنه السيبراني، لا سيما وأن ناقلات التهديدات في الوقت الحالي تتطور بصورة مستمرة ما يجعل الكشف والاستجابة الاستباقية هي الحل

الأمثل لذلك وتكون من خلال تنسيق الأمن والاستجابة المختلفة للأدوات التي تنفذ العلامات مثل إغلاق الموجهات والمنافذ ونقاط النهاية في وقت قريب من الحقيقة[16].

ثانيا- استخدام كآلية لتعزيز الأمن السيبراني من خلال التنبؤ

يمكن للعراق أن يطور تقنيات الذكاء الاصطناعي لتعزيز أمنه السيبراني من خلال ما توفره هذه التقنيات من ميزات كبيرة من خلال التنبؤ، إذ بدأ عدد كبير من الدول والمؤسسات العالمية الكبرى تستخدم التنبؤ بالتهديدات السيبرانية، ويتم ذلك من خلال إجراء عملية مسح شامل للبيانات وإجراء تنبؤات بواسطة القيام بعمليات تدريب للنظام على تلك الخطوات، إذ تستطيع الدول التي تستخدم الذكاء الاصطناعي في هذا الجانب أن تستخدم أيضًا التكنولوجيا لهذا الغرض، من أجل تحديد أهم نقاط الضعف الحرجة وكذلك تحديد أصل وطوبولوجيا الشبكة بشكل تلقائي وتطوير النظام الدفاعي للشبكة بشكل مستمر ليجعلها قادرة على صد الهجمات السيبرانية المحتملة[17].

ويعد التحليل البياني من الآليات الهامة التي تمكن الدول من فهم البيانات التي تجمعها وتحولها الى معلومات وقرارات هامة بواسطة الذكاء الاصطناعي الذي يمكن العاملين في الأمن السيبراني من تسريع عملية التحليل وتطوير دقتها لاسيما البيانات الضخمة وتحديد الاتجاهات والأنماط والتنبؤ بالمستقبل مما يمكن من تسريع أتخاذ القرار وكذلك التنبؤ بالهجمات السيبرانية قبل حدوثها، أي من خلال دمج الذكاء الاصطناعي بالأمن السيبراني نستطيع تكوين أنظمة أمان وحماية آلية تستطيع الكشف بشكل تلقائي عن التهديدات والبرامج الضارة والتنبؤ بالهجمات التي يمكن ان تتعرض لها الدولة[18].

أصبح الذكاء الاصطناعي جزءاً لا يتجزأ من الأمن السيبراني لدرجة أن يصعب الفصل بينهما، وذلك لقدرة أنظمة الذكاء الاصطناعي التي توجد في الحاسوب على إظهار التهديدات ومن ثم التصدي بسرعة عالية وذلك في حالة توظيفها بشكل صحيح ضمن منظومة الأمن السيبراني، لاسيما أن الأمن السيبراني وتقنيات الذكاء الاصطناعي ترتبط بصورة مباشرة أو غير مباشرة بخصوصية الأفراد التي تعد واجبة الحماية، وهذه المعلومات يمكن اختراقها ومن ثم إساءة استخدامها من خلال العمل على اختراق الأمن السيبراني للدول والاشخاص وانتهاك خصوصية بياناتهم[19].

يجب على العراق تطوير تقنيات الذكاء الاصطناعي من خلال الاستفادة من التجارب الدولية، وتعد الصين من أكبر المنافسين التكنولوجيين إذ تمتلك نظام متقدم وموارد معززة لذلك تتيح لها الفوز بهذه المنافسة، واليوم تعتمد عليه بشكل كبير من أجل توسيع نفوذها ومنافسة القوة العسكرية والاقتصادية للدول الكبرى المنافسة، وكذلك تعمل على تمويل المشاريع الضخمة التي تتعلق بالبنى التحتية الرقمية العالمية[20].

جدول (1) نمو السوق العالمية للذكاء الاصطناعي ومستقبلها

ت	السنة	النسبة
1	2022	%23.6
2	2024	%46.3
3	2027	%174.7

المصدر: حنان عباس سلمان، ابتسام كاظم جاسم، القوة السيبرانية واثرها على القوة الاقتصادية – الصين انموذجا، مجلة مركز دراسات الكوفة، العدد 70، جامعة الكوفة، 2023، ص 637.

ورغم الجهود الكبيرة التي يقوم بها العراق في هذا المجال لكن تتطلب مواجهة هذه التهديدات الحالية تشكيل هيئة وطنية موحدة لجميع الأجهزة والمؤسسات التي يمكن أن تساعد في منع ومواجه التهديدات للأمن السيبراني العراقي، ويكون عملها ضمن الاستراتيجية الوطنية للأمن السيبراني لكن بصلاحيات أكبر، تقوم بتعزيز الأمن السيبراني العراقي، وكذلك تعمل على تعديل التشريعات الحالية حتى تتمكن من مواجهة التهديدات المعاصرة، وكذلك إرساء ثقافة عامة للأمن السيبراني على صعيد المؤسسات والافراد، فضلاً عن تطوير البحث العلمي في الجانب المتعلق بالأمن السيبراني والذكاء الاصطناعي وتدريب وتنمية المهارات الرقميَّة بشكلٍ مستمر، لمواكبة المستجدات الإلكترونيَّة، على مستوى المنطقة والعالم[21].

ثالثا- استخدامه كآلية لتعزيز الأمن السيبراني من خلال الاستجابة

تطورت تقنيات الذكاء الاصطناعي للاستجابة للتهديدات السيبرانية بشكل كبير، اذ تتيح هذه التقنيات للدول والمؤسسات القيام باستخدام الذكاء الاصطناعي باستمرار من أجل اكتشاف الهجمات والتصدي لها في الوقت ذاته، ويمكن أيضًا استخدام الذكاء الاصطناعي في اتمتة إنشاء رقعة افتراضية للتهديدات المكتشفة فضلًا عن تطوير أدوات حماية جديدة، ويعمل الذكاء الاصطناعي أيضًا على مساعدة الدول والمؤسسات العالمية على خفض التكلفة

وتوفير الوقت من أجل الاستجابة للتهديدات ومواجهة الانتهاكات، بغض النظر عن شكل الاشكال والخصائص المحددة التي تستعمل فيها[22].

ومن خلال اعتماد كثير من الدول على التكنولوجيا في مجالات عديدة كالاتصالات والتمويل والنقل والرعاية الصحية والأمن السيبراني والطاقة بشكل متزايد مما جعل حالات القرصنة وسرقة البيانات الهوية والتجسس يكون لها أثر كبير على عمل مؤسسات الدولة ويمثل تحدي كبير لأمنها القومي، مما يتطلب اتخاذ تدابير الأمن السيبراني من أجل ضمان حماية الأفراد والشركات والحكومات من الهجمات السيبرانية وبما يضمن توفير الحماية للبيانات الشخصية وزيادة طرق التشفير وجدران الحماية وإجراءات الأمان الأخرى من أجل تحقيق حماية فعالة للبيانات وكذلك اصبحت البنية التحتية لتقنيات الذكاء الاصطناعي معرضة بصورة كبيرة للهجمات والاختراق، وفي الوقت الحالي أصبحت اغلب مؤسسات الدولة تعتمد على التكنولوجيا وتكون مترابطة مثل شبكات الكهرباء وشبكات النقل ومرافق الرعاية الصحية والاتصالات ... الخ، مما يجعل الهجمات السيبرانية تؤدي إلى الحاق الضرر بالخدمات، مما يتطلب توفير الحماية للبنية التحتية من خلال تعزيز الامن السيبراني، فهناك فرصة إذا أراد العراق تعزيز أمنه السيبراني فهناك فرصة كبيره أمامه لذلك، من خلال استعمال تقنيات متطورة من الذكاء الاصطناعي بواسطة التعلم الآلي من أجل حماية الشبكات وهذا يساعد بشكل كبير على التعرف على الهجمات السيبرانية والقدرة على مواجهتها ومنعها في الوقت المناسب وهذا يجعل المؤسسات قادرة على مواجهة التحديات الناشئة وكذلك فإن تعلم الآلة بأتمتة الإجراءات الأمنية (كشف التهديدات والتحديات والقدرة على منعها والتعامل معها يساعد في تقليل جهود ومسؤولية الأمن البشري) فضلا عن ذلك فإن تحول المجتمعات ودمجها بالذكاء الاصطناعي ممكن أن يؤدي الى الوصول الى أهداف التنمية المستدامة وكذلك تنظيم التقنيات من أجل الوصول الى الأهداف الاجتماعية وبما يساهم في الاستخدام الأمني والأخلاقي ويساعد ذلك الشكل من المجتمعات في تحقيق السلامة والاستدامة والمسؤولية الاجتماعية كما أن تلك التقنيات تنظم الاستدامة البيئية أي الحد من انبعاثات الغازات الدفيئة والنفايات وتعزيز الاقتصاد الدائري إذ يجب أن تكون أيضا صديقة للبيئة ختاما لقد غير الذكاء الاصطناعي أنظمة الخدمات الاجتماعية كالخدمات الصحية والنقل والتعليم والتمويل وآثار قضايا أخلاقية[23].

ويعد تعزيز الأمن السيبراني، ومنع الهجمات السيبرانية من الامور الهامة نتيجة اعتماد المؤسسات بشكل كبير على التكنولوجيا في عملها، وإذا اراد العراق تعزيز أمنه السيبراني فإن الطريقة الصحيحة تكون من خلال تطوير وتعزيز الوعي الأمني وأمن المعلومات، والاجراءات الوقائية لحماية الشبكات من خلال تدريب الموظفين وتثقيف الجمهور العام للمستخدمين، وكذلك استعمال الأجهزة المتطورة من أجل منع ومكافحة الاختراقات، وتقييم الأضرار والعوامل المؤثرة فيه، فضلا عن استفادة العراق من الخبرات الدولية في هذا المجال واستخدام الدبلوماسية العراقية بتكوين إطار قانوني دولي قادر على التصدي بشكل فعال للهجمات السيبرانية من خلال تبادل المعلومات والخبرات والوصول الى قوانيين دولية فعالة من اجل توفير الحماية للبيانات ومكافحة الهجمات السيبرانية، ومعاقبة المتسللين، وبواسطة هذه التدابير تكون الدول والمؤسسات قادرة على التصدي لتهديدات الإرهاب السيبراني وحماية الأنظمة والمعلومات الحساسة ومواجهة التحديات الجديدة في عصر الذكاء الاصطناعي، كما إن اهتمام الافراد بأمن بياناتهم ووعيهم بمخاطر تهديدات الإرهاب السيبراني يلعبان دوراً هاماً في الحفاظ على سلامتهم الشخصية وأمنهم الرقمي[24].

ويحقق الذكاء الاصطناعي مزايا كبيرة تساعد في تعزيز الأمن القومي للدولة بشكل كامل، إذ بدأت الدول تعتمد بشكل كبير على تقنيات الذكاء الاصطناعي لتعزيز أمنها القومي، وذلك لأن الأنظمة المعززة بتقنيات الذكاء الاصطناعي أثبتت قدرتها في مسالة الاستطلاع ودقة تنفيذ الضربات، واختراق الدفاعات الجوية المتطورة متعددة المستويات، وكذلك شن الحرب الإلكترونية من خلال الفضاء السيبراني، والعمليات غير القتالية والدعم التوجيهي للصواريخ لدقة عمليات الاستهداف، وبالتالي فإن تعزيز الأمن السيبراني باستخدام الذكاء الاصطناعي أصبح ساحة للتنافس بين الدول، إذ تتسابق هذه الدول من أجل النجاح في تطوير تقنيات الذكاء الاصطناعي بشكل يجعلها تفوق على الأطراف الأخرى، مما يجعلها تمتلك ميزة الردع مثل هذه التقنيات المزودة بالذكاء الاصطناعي لتحليل البيانات وتحديد الأنماط ذات الصلة بالهجمات المحتملة بسرعة أكبر، لذا جاءت أهمية تعزيز الوعي العام بمجال الأمن السيبراني، بما يتماشى مع التطور التكنولوجي في مجال الحوسبة السحابية وإدارة البيانات وحوكمة المعلومات وتقنيات الذكاء الاصطناعي، وكذلك تطوير البرمجيات المقاومة للهجمات السيبرانية

من خلال تزويد أنظمة أمن المعلومات بأحدث الأساليب والتقنيات لاسيما تقنيات الذكاء الاصطناعي للتصدي للتهديدات والهجمات السيبرانية المحتملة[25].

ويستطيع العراق استخدام تقنيات الذكاء الاصطناعي التي تعطي البرامج المدعومة بالذكاء الاصطناعي استجابة آلية للأحداث الأمنية في الوقت الحقيقي، اذ انها قادرة على ابعاد الأجهزة المخترقة، ومنع الوصول غير المصرح به إلى الشبكات، ومنع انتشار التهديدات، فضلا عن استخدام وتحليل البيانات لزيادة القدرة التنبؤية للبيانات القديمة من اجل استباق الهجمات واماكن الضعف في المستقبل، مما يجعل الدول قادرة على اتخاذ التدابير الاستباقية الوقائية قبل حدوث الهجمات، وتعمل تقنيات الذكاء الاصطناعي دورًا مهمًا في إدارة أماكن الضعف من خلال مسح وتعريف الخلل في الشبكات والنظام العام في المؤسسات نتيجة لإمكانية تصنيف أماكن الضعف وفق التأثير المحتمل، مما يجعل الدولة قادرة على تخصيص مواردها بفاعلية وكفاءة لمواجهة المشاكل الحساسة، وكذلك تمكن خاصية تحليل تقنيات معالجة اللغة الطبيعية المدعومة بالذكاء الاصطناعي كميات ضخمة من البيانات غير المنظّمة من مصادر عديدة مثل المقالات الإخبارية والمدونات ومواقع الاجتماعي، ما يجعل خبراء الأمن قادرين دراية بالتهديدات الناشئة وتقنيات الهجوم الآخذة في التطوّر، وكذلك يجب على العراق الاستفادة من أنظمة استعمال التعلّم الآلي لمقاومة الفيروسات والبرامج الضارة لان بذلك يمكن من توفير الحماية للمؤسسات والبيانات ومعلومات الموظفين والزبائن الشخصية للحفاظ على تفوّقها في قضية الأمن السيبراني[26].

الخاتمة

أصبحت تحديات الأمن السيبراني من بين أكبر التحديات التي تهدد الأمن القومي للدول، نظرًا لارتباط مؤسسات الدولة الهامة والحساسة مثل قطاع الطاقة والأمن والاقتصاد ضمن شبكة مترابطة لذلك يمكن أن يؤدي اختراق او تعطيل هذه المؤسسات الى فوضى وخسائر مالية كبيرة نتيجة توقف كثير من الخدمات، ويمكن أن يؤدي ذلك الى تهديد الأمن القومي للدولة من خلال تسريب معلومات حساسة تتعلق بالدولة أو أفرادها.

ونظرًا لعدم نجاعة الحلول التقليدية السابقة في منع عمليات الاختراق وتهديد الأمن السيبراني للدول، فضلا عن الوقت الذي قد تستغرقه هذه الحلول أضافة للجهد الكبير الذي

يبذل في ذلك، وكذلك ارتفاع التكلفة المادية لتوفير متطلبات الأمن السيبراني لاسيما الأجهزة والمعدات والخبراء.

كل ذلك جعل الدول تبحث عن حلول ناجعة وسريعة وفعالة تعزز بها أمنها وتحافظ من خلالها على مواردها، فأصبح الذكاء الاصطناعي يمثل أهم ساحة للتنافس بين الدول سعيا منها لتعزيز أمنها وامتلاك تقنيات تجعلها الأفضل بين الدول المتنافسة.

ورغم الإجراءات والاصلاحات التي يقوم بها العراق لتعزيز أمنه السيبراني من خلال الاعتماد على حلول ومبادرات عديدة، من بينها استراتيجية الأمن السيبراني التي انطلقت عام 2017، لكن رغم ذلك لا زال العراق يحتاج الى خطوات اضافية تجعله قادراً على منع الهجمات السيبرانية او القدرة على الاستجابة السريعة من اجل تقليل اثارها، وذلك من خلال تطوير تقنيات لذكاء الاصطناعي التي تحقيق نتائج كبيرة في مجال تعزيز الامن السيبراني العراقي من خلال قدرتها على كشف التهديدات، فضلا عن امكانية التنبؤ من خلال القيام بعملية مسح شامل للبيانات واجراء تنبؤات بواسطة عمليات تدريب النظام على تلك الخطوات، مما يجعلها قادرة على التبوء بالهجمات واكتشاف مناطق الضعف التي يمكن استهدافها، وكذلك تستطيع تقنيات الذكاء الاصطناعي توفير القدرة على الاستجابة الفعالة للتهديدات بشكل آلي والقدرة على تطوير وسائل حماية جديدة لها.

المصادر والمراجع

[1] نبيل محمد عبدالرحمن، التحكم في منحدرات الخطوط السريعة باستخدام الذكاء الاصطناعي،(الرياض: جامعة الملك سعود، 2000) ص 47-48.

[2] المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات ECCI، دور الذكاء الاصطناعي في الأمن السيبراني، وحدة الدراسات(26)، تاريخ النشر 2024/2/3، على الرابط: https://2u.pw/89DIGVqK، تم الاطلاع 2024/3/1.

[3] حسام عبد الامير خلف، وهج علي حمزة، مفهوم الامن السيبراني وعلاقته بالذكاء الاصطناعي، مجلة جامعة الانبار للعلوم القانونية والسياسية، المجلد، 13، العدد 2، جامعة الانبار، 2023، ص 655-656.

[4] مركز الاتحاد للاخبار، دراسة جديدة لـ«ترينديز» تقرأ العلاقة بين الذكاء الاصطناعي والأمن السيبراني، تاريخ النشر: 2024/4/10، على الرابط: https://2u.pw/jRJlLmhy. 2024 4/ 15 ، تم الاطلاع بتاريخ

[5] حسام عبد الامير، مصدر سبق ذكره، ص 656.

[6] موقع قناة سكاي نيوز الاخباري، مواجهة التهديدات السيبرانية في عصر الذكاء الاصطناعي خطوات دفاعية بتوظيف نظمه المتطورة، تاريخ النشر 18/ 4/ 2024، على الرابط: https://2u.pw/260Wsvku، تم الاطلاع بتاريخ 15 / 3 / 2024.

[7] محمد سالم صالح النجار، الذكاء الاصطناعي ودوره في مكافحة الارهاب، المجلة العلمية لجهاز مكافحة الارهاب، العدد 6، المجلد 3، بغداد، 2023، ص 87.

[8] سالم زعموكي، فتيحة حبالي، الذكاء الاصطناعي وانعكاساته الاقتصادية على العالم، مجلة التراث، المجلد، 13، العدد 4، الجزائر، 2023، ص 39.

[9] ألبانا ايسيني، الذكاء الاصطناعي والامن السيبراني: دراسة فيما يخبئه المستقبل، ترجمة : باسم علي خريسان، (بغداد: مركز البيان للدراسات والتخطيط، 2022)، ص 4.

[10] محمد محمد الهادي، الذكاء الاصطناعي معالمه وتطبيقاته وتأثيراته التنموية والمجتمعية، (القاهرة، الدار المصرية اللبنانية، 2021)، ص 108.

[11] صحيفة المواطن، 20 مليون تهديد في العراق: تقرير الأمن السيبراني يكشف حصيلة 2022، تاريخ النشر 17 / 7 / 2023، على الرابط: https://2u.pw/pCgENrYx، تم الاطلاع بتاريخ 25/ 3/ 2024.

[12] جاسم يونس الحريري، قراءة في التحديات تجاه العراق ودول مجلس التعاون الخليجي بعد 2018، (عمان: دار الجنان للنشر والتوزيع، 2022)، ص 126.

[13] صفد الشمري، ما واقع الامن السيبراني في العراق، جريدة الصباح العدد 5135 ، بتاريخ 6/8/ 2024.

[14] مروان سالم العلي، التحديات الاستراتيجية للأمن الوطني العراقي في ظل المتغيرات الدولية، مجلة تكريت للعلوم السياسية، المجلد 2، العدد 20، جامعة تكريت، 2020، ص 57.

[15] صفد الشمري، مصدر سبق ذكره.

[16] محمد محمد الهادي، الذكاء الاصطناعي: معالمه وتطبيقاته وتاثيراته التنموية، (القاهرة: الدار المصرية اللبنانية، 2021)، ص 276.

[17] ألبانا ايسيني، مصدر سبق ذكره، ص 4-5.

[18] بسيوني محمد الخولي، رؤية الاسلام للتاثير المبتكر للذكاء الاصطناعي، (القاهرة: مثابة الابداع للطباع والنشر والتوزيع، 2024)، ص 242.

[19] حسام عبد الامير خلف، وهج علي حمزة، مصدر سبق ذكره، ص 654.

[20] حنان عباس سلمان، ابتسام كاظم جاسم، القوة السيبرانية واثرها على القوة الاقتصادية – الصين انموذجا، مجلة مركز دراسات الكوفة، العدد 70، جامعة الكوفة، 2023، ص 637.

[21] صفد الشمري، مصدر سبق ذكره.

[22] ألبانا ايسيني، مصدر سبق ذكره، ص 5.

[23] بسيوني محمد الخولي، مصدر سبق ذكره، ص 424.

[24] فاضل عباس حسن، تهديدات الارهاب السيبراني في عصر الذكاء الاصطناعي، بحث منشور في جامعة كربلاء، تاريخ النشر: 2024/1/17، على الرابط: https://uokerbala.edu.iq/archives/30707، تم الاطلاع بتاريخ 5/ 4/ 2024.

[25] هالة احمد الحسيني، دعاء هشام جمعة، الذكاء الاصطناعي وتوظيفه في المؤسسات الاعلامية، (القاهرة: العربي للنشر والتوزيع، 2023)، ص 16.

[26] صحيفة الشرق الاوسط، نظم الذكاء الاصطناعي تساهم في صد الهجمات السيبرانية، تاريخ النشر: 2023/11/15، على الرابط:https://2u.pw/usogi8o ، تم الاطلاع بتاريخ 2024/4/10.

ملف العدد
الأمن السيبراني
درع التحول الرقمي العراقي
(بين التحديات الراهنة وضرورات المستقبل)

دور الأمن السيبراني
في تطور قوة الدولة العراقية: دراسة تحليلية وتوقعات مستقبلية

م.د. سالي سعد محمد

الجامعة العراقية/ كلية القانون والعلوم السياسية

بفضل ثورة التكنولوجيا والمعلومات ودخول العالم العصر الرقمي أصبح الأمن السيبراني من الموضوعات المهمة لارتباطه المباشر في جميع جوانب الحياة سواءً السياسية ، العسكرية، الاقتصادية، الاجتماعية ، وحتى الثقافية ، ويعد الاهتمام به من أولويات الأمن القومي لأي دولة ، وذلك لأنه كلما زاد التشابك زادت التهديدات السيبرانية مما يؤدي بالتأثير على قوة وأمن الدولة، والعراق بعد عام (2003) شهد هذا التطور والانفتاح في المجال المعلوماتي والتقني مما أدى بأن يكون أكثر عرضة للهجمات السيبرانية .

الكلمات المفتاحية: الأمن السيبراني ، العراق ، التهديدات السيبرانية.

The role of cybersecurity in the development of the strength of the Iraqi state: an analytical study and future expectations

Dr. Sally Saad Mohammad

Iraqi University / College of Law and Political Science

As a result of the technology and information revolution and the world entering the digital age, cybersecurity has become one of the important topics because of its direct connection to all aspects of life, whether political, military, economic, social, or even cultural. Paying attention to it is considered one of the national security priorities of any country, because the greater the interconnection, the greater the cyber threats, which This leads to an impact on the strength and security of the state, and Iraq after the year (2003) witnessed this development and openness in the information and technical field, which leads to it being more vulnerable to cyber attacks .

Keywords: cybersecurity, Iraq, cyber threats.

الاستلام	الارجاع	القبول
2024/05/02	2024/06/14	2024/06/20

المقدمة

يُعد الأمن السيبراني من التحديات الأمنية المعاصرة إذ أصبح يؤدي دوراً حاسمًا في قوة الدولة في العصر الحديث، ويشكل قيمة مضافة لكل دولة، وله علاقة مباشرة باستقرارها إذ يؤثر بشكل كبير على القدرة القومية للدولة ، وذلك بسبب ارتباطه بجميع قطاعات الحياة السياسية والأمنية والعسكرية والاقتصادية والتقنية حتى الثقافية، وأصبح له دور فعال في تسيير مختلف الموارد في العالم، ويشهد العراق منذ عام (2003) انفتاح وتطور كبير في المجال التقني والمعلوماتي ويعد الأمن السيبراني حاجة ملحة للواقع العراقي، إلا أنه لا يزال يعاني من حالة ضعف وعدم استقرار في هذا المجال مقارنة بالدول الأخرى ، وذلك بسبب عدم امتلاكه القدرات الكافية التي تؤهله إلى مواكبة هذه التحديات السيبرانية، والتي بدورها تؤثر على قوة الدولة العراقية واستقرارها، مما يتطلب على الدول كافة ومنها العراق تكثيف جهودها لتعزيز الأمن السيبراني من خلال تطوير السياسات والتشريعات الخاصة به، وتعزيز التعاون الدولي لمكافحة التهديدات السيبرانية، ويجب أن تعد ذلك جزءً من استراتيجياتها للحفاظ على الاستقرار والتطور المستدام ، وذلك لأن نقص الأمن السيبراني يؤدي إلى فقدان الثقة في الحكومة والاقتصاد، مما يضعف قدرتها على التنافس على الصعيدين الوطني والدولي.

إشكالية البحث:

بسبب التطورات الرقمية التي يشهدها العالم، ازدادت معها التحديات السيبرانية واختلفت آثارها وانعكاساتها وامتددت لتشمل مختلف الجوانب السياسية والعسكرية والاقتصادية والاجتماعية والتقنية والثقافية، مهددة بذلك قوة الدولة واستقرارها ومن ذلك نطرح السؤال البحثي المركزي الآتي : **كيف يؤثر الأمن السيبراني على قوة وتطور العراق ؟**

وتندرج ضمن السؤال البحثي الأسئلة الفرعية الآتية:

1- كيف أثر الفضاء السيبراني على الأمن والقوة والحرب ؟
2- ماهي أهمية الأمن السيبراني؟ وما علاقته بقوة الدولة؟
3- ما هو واقع الأمن السيبراني في العراق؟
4- كيف تواجه الدولة العراقية التحديات السيبرانية؟ وما هي الآليات التي يجب أتباعها لتعزيز الأمن السيبراني؟ وما هو مستقبل الأمن السيبراني العراقي؟

أهمية البحث :

تأتي أهمية البحث من أهمية الموضوع الذي نبحث فيه والمتمثل بالقوة والأمن السيبراني وأثرهم على قوة الدولة وتطورها ، وذلك من خلال الدور الذي تؤديه في مختلف القطاعات وتوفير تقنيات حديثة تواكب تطورات العصر التكنولوجي الحالي ومجابهة مستخدمي القوة السيبرانية.

فرضية البحث :

ينطلق البحث من فرضية مفادها أن الأمن السيبراني أصبح جزء مهم في استراتيجيات أي دولة في العالم ولاسيما العراق موضوع بحثنا ، لذلك يجب أن تعمل كل الدول على زيادة جهودها لضمان كل تحدياته وانعكاساته السلبية والايجابية للحفاظ على قوة الدولة واستقرارها .

مناهج البحث :

تم الاعتماد على مناهج تجمع بين كل من المنهج الوصفي والمنهج التحليلي عن طريق وصف الظاهرة ومن ثم العمل على تحليلها وفق مؤشرات تطبيقية وعلمية.

المبحث الأول: الأمن السيبراني وعلاقته بتطور وقوة الدولة

يشهد العالم أنتشار في تكنولوجيا المعلومات، ومن ذلك أصبح للخطر الإلكتروني تحدي وتهديد واضح ومؤثر في أمن واستقرار الدولة وأصبح يشكل أحد أشكال وأدوات قوتها، كما وأصبح هناك حاجة ضرورية تعمل عليها جميع الدول وهي الوصول الى استراتيجيات فعالة ومتطورة تضمن درء الاخطار الإلكترونية والاستفادة من مزاياها ، ومن ذلك سنتناول في هذا المبحث ثلاث مطالب كالآتي :

المطلب الاول: مفهوم الامن السيبراني

ظهر مفهوم الأمن السيبراني بعد الحرب الباردة استجابة للمزيد من الابتكارات التكنولوجية والظروف الجيوسياسية المتغيرة، وقد تم استخدامه لأول مرة من قبل علماء الكمبيوتر في أوائل التسعينات للتأكيد على سلسلة من حالات عدم الأمان المرتبطة بأجهزة الكمبيوتر، لكنه تجاوز مفهومه التقني لأمن الكمبيوتر عندما حث المؤيدين على أن التهديدات الناشئة عن التقنيات الرقمية من الممكن أن يكون لها عدة آثار اجتماعية مدمرة[1].

تطلق كلمة سيبراني (cyber) على كل ما يتعلق بالشبكات الإلكترونية الحاسوبية، وشبكة الإنترنت، والفضاء السيبراني، والفضاء الإلكتروني (Cyber space) ، والأخير يعني كل ما يتعلق بشبكات الحاسوب، والإنترنت، والتطبيقات المختلفة وكل الخدمات التي تقوم بتنفيذها كتحويل الأموال عبر النت، أو الشراء أون لاين وغيرها من الخدمات في جميع مجالات الحياة على مستوى العالم[2].

وأن مصطلح الأمن السيبراني شامل يطلق على (أمن المعلومات) شبكة الأنترنت، و (أمن العمليات الإلكترونية)، (وأمن الشبكات) ، (وأمن التطبيقات)، والذي هو عبارة عن خطوات دفاع عن البيانات والمعلومات على جميع الأجهزة الإلكترونية المرتبطة بشبكة الأنترنت من الهجمات الضارة، وعمليات القرصنة وسرقة البيانات، والتخريب، والوصول للمعلومات الحساسة، أو الشخصية لتغييرها أو تدميرها، لأغراض متعددة ومنها الاستيلاء على المال من المستخدمين وغيرها، ويطبق الأمن السيبراني في جميع العلميات والتطبيقات الإلكترونية من المواقع على شبكة الأنترنت التي تخص الأفراد العاديين أو الدولة، الى المصارف والحسابات البنكية، الى عمليات الأقمار الصناعية والعلميات العسكرية [3].

وبحسب (الاتحاد الدولي للاتصالات) في تقريره حول (اتجاهات الإصلاح في الاتصالات للعام2010-2011) فإن الأمن السيبراني هو: " مجموعة من المهمات مثل تجميع وسائل، وسياسات وإجراءات أمنية، ومبادئ يمكن استخدامها لحماية البيئة السيبرانية، وتهدف الحماية إلى جعل المعتدون يعدلون عن خططهم أو منعهم من تنفيذها عبر وضع خطة تتلاءم مع المحيط التقني والبشري والتنظيمي والقانوني للأفراد والمؤسسات"[4].

وقدمت (وزارة الدفاع الأمريكية) تعريف دقيق للأمن السيبراني وعدته: بأنه " جميع الاجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها الإلكترونية والمادية ومن مختلف الجرائم، الهجمات، التخريب، التجسس، والحوادث " [5].

وهناك تعريف للأمن السيبراني للكاتبان(Pekka & Martti): ويشيران بأنه " مجموعة إجراءات اتخذت في الدفاع ضد الهجمات التي تتعرض لها من قراصنة الكمبيوتر وعواقبها، ويتضمن تنفيذ التدابير المضادة المطلوبة"[6].

كما وعرفت (المنظمة الدولية للتوحيد القياسي) الأمن السيبراني أو أمن الفضاء الإلكتروني بأنه: " الحفاظ على سرية وسلامة وتوافر المعلومات في الفضاء السيبراني، كما

وعرف الفضاء السيبراني على أنه: " البيئة المعقدة الناتجة عن تفاعل الأشخاص والبرامج والخدمات على الإنترنت عن طريق تقنية الأجهزة والشبكات المتصلة به والتي لا وجود لها في أي منها شكل مادي"[7].

وعليه فالأمن السيبراني ما هو إلا آلية دفاع لخلق حماية فعالة من أي تهديدات ناشئة من الأجهزة والأنظمة الإلكترونية المتصلة بالإنترنت، ووضع إجراءات ومعايير لازمة لمواجهة هذه التهديدات، ويعد الأمن السيبراني اليوم شكل من أشكال الأمن القومي.

المطلب الثاني: أبعاد الأمن السيبراني

يتضمن الأمن السيبراني أبعاد متعددة وتشمل عدة جوانب العسكرية، السياسية، الاقتصادية، الاجتماعية، والإنسانية، والهدف من ذلك تحقيق منظمة أمنية متكاملة تعمل على الحفاظ على الأمن الوطني للدولة من أي تهديدات سيبرانية محتملة، وعليه سوف نوضح هذه الأبعاد بالآتي:

1- **البعد العسكري**: يتجلى هذا البعد في الحفاظ على قدرة الوحدات العسكرية على التواصل عبر الشبكات العسكرية، مما يؤدي بالسماح بتبادل المعلومات والأوامر وتدفقها وهذه هي الفكرة الأساسية التي طورت بسببها الشبكات والانترنت وذلك لإصابة الأهداف عن بعد، إلا أنها في الوقت ذاته تمثل نقطة ضعف، خصوصاً إذا لم تؤمن جيداً من الاختراق الذي قد يؤدي إلى تدمير قواعد البيانات العسكرية، أو قطع الاتصالات بين القيادة والوحدات العسكرية، بالإضافة الى إمكانية التحكم في بعض الأسلحة وخروجها عن السيطرة مثل الطائرات بدون طيار، والصواريخ الموجهة ضد أقمار صناعية [8] ، ويعد فايروس (ستاكسنت Stuxnet) بداية لاستخدام القوة السيبرانية لتدمير البنية المادية إذ هاجم حواسيب أجهزة الطرد المركزي الإيرانية والذي تم زرعه داخل المفاعل في منتصف عام (2008) [9].

2- **البعد السياسي:** يتسبب البعد السياسي في مشاكل متعددة في العلاقات بين الدول لذا من الضروري إعادة النظر من قبل الدول في سياساتها الخارجية ومثال على ذلك التسريبات المختلفة للوثائق الحساسة والاختراقات التي غالبًا ما تؤدي إلى أزمات دبلوماسية بين الدول ، والدور البارز للشبكات الاجتماعية في تحقيق الأهداف

السياسية مثل نشر رسائل سياسية على شبكات التواصل الاجتماعي ، وتنظيم المظاهرات الافتراضية وحركات الاحتجاج الإلكترونية ، وعمل كمجال فعال للحملات الانتخابية والدعاية لمختلف الفاعلين الدوليين، بالإضافة الى أن الجماعات الإرهابية تستخدم المواقع الإلكترونية والإنترنت من أجل تحقيق العديد من الأهداف، مثل نشر الأفكار، وتعبئة الموارد المالية، وتنسيق الهجمات الإرهابية، وتجنيد المتعاطفين[10]، كما ويعد التدخل الروسي السيبراني في الانتخابات الأمريكية أبرز دليل على ضرورة وأهمية الأمن السيبراني في بعده السياسي، لذا يستوجب على الدول العمل على حماية أمنها الداخلي من هذه التهديدات [11].

3- **البعد الاقتصادي**: يعد الأمن السيبراني في المجال الاقتصادي مجال فعال وأساسي، إذ أن الأنترنت أساسي للمعاملات التجارية والمالية والاقتصادية وأصبح يشكل محور رئيسي للتطور الاقتصادي، إذ تساعد الحواسيب في تسيير وتطوير الصناعات وتحريك الاقتصاد، وأصبح الكل مترابطاً عبر شبكات الكمبيوتر بقطاعات المجتمع كافة سواءً أفراد أو جماعات، كما وأزداد الاعتماد على التكنولوجيا الرقمية في تخزين البيانات والمعلومات، كما وأصبحت المعاملات المالية والاقتصادية جميعها محوسبة، وشبكات البنوك والبورصات وشركات الأسواق المالية مرتبطة ببعضها البعض بنظم وشبكات إلكترونية[12].

4- **البعد الاجتماعي**: يفوق مستخدمي الأنترنت (4 مليارات) شخص في العالم، وأكثر من(2,6 مليار) شخص يستخدمون مواقع التواصل الاجتماعي، مما يجعلها أكبر تجمع للتفاعل والتواجد البشري، مما يفتح آفاق واسعة لتبادل الأفكار والخبرات الجيدة، لكن في المقابل يعرض أخلاقيات المجتمع للخطر، وذلك لصعوبة مراقبة محتوى الأنترنت، كما ويعرض الهويات لعمليات اختراق خارجي قد تتسبب في تهديد السلم الاجتماعي للدولة ، لذلك من الضروري توعية جميع المستخدمين لشبكات المعلومات الدولية بأهمية الفهم الصحيح للأمن، والخطوات الأساسية لتعزيز مستوى الأمن إذا تمت صياغة هذه الخطوات بوضوح وتحديدها وتنفيذها بحكمة، ويتطلب ذلك حملات إعلامية وتربية مدنية تواجه التحديات والمخاطر، وتدابير أمنية وقائية ورادعة من أجل تثقيف جميع المواطنين، بالإضافة الى التأكيد على الالتزامات

الأمنية والمسؤولية الشخصية وتدابير الردع، وعواقب القانون المحتملة لعدم الامتثال للالتزامات الأمنية بشكل عام فهناك حاجة لتوفير التعليم والتدريب في مجال تكنولوجيا المعلومات والاتصالات، وليس فقط في تدابير الأمن والردع، كما ويجب غرس ثقافة الأمن في ثقافة تكنولوجيا المعلومات، ومن الضروري تطوير مجموعة من الأخلاقيات الأمنية التي يتم قبولها واحترامها من قبل جميع العاملين في الفضاء السيبراني[13] .

5- **البعد القانون**: توجد هناك علاقة متبادلة بين القانون والتكنولوجيا إذ أن التطورات التكنولوجية المتسارعة تتطلب مواكبة التشريعات القانونية لها، من خلال وضع أطر وتشريعات للأعمال القانونية وغير القانونية في الفضاء السيبراني، ولكن بشكل عام فإن الجريمة السيبرانية تفتقد في معظم البلدان الى الأطر القانونية الصارمة للتعامل معها، وذلك بسبب عوامل مثل طبيعة هذه الجرائم نفسها، وصعوبة تحديد مرتكبي هذه الجرائم، ومرونة التعريفات المتعلقة بتكنولوجيا المعلومات، فإن الجريمة السيبرانية لا تعرف حدوداً وطنية، إضافة إلى الأمر الذي يتطلب تفعيل تعاون دولي مشترك لمكافحتها [14].

المطلب الثالث: أهمية الأمن السيبراني وعلاقته في تطور قوة الدولة

نتيجة لثورة التكنولوجيا والاتصالات وظهور الفضاء الإلكتروني ازدادت العلاقة بين الأمن والتكنولوجيا، وطرأت تحولات جديدة على مفهوم القوة وظهور ما يسمى (بالقوة الالكترونية) والتي تم إلى توزيعها بين عدد أكبر من الفاعلين من غير الدول بعد أن كانت الأخيرة هي المحتكر الوحيد للقوة، وحدد (جوزيف.س ناي) ثلاثة أنواع من الفاعلين الذين يمتلكون القوة السيبرانية وهم : أولا : الدولة والتي تكون لديها قدرة كبيرة على تفيذ هجمات سيبرانية وتطوير البنية التحتية وممارسة السلطات داخل حدودها ، وثانياً : الفاعلين من غير الدول وهم الذين يستخدمون القوة السيبرانية لأغراض هجومية أساساً، إلا أن قدرتهم على تنفيذ أي هجوم مؤثر تتطلب مشاركة ومساعدة أجهزة استخباراتية متطورة، ولكن يمكنهم اختراق المواقع الإلكترونية واستهداف الأنظمة الدفاعية. ومنهم الشركات متعددة الجنسيات، والمنظمات الإجرامية، والجماعات الارهابية، وثالثا: الأفراد الذين يمتلكون معرفة تكنولوجية

عالية والقدرة على توظيفها عادة ما تكون هناك صعوبة في الكشف عن هوياتهم، وصعوبة ملاحقتهم[15]، كما ظهرت أنماط لاستخدام موارد القوة الالكترونية أو الافتراضية، وميز بين الاستخدام الناعم لها والاستخدام الصلب، وقد أثر ذلك بدوره على سيادة الدول وبخاصة مع بروز دور الشركات التكنولوجية العابرة للحدود، وبروز أخطار القرصنة والجريمة السيبرانية، والجماعات الإرهابية[16]، أن الدول وكما نعلم تستخدم الفضاء الإلكتروني لاعتبارات الأمن والقوة العسكرية بشكل جعل عديدًا من الدول تدخل الفضاء الإلكتروني ضمن حسابتها الاستراتيجية وأمنها القومي، لذا فإن للأمن السيبراني أثره في قوة الدولة من خلال القوة الافتراضية والتي تعرف القدرة على الحصول على النتائج المرجوة من خلال مصادر المعلومات المرتبطة الكترونياً بالميدان المعلوماتي وذلك عبر أدوات القوة المختلفة، سواءً كانت عسكرية، أو اقتصادية، أو دبلوماسية، أو معلوماتية، وكذلك تعدد شكل علاقات القوى وظهور ما يسمى (علاقات القوى الافتراضية)[17]، ومن ذلك فإن الأمن السيبراني يعد ساحة عالمية واسعة وعابرة لحدود الدول والذي يمتد من داخل الدولة إلى نظام دولي ويشكل نوع من أنواع الأمن العالمي، ولاسيما عند وجود تهديد لجميع الفواعل الدولية وغير الدولية، وأهتم بوضع الإجراءات والمعايير التي تعرقل وصول المعلومات والبيانات إلى أشخاص غير شرعيين أو قانونيين ، لذلك أصبح هنالك مصالح للحفاظ على أمن الفضاء السيبراني الذي يكون جزء من الأمن العالمي ولاسيما عند تطور القدرات البشرية في انتاج تقنيات حديثة وتصاعد مخاطر التهديدات الإلكترونية على البنى التحتية للاتصال والمعلومات[18].

مما يعني بأن الأمن السيبراني هو مجال آخر لاستعراض القوى وممارسة النفوذ وتحقيق التفوق والتنافس الدولي بين الدول، إذ لا تحتاج الدولة الى جعل المزيد من الأراضي تحت سيطرتها، أو تمتلك الأسلحة التقليدية وأسلحة الدمار الشامل هي المعيار الأساسي لقياس قوة الدولة بعد ظهور الثورة المعلوماتية[19]، إذ يستطيع أحد أطراف الصراع أن يوقع خسائر فادحة ويتسبب في شل البنية المعلوماتية والاتصالية للطرف المستهدف عن طريق أسلحة وقدرات تكنولوجية وعسكرية كبرامج التجسس والفيروسات، أي أسلحة بأنواع جديدة تفضي الى أحراز النصر وكسب المعركة متجاوزة الفواعل، والحدود الجغرافية والتقليل من الخسائر المادية والبشرية، وبالتالي أضحى المفهوم الجديد للأمن يدور في فلك الحفاظ على سلامة الدولة في ظل تلك التطورات التكنولوجية ومن هنا أصبح الصراع الجديد يعنى بكل ما من شأنه

التنافس والترابط التكنولوجي وارتباط شكله وأنماطه في عصر المعلومات بمعرفة من يعرف؟ وأين؟ ولماذا؟ [20] .

لذلك فإن العلاقة بين الأمن السيبراني وقوة الدولة تزداد كلما زاد نقل المحتوى المعلوماتي والعسكري والأمني والفكري والسياسي والاجتماعي والاقتصادي والخدمي والعلمي والبحثي إلى الفضاء السيبراني، خاصة مع التسارع في تبني الحكومات الإلكترونية والمدن الذكية في العديد من الدول، واتساع نطاق وعدد مستخدمي الانترنت في العالم، والثورة الكبرى في أنترنت الأشياء، إذ أصبحت قواعد البيانات في حالة انكشاف خارجي، إضافة الى حملات الدعاية والمعلومات المضللة ونشر الشائعات أو الدعوة لأعمال تحريضية أو دعم المعارضة أو الأقليات، مما يساهم في تلاشي سيادة الدولة ويشكك في قدرتها على الحفاظ على أمنها القومي[21]، وكما لاحظنا فإن الأمن السيبراني لم يقتصر على البعد التقني وحسب، بل تجاوزه إلى أبعاد أخرى مثل الأبعاد الثقافية والاجتماعية والاقتصادية والعسكرية وغيرها، وهو ما عمل على دعم حقيقة أن الاستخدام غير السلمي للفضاء السيبراني يؤثر على الرخاء الاقتصادي والاستقرار الاجتماعي لجميع الدول التي أصبحت تعتمد على البنية التحتية الكونية[22].

المبحث الثاني: تحليل موقع العراق في مؤشر الأمن السيبراني

بعد أن دخل تأثير الفضاء السيبراني في مختلف جوانب الحياة الانسانية والاجتماعية والاقتصادية والسياسية والعسكرية، زاد اهتمام الدول بالأمن السيبراني ولأهمية الموضوع فقد أنشأت الأمم المتحدة ومن خلال الاتحاد الدولي للاتصالات والذي هو إحدى وكالاتها المتخصصة والمسؤولة عن الأمور المتعلقة بتكنولوجيا الاتصالات والمعلومات مؤشر خاص بالأمن السيبراني العالمي، ووفقا لذلك سنتحدث بالتفصيل في هذا المبحث عن ذلك عن طريق تقسيمه الى مطلبين كالآتي:

المطلب الأول: مؤشر الأمن السيبراني

أنشأت (الامم المتحدة) ومن خلال مبادرة من (الاتحاد الدولي للاتصالات) (ITU) والذي هو إحدى وكالاتها المتخصصة والمسؤولة عن الأمور المتعلقة بتكنولوجيا الاتصالات والمعلومات مؤشر خاص لحالة الأمن السيبراني للدول عبر أنحاء العالم ويدعى "مؤشر الامن

السيبراني العالمي" (Global Cybersecurity Index) ويشار له بالاختصار (GCI) ، وهو مؤشر مركب وذو فاعلية لقياس مدى التزام الدول بمعايير الأمن السيبراني على المستوى العالمي، ويهدف الى حماية المعلومات والممتلكات من السرقة والفساد، أو الكوارث الطبيعية، ويسمح للمعلومات والممتلكات أن تبقى منتجة وفي متناول مستخدميها المستهدفين، كما يمنح نظرة ثاقبة على مشاركة الدول ذات السيادة في الأمن السيبراني، ويصدر هذا المؤشر وتقريره منذ عام (2015) ويعرض هذا المؤشر والتقرير الخاص به كفاءة دول العالم في الامن السيبراني واجراء مقارنات فيما بينها، ويجمع(25) معياراً في مقياس واحد لرصد التزام(193) دولة عضوا في الاتحاد الدولي للاتصالات بالأمن السيبراني ، وتقسم هذه المعايير على أساس خمسة ركائز متنوعة، وذلك لأن الأمن السيبراني مفهوم يشمل ويتضمن قطاعات واسعة ومتعددة في جميع جوانب الحياة، وأن أسس تقييم البلدان في المؤشر هي كالآتي :

1- التدابير القانونيّة: أن تطبيق مفهوم الأمن السيبراني يتطلب تشريعات وقوانين يجب تشريعها وسنها، مثل الجرائم الإلكترونية التي يتوجب سن عقوبات لملاحقة مرتكبيها.
2- التدابير التقنيّة: تعد التكنولوجيا عامل الدفاع الأول لتحقيق الأمن السيبراني والتصدي للهجمات الإلكترونية، لذلك يجب أن يكون لدى كل الدول إجراءات تكنولوجية لاكتشاف وتحديد الهجمات الإلكترونية وتدابير للرد عليها، ومن هذه التدابير التقنية المهمة والتي يركز عليها المؤشر هي وجود (هيئة متخصصة في مجال الأمن السيبراني) تعمل كمركز وطني أو ما شابه ذلك.
3- التدابير التنظيميّة: وتعد إجراءات ضرورية تنفذها أي دولة في المجال السيبراني، ويتوجب وجود خطة وهدف استراتيجي قابل للتنفيذ لتحقيق متطلبات الأمن السيبراني.
4- تنمية القدرات: وتتم من خلال إعداد القدرات البشريّة والمؤسسيّة، وتعزيز المعرفة والوعي المجتمعي بقضايا الأمن السيبراني، كما وتتضمن تنمية القدرات وتوفير الموارد التي تساعد على إجراء البحوث وبرامج التطوير والتدريب والتعليم في مجالات الأمن السيبراني.

5- التعاون: أن تحقيق الأمن السيبراني إذ يتطلب تعاون مُشترك بين كافة مؤسسات الدولة وقطاعاتها، بالإضافة الى تعزيز الحوار والتنسيق لجعله أكثر شمولاً، ولا تقتصر على المجال المحلي والوطني إنما يجب أن يتوسع هذا التعاون الى العالمي بين الحكومات والدول المختلفة [23].

ويختلف ترتيب الدول في مؤشر الأمن السيبراني العالمي وفقاَ لمدى تحقيقها للركائز المطلوبة لبناء أمن سيبراني، و تظهر نتائج المؤشر تحسناً وتعزيز لجميع الركائز الخمس ، لكن الفجوات الإقليمية في القدرات السيبرانية لا تزال قائمة، ويستند الإصدار الأخير من مؤشر الأمن السيبراني العالمي إلى البيانات عنها بمستوى قياسي لمشاركة الدول الأعضاء من(105) استبيان في نسخة عام(2014-2013) إلى(150) استبياناً في عام(2020) ، وعند معاينة المؤشر نجد بأن دول عربية مثل المملكة العربية السعودية والتي حققت تقدم كبير فيه المؤشر تحتل المرتبة (2) و درجة (99,54) بعد الولايات المتحدة الأمريكية ، ودولة الأمارات العربية المتحدة والتي أحتلت المرتبة(5) بدرجة (98,06)، وسلطنة عمان بالمرتبة (21) وبدرجة (96,04) ، ومصر بمرتبة (23) وبدرجة (95,48) [24] .

ومن أجل الحصول على مجموع نقاط مؤشر الأمن السيبراني لأي دولة وهذه النتائج يستخدم المؤشر البيانات التي يتم جمعها من الدول ووضع أسئلة لتقييم الالتزام، ويتم ترجيح هذه الأسئلة من خلال التشاور مع مجموعة من الخبراء، ويلاحظ من النتائج هذا المؤشر وجود فجوات كبيرة في قدرات توفير وإتاحة الأمن السيبراني على مستوى دول العالم، فمثلا تمتلك الولايات المتحدة الأميركية، والمملكة المتحدة بنى تحتية مختلفة تماماً من حيث القدرة والكفاءة، عن تلك التي تمتلكها دول مثل العراق، ولبنان ، واليمن ، وجيبوتي ، لكن في الوقت ذاته أظهرت دول مجلس التعاون الخليجي بنتائجها في هذا المؤشر أنها تفوقت على العديد من الدول الغربية الأخرى والبلدان الأكثر تقدما منها اقتصادياً ومن حيث القدرات الأمنية السيبرانية واستدامة البنى التحتية البشرية، والتدابير التعاونية لخلق بيئة تقنية أمنة، ووفقاً لكل ذلك أن مؤشر الأمن السيبراني يلخص إلى تحذير وفكرة بأن الأمن السيبراني يتطور باستمرار، وعلى الدول أن تعمل إلى نُهج مستدام ومطور لضمان أن تظل كافة البرامج والحلول الرقمية أمنة وموثوقة [25].

المطلب الثاني: موقع العراق في مؤشر الأمن السيبراني

أن العراق مثل أي دولة في العالم يواجه تحدي الفضاء السيبراني في مختلف مجالاته ومنها المجال الأمني، وأن البلاد وجدت نفسها تدخل في هذا الفضاء الواسع وسريع الحركة من الفضاء الحقيقي إلى الفضاء الافتراضي من دون المرور بمرحلة انتقالية، فالبنى المادية والبشرية في العراق ما زالت غير قادرة على التفاعل والتصدي مع التحديات المتعددة للفضاء السيبراني بصورة جيدة وفعالة، على الرغم من توافر العديد من البنى التحتية الرئيسة من تقانات ومهارات لدى الأجهزة المختصة في العراق ، إذ أعلنت مستشارية الامن الوطني عن (استراتيجية الامن السيبراني العراقي) منذ عام (2017) ، لتوفير التدابير والإجراءات الاستراتيجية لضمان أمن وحماية الوجود في الفضاء السيبراني، وحماية البنية التحتية الحيوية للمعلومات، وبناء ورعاية مجتمع انترنت موثوق فيه في العراق، كما حددت التهديدات السيبرانية الرئيسة الجريمة الإلكترونية، والإرهاب الإلكتروني، والصراع السيبراني، والتجسس السيبراني، الى جانب اساءة معاملة الاطفال واستغلالهم الكترونياً، وشددت الاستراتيجية على ضرورة تقييم مواطن الضعف الوطنية في المجال السيبراني وقياس الاثار والفرص، كما وضعت الاستراتيجية خريطة طريقة من ثماني محاور، متمثلة بالحكومة الفعالة، والاطار التشريعي والتنظيمي، واطار تكنولوجيا الأمن السيبراني، وثقافة الامن السيبراني وبناء القدرات، والبحث والتطوير نحو الاعتماد على الذات، والامتثال والتنفيذ، والجاهزية لحوادث الأمن السيبراني، الى جانب التعاون الدولي، بالإضافة الى ذلك جرى الإعلان عن (فريق وطني مشترك مختص للاستجابة للحوادث السيبرانية وحماية البنية التحتية للأنترنت) يعمل تحت إشراف مستشارية الأمن الوطني العراقي، لنشر الوعي في مجال حماية الخصوصية والحماية الذاتية للأفراد والمؤسسات على الانترنت ، وغيرها من التدابير على الرغم من تحديات التشريعات العراقية النافذة، التي ما زالت لا ترتقي إلى مستوى التحولات الرقمية التي تشهدها المجتمعات المعاصرة، والمخاطر الحديثة التي تواجهها، ومنها ما يرتبط بالأمن السيبراني[26] .

وعند البحث في الامكانيات العراقية في مجال الأمني السيبراني سوف نجد بأن العراق لا يزال يحتاج الكثير من الجهود المعرفية، والادارية، والقانونية ، والتقنية لكي يكون قادر على التأثير في المجال الامني السيبراني ، وقادر على حماية أمنه من التهديدات السيبرانية،

فحالة الضعف التي يعيشها تعد المشكلة الأكبر، إذ لا يزال العراق يعاني من عدم الاستقرار العام، وما يؤكد على ذلك هو مكانته وترتيبه في مقياس مؤشر الأمن السيبراني العالمي الذي يعتمد في قياسه على خمسة ركائز للأمن و تحليل ثمانون مؤشر فرعي ، ينظر الجدول رقم (1) التالي :

جدول رقم (1)

ترتيب العراق في مؤشر الأمن السيبراني

الدولة	التقييم في عام 2017	التقييم في عام 2018	التقييم في عام 2020
العراق	مرتبة **(158)** عالمياً مرتبة **(19)** عربياً	مرتبة **(107)** عالمياً مرتبة **(13)** عربياً	مرتبة **(129)** عالمياً مرتبة **(17)** عربياً

المصدر : من أعداد الباحثة بالاعتماد على تقارير مختلفة :

Global Cybersecurity Index, International Telecommunication Union DevelopmentSector, Publications on: https://www.itu.int/en/ITUD/Cybersecurity/Pages/global-cybersecurity-index.aspx

يلاحظ من الجدول أعلاه أن العراق وعلى الرغم من التحسن الذي حدث في موقعه في المؤشر لعام (2018) وحصوله على (107) عالمياً و(13) محلياً، بعد ان كان في عام(2017) في المرتبة (158) عالميا و(19) محلياً ، لكن وبحسب أخر احصائية عام (2020) للمؤشر تراجع العراق (22) مرتبة عالمياً و (4) مراتب عربيا ، أذ حصل فيها على المرتبة(129) عالميا في المؤشر من اصل(193) دولة، حصل على المرتبة(17) عربياً وأنه متقدماً على كل من دولة موريتانيا والصومال، وجزر القمر، وجيبوتي، واليمن، بينما تصدرت عليه بقية الدول العربية بما فيها سوريا، ولبنان، وفلسطين، وليبيا، والسودان[27]

وأشار مركز الاعلام الرقمي (DMC) سبب التراجع هو : " أن العراق لم يقدم اجابات عن الاستبيان الذي جمعه فريق المؤشر والذي تضمن بعض المعلومات والبيانات، وهو الامر الذي يطرح عدة اسئلة حول سبب هذا التجاهل للجهات المسؤولة عن هذا ملف الامن السيبراني في العراق" ، وتشير بعض الدراسات ان هذا التراجع في الملف الامني السيبراني إنما يعود إلى عدم وجود مؤسسة متخصصة بالأمن السيبراني في العراق(وما هو موجود عبارة عن أقسام في دوائر مختلفة تفتقد للتنسيق أو التعاون المحترف في هذا الجانب، وكل جهة منها تعمل بمفردها)[28].

المبحث الثالث: تحديات الأمن السيبراني في العراق: استراتيجيات للمعالجة ورؤية المستقبل

أن السباق العلمي والمعلوماتي في مجال ثورة التكنولوجيا والمعلومات، يتطلب منا ان نواكب هذه التطورات بسرعة وفاعلية، حتى نحقق السيطرة والنجاح بالتصدي لجميع التحديات السيبرانية التي تهدد أمن العراق واستقرار وقوة الدولة فيه، وفي الوقت ذاته العمل على امتلاك تقنية الامن السيبراني والتي بدورها تشكل أحد الحلول الناجحة للتصدي لمشاكل الدولة وزيادة قوتها، ووفقاً لذلك سنقسم هذا المبحث الى ثلاث مطالب كالاتي:

المطلب الأول: تحديات الامن السيبراني في العراق

أن تسارع العصر الرقمي وتقدمه يعرض البلاد الى تحديات متعددة وذلك لارتباط الأمن السيبراني في جميع المجالات وأن أهم التحديات التي تواجه الأمن السيبراني في العراق تتضمن عدة جوانب، وهي كالاتي:

1- **تحديات في مجال تشريعات الأمن السيبراني** : إذ يعاني العراق من ضعف القوانين والتشريعات الحكومية التي تنظم الأمن السيبراني والمعلوماتي ، وأنها لا تزال غير كافية وغير متكاملة، ويحتاج العراق إلى تشريعات أكثر شمول وصرامة في تطبيقها لحماية النظام السيبراني ومكافحة الجرائم السيبرانية [29].

2- **التحديات السياسية والاقتصادية**: أدت السنوات الماضية من عدم الاستقرار والعنف السياسي في العراق إلى عدم إعطاء الأولوية لتنظيم المجال السيبراني وتعامل الحكومة معه، كما وان الوضع السياسي والاقتصادي المتقلب في العراق يؤثر على قدرة الحكومة في تخصيص الموارد والجهود اللازمة لتعزيز الأمن السيبراني وتحسين البنية التحتية التقنية.

3- **التحديات التكنولوجية:** على الرغم من التطور التكنولوجي السريع في العالم، إلا أن العراق لا يزال يعاني من نقص في البنية التحتية التكنولوجية اللازمة لتأمين النظام السيبراني، وأن الحكومة والمؤسسات مازالت تواجه صعوبة في تطوير وتحديث أنظمتها السيبرانية وتأمينها بشكل فعال.

4- **ارتباط منظومات الانترنت في العراق بالخارج:** وفقاً لذلك أن الأمن السيبراني العراقي مرتبط بدول وشركات خارجية، وهذا يتطلب من الحكومة العراقية إنشاء

شراكة فعالة مع شركات محلية لإقامة علاقات موثوق بها وفعالة لسد النقص في هذا المجال.

5- **قلة صرف الأموال المخصصة للأمن السيبراني** فهي قليلة بالمقارنة مع دول الجوار[30].

6- **ضعف البنية التحتية السيبرانية:** يعاني العراق من ضعف في البنية التحتية التقنية والأمنية، ونقص الكفاءات الفنية والموارد البشرية المتخصصة في مجال الأمن السيبراني، مما يجعله أكثر عرضة للاختراقات والهجمات السيبرانية، التي تستهدف البنية التحتية التقنية والمؤسسات الحكومية والشركات الخاصة. والتي من الصعب التصدي لها بشكل فعال ، مما يؤثر على الأمن الوطني والاقتصادي في العراق.

7- **نقص الوعي السيبراني لدى المواطنين والمؤسسات:** على الرغم من أهمية الأمن السيبراني، إلا أن الوعي به لا يزال ضعيفًا في العراق مما يؤدي الى زيادة تعرض البلاد للتهديدات السيبرانية ويجعلها أكثر عرضة للاختراقات والاحتيال الإلكتروني، يعود ذلك إلى عدم توفر البرامج التثقيفية والتوعوية الكافية للمواطنين والمؤسسات بشأن أهمية الأمن السيبراني وكيفية حماية أنفسهم ومصالحهم الحيوية قلة عدد المؤتمرات وورش العمل والندوات عن الأمن السيبراني تزال محدودة جداً بالمقارنة مع دول الجوار ، وعدم تواجد العراق في المنتديات العالمية المعنية بالأمن السيبراني [31].

المطلب الثاني: استراتيجيات المعالجة

إن تحقيق الأمن السيبراني في العراق يتوجب اعطاءه أولوية عالية، ويتطلب جهودًا متكاملة وشاملة متعددة الأبعاد من الحكومة والمؤسسات والمواطنين لضمان استقرار الدولة وتطورها، لذا يجب تبني هذه المعالجات والتي وضعناها وفقاً للتحديات التي تواجه الأمن السيبراني في العراق وهي كالاتي :

1- **تطوير السياسات والتشريعات:** يجب العمل على تطوير السياسات الخاصة بالامن السيبراني، وتوفير الإطار القانوني والتنظيمي اللازم لمكافحة التهديدات السيبرانية بفعالية اكبر وذلك من خلال التخطيط لنظام تشريعي وقانوني وقضائي محكم في مجال الأمن السيبراني وتوفير معايير ولوائح وطنية للأمن السيبراني في كل من

القطاعين العام والخاص، وخلق بيئة قانونية تمكينية للمؤسسات وتحديد عقوبات لملاحقة الجرائم السيبرانية مع ضمان الحريات المدنية, والعراق يفتقر إلى الآن لقانون الجرائم المعلوماتية، سوف تستمر المخاوف من الجرائم السيبرانية في النمو مع استمرار سكان البلاد في الوصول إلى شبكة الإنترنت ، وأن قوانين العقوبات والمدنية العراقية تحتاج الى تطوير وتفعيل ويجب أن تتضمن التشريعات العراقية المتعلقة بالفضاء الإلكتروني لوائح ومعايير يمكن للقطاعين العام والخاص الاعتماد عليها، يمكن الاستفادة من التجارب للدول الناجحة من خلال إجراء دراسة شاملة لكل من النجاحات والإخفاقات التي شهدتها البلدان والسلطات القضائية الأخرى هو جهد غير مكلف نسبيًا من شأنه أن يمكّن القضاء العراقي ويساعده على وضع تشريعات متعمقة تكون محدثة ومتكيفة مع سياقها واهتماماتها الخاصة[32].

2- **تطوير استراتيجية وطنية للأمن السيبراني**: يجب وضع استراتيجية وطنية شاملة للأمن السيبراني تحدد الأهداف والسياسات والخطط العملية لتعزيز الأمن السيبراني في العراق، إذ يمكن تحقيق تقدم في مجال الأمن السيبراني وتعزيز حماية البنية التحتية الرقمية والبيانات والمعلومات الحساسة، وإنشاء وكالة سيبرانية وطنية عراقية مخصصة يتم بموجبها تنفيذ السياسات السيبرانية، تكون مسؤولة عن التثقيف والتوعية السيبرانية وأمن المعلومات والدفاع عن الفضاء السيبراني الوطني العراقي مما يساهم في تعزيز الاستقرار والتنمية المستدامة [33].

3- **تطوير البنية التحتية السيبرانية**: يجب تعزيز البنية التحتية التقنية والأمنية في العراق من خلال استثمارات في البنية التحتية الرقمية، وتحديث الأنظمة والتقنيات لتلبية متطلبات الأمن السيبراني، باستخدام أفضل الوسائل التكنولوجية، من أجل مقاومة الاختراقات والتخريب، وضرورة الاطلاع على أفضل الطرق لحماية الأمن الدولة بشموليته، وحماية البنية المعلوماتية، بالإضافة الى تعزيز القدرات البشرية من خلال تطوير القدرات الفنية والتدريبية وتوفير التدريب والتعليم للموظفين والمختصين في مجال الأمن السيبراني.

4- **تعزيز التعاون الدولي والاقليمي والدخول في المعاهدات والاتفاقيات متعددة الجنسيات** المتعلقة بالأمن السيبراني أمر بالغ الأهمية أذ تشكل محركاً لتنمية القدرات،

لذا يجب على العراق أن يعمل ويتعاون مع الدول والهيئات الدولية على تبادل المعلومات لمواجهة التحديات السيبرانية التي تتعرض لها المؤسسات ، فإقليميا عن طريق التعاون مع عدد من الدول الاقليمية ذات التجارب الناجحة في تحقيق الأمن السيبراني ومثال على ذلك المملكة العربية السعودية التي عملت على حماية أمنها السيبراني عبر انشاء (الهيئة السعودية للأمن السيبراني) والتي جعلت من البلاد ان تحتل المرتبة (13) عالميا في مؤشر الامن السيبراني لعام(٢٠١٨)، المرتبة (2) عالمياً ضمن تقرير عام(2023) الصادر عن مركز التنافسية العالمي التابع للمعهد الدولي للتنمية الإدارية في سويسرا (IMD)، الهادف إلى تحليل وترتيب قدرة الدول على إيجاد بيئة داعمة ومحفزة للتنافسية والمحافظة عليها وتطويرها[34]، ومن بين هذه الهيئات هو (الاتحاد الدولي للاتصالات) الذي يخصص جزء أساسي من برامجه وخطط عمله لتحقيق الامن السيبراني ، وكذلك يمكن للعراق التعاون مع(المجلس الأوروبي) والذي اقر معاهدة مكافحة الجريمة السيبرانية، التي دخلت حيز التنفيذ عام (٢٠٠٤) داعيا جميع الدول الى التوقيع عليها، منذ تاريخ اقرارها في العام(٢٠٠١) وتعد احكام هذه المعاهدة، منسجمة مع متطلبات مكافحة الجريمة السيبرانية، لاسيما وانها تطلب من الدول الاعضاء، انشاء مراكز اتصال، تعمل بحسب مبدأ استمرارية الخدمة اي بمعنى تأمين متابعة على مدار الساعات، أذ تكون دائمة الاستعداد، للتجاوب مع الطلبات القادمة من خارج الحدود الجغرافية، وللتعاون مع القوات المعنية بمكافحة الجريمة، بسرعة وفعالية عالية [35].

5- **بناء نظام بيئي متكامل وجيد التنظيم وفعال للغاية للأمن السيبراني:** على الرغم من التحديات السياسية والاقتصادية في البلاد ، يجب الأخذ بنظر الاعتبار أن سيادة الفضاء الإلكتروني والأمن السيبراني عاملاً متزايد الأهمية في ضمان الرخاء والاستقرار المطلوبين ، ومما تجب الإشارة إليه أن مؤشر الأمن السيبراني التابع للاتحاد الدولي للاتصالات يمنح العراق درجة إجمالية قدرها(20,71) بذلك يحتل مرتبة متوسطة مقارنة بالدول الأخرى في المنطقة، وكما إن العراق يعد رابع أكبر اقتصاد في العالم العربي، وسادس أكبر اقتصاد في المنطقة، قادر تمامًا على بناء نظام بيئي متكامل، وبالنظر إلى توصيات الاتحاد الدولي للاتصالات ومقارنتها بواقع البنية

الحالية وحالة الأمن السيبراني في العراق، يمكن رسم خارطة طريق واضحة للدولة لتعزيز قدراتها ودفاعها وسيادتها بشكل مناسب متجاوزة كل التحديات والظروف الاقتصادية والسياسية التي تمر بها البلاد.

6- **التوعية والتثقيف**: ويتم ذلك عبر تعزيز الوعي الأمني بين أفراد المجتمع والمؤسسات من خلال حملات توعية وثقيفية حول المخاطر المتعلقة بالإنترنت وأهمية الأمن السيبراني وكيفية الوقاية من الهجمات السيبرانية والتصدي لها ، ويتم ذلك من خلال الورش والندوات التثقيفية ، والقيام بالمؤتمرات واللقاءات، والعمل على دعوة الباحثين والمشاركين المختصين المحليين والدوليين للاستفادة من خبراتهم، وتشجيع المؤسسات على إطلاق برامج حول الأمن السيبراني، ودعم الأبحاث في المؤسسات الأكاديمية، وتنشيط تشجيع الطلاب على الدخول في مجال الأمن السيبراني.

7- **وأخيراً** يحتاج العراق إلى زيادة استثماراته في استراتيجيته وسياساته السيبرانية ، وعلى سبيل المثال خصصت إيران مليار دولار سنوياً لذلك، والتي يبلغ نصيب الفرد من الناتج المحلي الإجمالي فيها نصف ما في العراق، وهي ميزانية تفوق المخصصات السيبرانية للعراق(36).

المطلب الثالث: مستقبل الأمن السيبراني في العراق

أن الأمن السيبراني عامل تمكين ومحرك رئيسي للتحول الرقمي والتنمية في العراق ، لذلك يجب اغتنام هذه الفرصة واتخاذ إجراءات مناسبة لتعزيزه من خلال بناء نظام بيئي مفتوح والتعاون مع أصحاب الاختصاص المحليين الشركاء الإقليميين والدوليين لكي يستثمر فوائد وفرص العصر الرقمي وتحقيق إمكاناته الكاملة، وأن الأمن السيبراني وكما لاحظنا لا يتعلق بالتكنولوجيا فحسب بل بجميع بالأفراد وفي كافة مجالات الحياة ، ووفقا لكل المعطيات والواقع للأمن السيبراني في العراق وتحدياته يظهر لنا بعض السيناريوهات المستقبلية والمتمثلة بالاتي(37):

1- احتمال زيادة التهديدات السيبرانية الدولية من قبل دول أو جماعات ذات مصالح متعددة مع العراق ولأسباب عديدة سواءً سياسية أو اقتصادية أو استخباراتية.

2- احتمال زيادة التهديدات السيبرانية المرتبطة بالاحتيال المالي، أو السرقة الإلكترونية وذلك بسبب الظروف الاقتصادية والاجتماعية الغير مستقرة في العراق مما يؤدي الى زيادة الاختراقات التي تهدف إلى التأثير على الاستقرار الاقتصادي والاجتماعي في البلاد.

3- احتمال زيادة خطر وقوع هجمات سيبرانية مستهدفة بسبب التوترات الإقليمية والصراعات المستمرة في المنطقة ، مما قد تنعكس على الأمن السيبراني في العراق.

4- احتمال تعزيز القدرة السيبرانية الحكومية وتطور قدرات الهجمات السيبرانية المحلية ربما تستثمر الحكومة في العراق تطوير القدرة السيبرانية بشكل متزايد وذلك لمواجهة كل التهديدات السيبرانية المستقبلية التي يتعرض لها العراق، بالإضافة الى أنه قد تشهد البلاد تطورات في القدرة السيبرانية المنفردة أو للمنظمات أو المجموعات المحلية لأغراض متعددة سياسية أو اقتصادية أو اجتماعية مما يعزز قدرات البلاد بشكل أكبر.

5- احتمال زيادة وتطور التعاون الدولي للعراق في مجال الأمن السيبراني مع الدول والمنظمات الدولية مما يساعد على تعزيز قدرات البلاد على مواجهة التهديدات السيبرانية والتصدي لها.

أن جميع هذه السيناريوهات تبرز من التحديات المتنوعة والفرص المحتملة المستقبلية للأمن السيبراني في العراق ، وتؤكد لنا ضرورة تبني استراتيجيات فعالة لتعزيز القدرة على التصدي للتهديدات السيبرانية المتزايدة .

الخاتمة :

أصبح الامن السيبراني جزء من أمن واستقرار الدولة و يعد مطلب أساسي لجميع الدول وبما فيها العراق وتسعى لتحقيقه ، ولا تكمن القوة السيبرانية في وجود عناصرها فقط أنما في طريقة استثمارها وتوظيفها لزيادة قوة وتطور الدولة ، لذلك يمكننا القول أن الأمن السيبراني فرصة حقيقية لقوة الدولة رغم تحدياته ومخاطره ، وعلى الرغم من تواضع أمكانيات العراق بهذا المجال، بسبب العديد والأزمات السياسية التي مرت بها البلاد، أذ لا يزال جزءا من منظومة أمنية اقل تطورا من البلدان اخرى في بقية بلدان العالم المتقدمة ، أذ يعاني العراق

من خلل في تبني أسس واضحة في كيفية التعامل مع التقنيات الحديثة ، وكيفية استثمار، وأن الية التواصل التقني والمعلوماتي لاستلام المعلومة الأمنية ضعيف ، ولا يتلاءم مع الحاجة الملحة للتسارع الرقمي مع الدول المتقدمة وشعوبها في البحث عن الأمن والاستقرار، مما يجعله دول ضعيفة تقنياً ، لذلك تحتاج البلاد لإيجاد أسس جديدة في إدارة الدولة وتعزيز أمنها، والعمل على إعادة النظر في البنى التحتية للمؤسسات في العراق، وبناء إستراتيجية أمنية رفيعة المستوى قد ينقل البلاد إلى مرحلة متقدمة من الأمن السيبراني تمكنه من مواجهة التحديات المستقبلية والاستمرار في التطور، لذلك فإن مستقبل الأمن السيبراني في العراق يواجه تحديات وفرصاً متنوعة.

المصادر والمراجع:

[1] تغريد معين حسن، الاثر العسكري للأمن السيبراني في الجغرافيا السياسية للدولة ، مجلة البحوث الجغرافية العدد (30) ، (العراق : 2019) ، ص240.

[2] منى عبد الله السمحان ، متطلبات تحقيق الامن السيبراني لأنظمة المعلومات الادارية بجامعة الملك سعود ، مجلة كلية التربية ، جامعة المنصورة ، العدد (111) ، (مصر : 2022) ، ص9.

[3] سالي سعد محمد ، الامن السيبراني ودور الجامعات في تعزيزه لدى الطلبة ، مركز حمورابي للبحوث والدراسات الاستراتيجية ،(العراق: 2022) ، ص2.

[4] سليم دحماني ، أثر التهديدات السيبرانية على الامن القومي الولايات المتحدة الامريكية أنموذجا (2001-2007) ، مذكرة ماجستير مقدمة الى كلية الحقوق والعلوم السياسية ، جامعة محمد بوضياف المسيلة ، الجزائر ، 2018، ص32-33

[5] Syed Rubab- Ahmed Awais - Muhammad Yasin, CyberSecurity: Where Does Pakistan Stand ?, (Sustainable Development Policy Institute, 2019) p2 .on http://www.jstor.org/stable/resrep243, (26/3/2024).

[6] ميار عادل فتحي – تقى حامد معوض ، دور القيادة السياسية الروسية في تعزيز الامن السيبراني (2012-2023) ، (المانيا : المركز الديمقراطي العربي، 2023)، في https://democraticac.de/?p=90695 ، (2024/3/25) .

[7] David G. Delaney , Cyber security and the Administrative National Security State: Framing the Issues for Federal Legislation, Maurer School of Law: Indiana University, Vol (40), p 252 .

[8] بوقرين عبد الحليم ، الأمن السيبراني والمضامين المفاهيمية المرتبطة به ، مجلة طبنة للدراسات العلمية الاكاديمية ، جامعة الاغواط ، العدد (2) ، (الجزائر : 2022) ، ص45.

[9] David W. Opderbeck, Cyber security and Executive Power, (Washington University Law Review) ,Volume (89) ,Issue (4), January/ 2012, P799.

[10] ابتسام علي حسين، فرص وقيود الاطراف المتنازعة على المجال العام السيبراني، ملحق مجلة السياسة الدولية ، العدد (٢٠٨) ،(مصر: 2017) ، ص١٤.

[11] Myriam Dunn Cavelty and Florian J. Egloff, “The Politics of Cyber security: Balancing Different Roles of the State.” St Antony’s International Review 15 no.1 2019 , P39 .

(12) بوقرين عبد الحليم ، مصدر سبق ذكره ، ص46 .
(13) أسماعيل زروقة ، الفضاء السيبراني والتحول في مفاهيم القوة والصراع ، مجلة العلوم القانونية والسياسية ، جامعة محمد بوضياف المسلة ، العدد (1) ، المجلد (10) ،(الجزائر: 2019) ، ص1022.
(14) بوقرين عبد الحليم ، مصدر سبق ذكره ، ص47.
(15)Joseph S. Nye JR, Cyber Power, (Harvard Kennedy School: 2010), P10.
(16) Markus Christen, Bert Gordijn Michele Loi , The Ethics of Cyber security ،the registered company Springer Nature, Switzerland AG ،P13
(17) تغريد معين حسن ، مصدر سبق ذكره ، ص245.
(18) حنان عباس سلمان- أبتسام كاظم جاسم، القوة السيبرانية واثرها على القوة الاقتصادية الصين أنموذجاً ، مجلة مركز دراسات الكوفة، العدد (70) ، (العراق: 2023) ، ص626.
(19) Venkatraman & Karun Gupta , Cyber security its Effects on National Security And International Relations, (Articles section of Manupatra Newsline : 13/ july /2016), P76, www.manupatra.com (25/3/2024).
(20) خالد وليد ، الفضاء السيبراني نحو امتلاك ناصية القوة، (قطر : مركز الجزيرة للدراسات، 2021)، في https://www.aljazeera.net/amp/opinions/ (2024/3/25) .
(21) تغريد صفاء- لبنى خميس، أثر السيبرانية في تطور القوة ، مجلة حمورابي، العدد (33-34) ، (العراق: 2020) ، ص152.
(22) أيهاب خليفة، القوة الالكترونية كيف يمكن أن تدير الدول شؤونها في عصر الانترنت،(القاهرة : دار العربي، 2017) ، 2017، ص54.
(23) للمزيد من التفاصيل ينظر الى تقارير الامن السيبراني : Global Cybersecurity Index,International TelecommunicationUnion DevelopmentSector, ITU Publicationshttps://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx .
(24) باسم علي خريسان ، الامن السيبراني في العراق : قراءة في مؤشر الامن السيبراني العالمي 2020 ، (العراق : مركز البيان للدراسات والتخطيط ، 2021) ، ص4-5.
(25) خالد وليد محمود، قراءة في مؤشر الأمن السيبراني لعام 2021، (قطر : مركز الجزيرة للدراسات ،٢٠٢٢) في (https://www.aljazeera.net/amp/opinions)، (٢٠٢٤/٤/١) .
(26) صفد الشمري ، مـاواقع الأمـن السـيبراني في العـراق ، (العـراق : جريـدة الصـباح ، 2021) ، فيhttps://alsabaah.iq/48007-.html, (2024/4/1) .
(27)حمزة محمود شمخي، مؤشر الامن السيبراني وموقع العراق فيه ، مقال منشور (العراق: جامعة كربلاء، ٢٠٢٢) في ، http://business.uokerbala.edu.iq/wp/archives/20636 (٢٠٢٤/٣/٢٩).
(28) العراق يتراجع عالميا وعربيا في الامن السيبراني ، (العراق : مركز الاعلام الرقمي العراقي، 2021) في https://dmc-iq.com/2021/06/30 / ، (2024/3/30) .
(29) مصطفى أبراهيم سلمان، الامن السيبراني واثرة على الامن الوطني العراقي، مجلة العلوم القانونية والسياسية، جامعة ديالى ، المجلد (10) ، العدد(1)، (العراق : 2021) ، ص174-175 .
(30) زهير خضير عباس – ظفر عبد مطر ، العراق والامن السيبراني الفرص والتحديات، مجلة واسط للعلوم الانسانية والاجتماعية، جامعة واسط ، المجلد (18) ، العدد(51)، (العراق : 2022) ، ص12-13 .
(31) مصطفى علي الطائي، تحديات النظام السيبراني في العراق،(العراق: صحيفة أقلامهم الالكترونية ، 2023) ، في https://jaredaiq.net/News (27/3/2024) .
(32) Shubbar Hashim ،Constructing an Interinstitutional and interministerial effort on Cyber Security in Iraq ،(Iraq : Al-Bayan Center Studies Series ،2022), P4-5.

(33) أسعد طارش عبد الرضا – علي أبراهيم مشجل ، الامن السيبراني ودوره في ظاهرة أنتشار الارهاب في العراق بعد عام 2003، مجلة دراسات دولية، مركز الدراسات الدولية ، العدد(80)، (العراق : 2020) ، ص184-185 .

(34) السعودية تحقق المرتبة الثانية عالميا في مؤشر الامن السيبراني ، (صحيفة الشرق الاوسط : لندن, 2023) في https://aawsat.com/% ، (2024/4/2) .

(35) منى الاشقر جبور، الامن السيبراني : التحديات ومستلزمات المواجهة ، (جامعة الدول العربية : المركز العربي للبحوث القانونية والقضائية ، 2012) ، ص7-8 .

(36) زهير خضير عباس – ظفر عبد مطر ، مصدر سبق ذكره ، ص13 .

(37) Omar H Salman , Cybersecurity is a critical necessity for Iraq's digital evolution, (tahawultech :13/12/2023),https://www.tahawultech.com/features/ (3/4/2024) and Mohammed Mahmood Abdullah and others,Designing Predictive Models for Cybercrime Investigation in Iraq,(International Journal of Cyber Criminology). Vol (16), Issue (2) July – December ,2022,P58.

ملف العدد
الأمن السيبراني
درع التحول الرقمي العراقي
(بين التحديات الراهنة وضرورات المستقبل)

الأمن السيبراني والتهديدات الأمنية المستجدة
قراءة في التجربة المصرية للأمن السيبراني

د. خديجة عرفة
رئيس محور التواصل المجتمعي
مركز المعلومات ودعم اتخاذ القرار
رئاسة مجلس الوزراء المصري

شهدت البيئة الأمنية تحولات مهمة خلال السنوات الأخيرة في ضوء مجموعة من التطورات التي طرأت على البيئة الأمنية مخلفة قائمة من التهديدات الأمنية المستجدة، والتي أصبحت تفرض تهديدات متزايدة لأمن الدول واستقرار المجتمعات. ومن بين تلك التهديدات الجرائم السيبرانية؛ فقد شهد العالم خلال السنوات الماضية تطورًا تكنولوجيًا هائلًا سمح بتدفق الأفكار وانتشارها بسرعة كبيرة داخل وعبر المجتمعات. وقد أسهم ذلك في تعزيز حرية التعبير والتواصل بين الأفراد، إلا أنه في الوقت ذاته، أصبح آلية لتأجيج الصراعات، وأصبح مجالا خصبا لممارسة أشكال مختلفة من الجرائم التي أضحت تهدد كل من أمن الأفراد واستقرار المجتمعات، وتتنوع مخاطر الجريمة الالكترونية فهناك المخاطر المجتمعية والمخاطر الاقتصادية إلا أن الجانب الأخطر هو تهديد الأمن القومي للدول، وقد دفعت تلك المخاطر بالمجتمعات المختلفة لتبني مجموعة من الإجراءات في مواجهة التهديدات السيبرانية ولتعزيز أمنها السيبراني. وقد اتخذت العديد من الدول العربية مجموعة من الخطوات فيما يتعلق تعزيز القدرة على مواجهة تلك التحديات، مع ملاحظة وجود تفاوتات كبيرة بين الدول العربية في هذا الشأن، وهو ما انعكس بشكل واضح على ترتيب الدول العربية فيما يتعلق بالمؤشرات الدولية الخاصة بالأمن السيبراني. يُضاف لذلك وجود تفاوتات بالنسبة للدول الواحدة فيما يتعلق بوضعها وفقًا للمؤشرات الفرعية. بحيث يتطلب التحرك في مواجهة التهديدات السيبرانية العمل على العديد من المسارات.، واتخذت مصر مجموعة مهمة من الخطوات من أجل تعزيز أمنها السيبراني وخاصة في المجالات القانونية والتنظيمية وأن كان هنالك ما زالت مجموعة من التحديات التي هناك حاجة للتحرك بشأنها فالتطور في طبيعة التهديدات السيبرانية مع صعوبة التنبؤ بها يتطلب التعاون بشكل أكثف فيما بين دول المنطقة للاستعداد لتلك التهديدات.

الكلمات المفتاحية: الأمن السيبراني، التهديدات الأمنية المستجدة، مصر ، الجرائم السيبرانية.

الاستلام	الارجاع	القبول
2024/04/20	2024/05/15	2024/06/06

Cybersecurity and emerging security threats: Read about the Egyptian cybersecurity experience

Dr. Khadija Arafa

Head of the community communication hub

Information and Decision Support Center -

Presidency of the Egyptian Council of Ministers.

In recent years, the security environment witnessed important transformations in the light of a series of developments, imposing a list of emerging security threats, which are increasingly posing threats to the security of states and the stability of societies. One of these threats is cybercrime; over the past years, the world has witnessed tremendous technological development that has allowed the flow of ideas and their spread very quickly within and across societies. This has contributed to the strengthening of freedom of expression and communication between individuals, but at the same time, it has become a mechanism for fueling conflicts and has become a fertile field for the practice of various forms of crimes that threaten both the security of individuals and the stability of societies. Cybercrime risks vary, as there are societal risks and economic risks, but the most serious aspect is the threat to the national security of countries. These risks have prompted different communities to adopt a set of procedures in the face of cyber threats and to strengthen their cyber security. Many Arab countries have taken a number of steps with regard to enhancing the capacity to face these challenges, noting that there are significant disparities between Arab countries in this regard, which is clearly reflected in the ranking of Arab countries in terms of international indicators on cybersecurity. In addition, there are disparities for individual states regarding their status according to the sub-indicators. So that moving in the face of cyber threats requires working on many tracks. Egypt has taken important steps to strengthen its cyber security, especially in the legal and regulatory fields. but there are still a number of challenges that need to be addressed, the evolution in the nature of cyber threats, with their difficulty in forecasting, requires more intensive cooperation among the countries of the region to prepare for those threats.

keywords: Cyber Security- Emerging Security threats – Egypt- Cyber Crimes.

المقدمة

تُشكّل التهديدات السيبرانية أحد الأنماط الجديدة لتهديد أمن الدول والمجتمعات المختلفة، وذلك كنتيجة لتأثير التطورات التكنولوجية على مفهوم الأمن؛ الذي اكتسب أبعادًا جديدة كنتيجة لجملة من التطورات والتحولات في البيئة الأمنية وتحديدًا منذ نهاية الحرب الباردة. بحيث أثرت التهديدات الأمنية المُستجدة على الجوانب والأبعاد المختلفة للأمن بمفهومه الشامل.

وتشهد كافة المجتمعات، وبدرجات متفاوتة، أشكال مختلفة من التهديدات السيبرانية والجرائم الإليكترونية التي تتفاوت في حدتها وتأثيراتها على تلك المجتمعات مما دفع بالأخيرة لتطوير إجراءات مضادة بما يشمله ذلك من وضع إطار تشريعي حاكم وتبني استراتيجيات وإنشاء كيانات تنظيمية وكذلك بناء قدرات العاملين في هذا القطاع بما يمكنهم من مواجهة تداعيات تلك التهديدات وكذلك التعاون الدولي وغير ذلك من الخطوات سواءً كانت بهدف مواجهة التداعيات السلبية للهجمات السيبرانية أو التحرك الاستباقي للحد من التهديدات القادمة.

وتتفاوت الأوضاع بين الدول العربية فيما يتعلق بدرجة الاستعداد في مواجهة التهديدات السيبرانية. وقد اتخذت مصر خلال السنوت الأخيرة العديد من الخطوات في مسار الحد من تداعيات التهديدات السيبرانية. ومع نجاح تلك الخطوات في وضع مصر في مكانة جيدة في مؤشر الأمن السيبراني العالمي والقدرة على الحد من تداعيات التهديدات السيبرانية، إلا أنه ما زالت هناك بعض التحديات التي تتطلب المزيد من التحركات.

1-التهديدات الأمنية المُستجدة وارتباطها بأمن الدولة

حظي مفهوم الأمن باهتمام كبير من قبل الدارسين وذلك في ضوء أهمية الظاهرة الأمنية لبقاء واستقرار المجتمعات وحياة البشر مما يتطلب البحث عن الآليات الكفيلة لضمان حماية أمن الدول واستقرار الأفراد والمجتمعات.

وتبلور مفهوم "أمن الدولة" State Securityبصورة واضحة منذ القرن السابع عشر، ليشهد المفهوم تطورات مهمة مع التحولات الكبرى التي شهدتها البيئة الأمنية الدولية ليكتسب أبعادًا مختلفة في كل مرحلة. فمع المراحل المهمة من مراحل التحول في النظام

الدولي كانت هناك مراجعات مهمة للمفهوم. فخلال فترة الحرب الباردة سيطرة البعد العسكري على المفهوم بشكل واضح، ومنذ ثمانينيات القرن العشرين حدثت مراجعة قوية للمفهوم بحيث ركزت الدراسات الأكاديمية على تعميق وتوسيع المفهوم التقليدي للأمن والقائم على البعد العسكري بالأساس. حيث ظهرت مجموعة من الأفكار النقدية لمفهوم الأمن. في محاولة إيجاد صيغ أخرى مُغايرة للصيغة التقليدية للأمن وبما يتناسب مع طبيعة التحديات المفروضة. ورغم كونها تحديات ليست بالجديدة على المجتمع الدولي، إلا أن ظروف الحرب الباردة حالت دون وضع في تلك التحديات في سياق النظرية الأمنية أو حتى التعامل معها كمصدر تهديد للأمن القومي للدول.

وتُشير التحليلات إلى أن الدراسات الأمنية خلال القرن العشرين مرت بأربع مراحل متمايزة ارتبطت بالأساس بالتحولات في البيئة الأمنية الدولية، لتمتد المرحلة الأولى منذ نهاية الحرب العالمية الأولى واستمرت حتى منتصف خمسينيات القرن العشرين، وفيها اتجهت الدراسات الأمنية نحو التركيز على مفاهيم الأمن الجماعي، وفي المرحلة الثانية التي استمرت طيلة الحرب الباردة فقد غلب عليها الاعتبارات المتعلقة بأمن الدولة ببعده العسكري ومفاهيم الردع العسكري وغير ذلك. وبدأت المرحلة الثالثة في إطار المراجعة التي شهدها مفهوم "أمن الدولة" منذ ثمانينات القرن العشرين حيث ظهرت نظريات الاعتماد المتبادل في المجال الاقتصادي، ومع نهاية الحرب البادرة بدأت المرحلة الرابعة والتي شهدت الجدل بشأن تعميق وتوسيع مفهوم أمن الدولة لتبرز مجموعة جديدة من المفاهيم الأمنية[1]. فالاقتراب التقليدي الذي قصر مصادر تهديد أمن الدولة على كونها مصادر خارجية ذات صبغة عسكرية التعامل معها يكون من خلال القوى العسكرية أصبح عاجزا أمام تلك التحولات وأصبحت كافة الدول على تنوع ما تمتلكه من مقدرات تواجه قائمة كبيرة من التحديات الأمنية المتشابكة والمعقدة والتي في أغلب الأحيان يكون صعب توقع حدوثها وربما حتى مصدرها.

وتشمل تلك القائمة من التهديدات الأمنية المستجدة الحروب والجرائم الإليكترونية وحروب الفضاء والتحديات والمخاطر البيئية والإرهاب الدولي في أبعاده الجديدة بما يفرضه من تحديات لأمن الدول والأفراد بشكل غير مسبوق، وكذلك الجريمة المنظمة، ومشكلات اللاجئين وغيرها.

وتُعرف التهديدات الأمنية المُستجدة بأنها: "ما ظهر على الساحة في الفترة الأخيرة من نوعيات حديثة للإجرام أو أساليب حديثة لارتكاب جرائم معروفة من قبل وكذلك كيفية الفرار من العدالة عن طريق تلك الأساليب"[2].

2-الجرائم السيبرانية كأحد التهديدات الأمنية المستجدة

شهد العالم خلال السنوات الماضية تطورًا تكنولوجيًا هائلًا سمح بتدفق الأفكار وانتشارها بسرعة كبيرة داخل وعبر المجتمعات. وقد أسهم ذلك في تعزيز حرية التعبير والتواصل بين الأفراد، إلا أنه في الوقت ذاته، أصبح آلية لتأجيج الصراعات، وأصبح مجالاً خصبًا لممارسة أشكال مختلفة من الجرائم التي أضحت تهدد كل من أمن الأفراد واستقرار المجتمعات. وكذلك أصبحت أداة من أدوات الصراع بين الدول. بحيث أصبح العالم يشهد سباقًا جديدًا للتسلح لكنه في الفضاء السيبراني. وهو فضاء له خصوصيته. وبذلك فقد أصبح هناك مجالًا مغايرًا، ممثلًا في الفضاء الرقمي Cyber Space. ويُعرف الاتحاد الدولي للاتصالات الفضاء الرقمي بأنه: "المجال المادي وغير المادي الذي يتكون أو ينتج عن عناصر هي: أجهزة الكمبيوتر، الشبكات، البرمجيات، حوسبة المعلومات، المحتوى، معطيات النقل والتحكم، ومستخدمو كل هذه العناصر".

كما تتنوع مخاطر الجريمة الالكترونية فهناك المخاطر المجتمعية كنشر الشائعات والتأثير على الأطفال وانتهاك الخصوصية وتهديد قيم وثوابت المجتمع، وكذلك المخاطر الاقتصادية ومن ذلك تهديد الاقتصاد القومي للدول واستهداف القطاعات الحيوية أو الإضرار بالاقتصاد القومي عن طريق نشر معلومات خاطئة وإشاعات قد تؤدي إلى إعراض المستثمرين عن الاستثمار وغير ذلك.

إلا أن الجانب الأخطر هو تهديد الأمن القومي للدول من خلال:

-تهديد الأمن القومي للدول من خلال الاستيلاء على أسرار عسكرية وحربية مهمة، وكذلك سرقة بيانات حكومية خطيرة.

-التأثير على استقرار الدول من خلال نشر الأفكار المتطرفة، وتجنيد الأفراد للانضمام للتنظيمات الإرهابية العابرة للحدود باستخدام الأدوات التكنولوجية الحديثة.

-الإضرار بالبنية التحتية للدول من خلال شن هجمات إلكترونية على شبكات الكهرباء ومحطات المياه وشركات الرعاية الصحية بما يؤدي في بعض الأحيان إلى توقفها عن العمل بشكل جزئي أو كلي.

وقد تعددت المفاهيم التي تناولت مفهوم الجريمة الإلكترونية، ومن أبرزها المفهوم الصادر عن الأمم المتحدة والذي يعرفها بأنها: «مجموعة واسعة من الجرائم، بما في ذلك الجرائم ضد البيانات وأنظمة الحاسبات (مثل القرصنة)، والتزوير والاحتيال المرتبط بالكمبيوتر (مثل التصيد الاحتيالي)، والجرائم المتعلقة بالمحتوى (مثل نشر المواد الإباحية المتعلقة بالأطفال)، ومخالفات حقوق الطبع والنشر (مثل نشر المحتوى المسروق أو المقرصن)[3].

وتتسم الجريمة الالكترونية بالعديد من الخصائص من بينها[4]:

1-جريمةٌ لا تتقيّد بمكانٍ أو زمانٍ مُحدّدين.

2-صعوبة معرفة مرتكب الجريمة إلا باستخدام وسائل أمنيّة ذات تقنية عالية.

3-صعوبة قياس الضّرر المُترتّب عليها، كونه ضررًا يمسّ القيم المعنوية أو الماديّة أو كليهما معًا.

4-سهولة ارتكابها، بسبب غياب الرّقابة الأمنية.

5-سهولة إخفاء وطمس مَعالم الجريمة والدّلائل التي تُشير إلى مرتكبها.

6-مقارنة بالجرائم التقليدية تُعدّ الجريمة الإليكترونية أقل جهدًا وعنفًا.

كما تتعدد تصنيفات الجرائم الإلكترونية، ما بين جرائم تستهدف الأفراد، وأخرى تستهدف الشركات، كما أنَّ بعضها يستهدف البيانات، وأخرى تستهدف أجهزة الحاسبات، وبصفة عامة يمكن تقسيم الجرائم الإلكترونية إلى عدة أنماط، منها: جرائم ضد السرية والنزاهة وتوافر البيانات ونظم الحاسبات، والجرائم المتعلقة بأجهزة الحاسبات، والجرائم المتعلقة بالمحتوى غير القانوني، والجرائم المتعلقة بحقوق النشر. يُضاف لذلك المطاردة الإلكترونية، وهي الجرائم المُتعلّقة بتعقّب أو مطاردة الأفراد عن طريق الوسائل الإلكترونيّة بهدف تعريضهم للمضايقات الشّخصية أو الإحراج العام أو السّرقة المالية، وتهديدهم.

وتُشير الدراسات إلى أنَّ الجرائم الإليكترونية تعتمد على عدد من الأساليب والأدوات من أبرزها[5]:

1-الهندسة الاجتماعية Social Engineering

2-مسح المنافذ Port Scanning

3-كسر كلمات السر Password Cracking

4-التجسس على رزم البيانات Packet Sniffing

5-مسح تحديد قابلية التعرض للهجوم Vulnerability Scanning

6-مسح الخطوط الهاتفية War Dialing

7-الإدارة عن بعد Remote Administration

8-استراق ضربات لوحة المفاتيح KeyStroke Monitoring

9-إغراق الذاكرة المؤقتة Buffer Overflows

10-اختطاف جلسة الاتصال الشبكي Session Hijacking

11-تمويه العنوان الشبكي IP Spoofing

12-التخفي الشبكي Anonymity

13-التشفير Cryptography

14-إخفاء وتمويه الرسائل Steganography

15-مولدات أرقام بطاقات الائتمان.

كما تتعدد تصنيفات الجرائم الإلكترونية، ما بين جرائم تستهدف الأفراد، وأخرى تستهدف الشركات، كما أن بعضها يستهدف البيانات، وأخرى تستهدف أجهزة الحاسبات، وبصفة عامة يمكن تقسيم الجرائم الإلكترونية إلى عدة أنماط، منها:

-جرائم ضد سرية ونزاهة وتوافر البيانات ونظم الحاسبات

-الجرائم المتعلقة بأجهزة الحاسبات:

-الجرائم المتعلقة بالمحتوى غير القانوني

-الجرائم المتعلقة بحقوق النشر

-المطاردة الإلكترونية: هي الجرائم المُتعلّقة بتعقّب أو مطاردة الأفراد عن طريق الوسائل الإلكترونيّة بهدف تعريضهم للمضايقات الشّخصية أو الإحراج العام أو السّرقة المالية، وتهديدهم.

-الإرهاب الإلكتروني: أتاح الفضاء الإلكتروني الفرصة أمام انتشار الأفكار المتطرفة ودعم الإرهاب، حيث عدت وسيلة سهلة وسريعة وغير مكلفة أمام الجماعات الإرهابية

لتجنيد الأفراد للانضمام إليها، والتواصل فيما بينهم ومع العالم الخارجي، ونشر المواد التدريبية وأشرطة الفيديو والترويج للأفكار الإرهابية وغيرها.

-الجرائم السّياسية الإلكترونية: هي جرائم تستهدف المواقع العسكرية للدول، فضلاً عن الأجهزة الاستخباراتية، وذلك بهدف سرقة معلومات تتعلّق بالدّولة وأمنها.

وبذلك فقد دفعت المخاطر المرتبطة بالجرائم الإليكترونية بالدول المختلفة بتبني إجراءات خاصة بضمان أمنها السيبراني Cyber Security. ويُعرف الأمن السيبراني بأنه: "جميع الاجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع اشكالها الإلكترونية والمادية من مختلف الجرائم والهجمات والتخريب والتجسس والحوادث" (وزارة الدفاع الأمريكية).

كما يُعرف بأنه " أمن المعلومات على أجهزة وشبكات الحاسب الآلي، بما في ذلك العمليات والآليات التي يتم من خلالها حماية معدات الحاسب الآلي والمعلومات والخدمات من أي تدخل غير مقصود أو غير مصرح به أو تغيير أو إتلاف قد يحدث" (وزارة الاتصالات وتكنولوجيا المعلومات-مصر).

ويُعرفه الاتحاد الدولي للاتصالات بأنه "مجموعة من المهمات، مثل تجميع وسائل، وسياسات، واجراءات أمنية، ومبادئ توجيهية، ومقاربات لإدارة المخاطر، وتدريبات، وممارسات، وتقنيات، يمكن استخدامها لحماية البيئة السيبرانية وبيانات ومعلومات المؤسسات والمستخدمين".

وتُعرفه وزارة الأمن الداخلي الأمريكي بأنه "النشاط، أو العملية، أو القدرة، أو الإمكانية، أو الحالة التي يتم بموجبها حماية نظم المعلومات والاتصالات والدفاع عنها ضد الضرر أو الاستخدام أو التعديل غير المصرح به أو الاستغلال".

وللتهديدات السيبرانية تأثيراتها على المجتمعات المختلفة؛ وتُشير الإحصاءات إلى أنه خلال عام 2022 تعرض نحو 40% من مستخدمي الانترنت في جميع أنحاء العالم إلى جرائم إليكترونية. وهذه الجرائم تتنوع في أشكالها ودرجة تأثيرها على أمن الأفراد.

وتُعدّ الصين الأكثر استهدافًا بالهجمات السيبرانية بنسبة 18.83% تليها الولايات المتحدة الأمريكية بنسبة 17.05%، ثم البرازيل 5.63%، فالهند 5.33%، ويليها ألمانيا 5.10%، ثم فيتنام 4.23%، وتايلاند 2.51%، ثم روسيا 2.46%، وإندونيسيا 2.41%، وهولندا 2.20%[6]. فقد تم اختراق حسابات 1 من كل 2 من مستخدمي الإنترنت

الأمريكيين في عام 2021. كما تأثر 53.35 مليون مواطن أمريكي بالجرائم الإلكترونية في النصف الأول من عام 2022[7].

هذه الجرائم لها تكلفة اقتصادية مرتفعة على الأفراد والدول، وتؤثر على مسارات التنمية في الدول مما ينعكس سلبًا على احتياجات الأفراد. إذ تُشير التقديرات إلى أنه خلال عام 2023 بلغت التكلفة الاقتصادية للهجمات السيبرانية 8 تريليون دولار، أي في المتوسط 21.9 بليون دولار يوميًا. هذه المبالغ كان يمكن تخصيصها لأغراض تنموية تصب في مصالح الأفراد في المجتمعات المختلفة. وأن الشركات الصغيرة والمتوسطة وفقًا لإحدى الدراسات والتي يقل عدد العاملين بها عن 100 عامل أكثر عرضة لتلك الهجمات بمعدل ثلاث مرات أكثر مقارنة بالشركات الكبرى، وهو الأمر الذي من شأنه التأثير على العاملين بتلك الشركات والتي قد تصبح أكثر عرضة للتوقف عن العمل[8]. وبذلك يتضح حجم التأثير الكبير للجرائم الإليكترونية على أمن الأفراد.

ومن المتوقع أنَّ تبلغ التكلفة الاقتصادية للهجمات السيبرانية 10.5 تريليون دولار بحلول 2025[9]. أي في المتوسط 28.8 بليون دولار يوميًا. بمعدل زيادة بلغ بين عامي 2023 و2025 ما نسبته 31.5%. وبذلك يتضح حجم التطور الكبير في التأثير الاقتصادي لتلك الجرائم في وقت يُعاني فيه الاقتصاد العالمي والأمن الاقتصادي للأفراد من مشكلات عدة.

وقد زاد متوسط تكلفة خروقات البيانات في الساعة على مستوى العالم لتصل في عام 2021 إلى 671.787 دولار في الساعة بعد أن كان 2054 دولار في الساعة عام 2021. [10] وخلال الفترة ذاتها زاد عدد ضحايا خروقات البيانات من 6 ضحايا إلى 97ضحية في الساعة. كما كلفت الجرائم الإلكترونية الشركات البريطانية ما معدله 4200 دولار في عام 2022. فقد أبلغت 39 ٪ من الشركات البريطانية عن تعرضها لهجوم إلكتروني في عام 2022[11].

ويُعدّ التصيد الاحتيالي هو الشكل الأكثر شيوعا للجرائم الإلكترونية. وخلال ذروة وباء كوفيد ارتفعت حوادث التصيد الاحتيالي بنسبة 220% عام 2021. في حين يعد الاحتيال الاستثمار هو الأكثر تكلفة، ففي عام 2022خسر كل ضحية في المتوسط 70811 دولارا[12]. في حين أن المتوسط في حالة التصيد الاحتيالي يبلغ 136 دولار.

3-التجربة المصرية في مجال الأمن السيبراني

مع تزايد التهديدات السيبرانية اتخذت العديد من الدول العربية مجموعة من الخطوات فيما يتعلق تعزيز القدرة على مواجهة تلك التحديات، مع ملاحظة وجود تفاوتات كبيرة بين الدول العربية في هذا الشأن، وهو ما انعكس بشكل واضح على ترتيب الدول العربية فيما يتعلق بالمؤشرات الدولية الخاصة بالأمن السيبراني. يُضاف لذلك وجود تفاوتات بالنسبة للدول الواحدة فيما يتعلق بوضعها وفقًا للمؤشرات الفرعية. بحيث يتطلب التحرك في مواجهة التهديدات السيبرانية العمل على العديد من المسارات.

وفيما يتعلق بوضع مصر في مواجهة التهديدات السيبرانية، فقد كانت هناك العديد من الخطوات التي اتخذت خلال السنوات الأخيرة.

إذا ما نظرنا إلى مؤشر نضج التكنولوجيا الحكومية GovTech Maturity Index، وهو مؤشر مركب أطلقه البنك الدولي يستند إلى 48 مؤشرًا فرعيًا في أربعة جوانب هي: الأنظمة الحكومية الأساسيةCore Government Systems، وتعزيز تقديم الخدمات Public Sector Delivery، والمشاركة الرقمية للمواطنينDigital Citizen Engagement ، وتعزيز عوامل التكنولوجيا الحكوميةGovTech Enablers . ويتم تطبيقه في 198 دولة. ويهدف المؤشر إلى قياس فجوات التحول الرقمي. ويوضح الجدول التالي وضع مصر في المؤشرات الفرعية الأربع[13]:

المؤشر الفرعي	قيمة المؤشر في مصر	أقصى قيمة للمؤشر
الأنظمة الحكومية الأساسية	0.78	0.99
تعزيز تقديم الخدمات	0.79	1
المشاركة الرقمية للمواطنين	0.63	4
تعزيز التكنولوجيا الحكومية	0.8	0.98

وبذلك يتضح ضرورة بذل جهد أكبر فيما يخص المشاركة الرقمية للمواطنين.

ووفقا لمؤشر الأمن السيبراني 2022 والصادر عن الاتحاد الدولي للاتصالات، والذي يقيس حالة الأمن السيبراني لكل بلد باستخدام خمسة معايير، هي: المعيار القانوني، التقني، بناء القدرات، التعاون، والتنظيمي. فقد جاءت السعودية في الترتيب الثالث عالميا والأول عربيا،

والإمارات في الترتيب الثاني عربيا والعاشر عالميا، وسلطنة عمان في الترتيب الـ 28 عالميا والثالث عربيا، وجاءت مصر في الترتيب الـ 30 عالميًا والرابع عربيًا.

وبذلك يلاحظ حدوث تراجع في ترتيب مصر، فوفقًا لمؤشر الأمن السيبراني لعام 2017، فقد جاءت مصر في الترتيب الثاني عربيًا والرابع عشر عالميًا. أما وفقًا لنسخة 2020 من المؤشر، فقد جاءت مصر في الترتيب الـ 23 عالميًا والرابع عربيًا[14].

ويقيس المؤشر حالة الأمن السيبراني لكل بلد باستخدام خمسة معايير، هي: المعيار القانوني، التقني، بناء القدرات، التعاون، والتنظيمي.

وقد بلغت قيمة مؤشر عام 2020 في مصر 95.48 نقطة، حيث تتراوح قيمة المؤشر ما بين 1 و100. وقد جاء مجموع المؤشر على النحو التالي: التدابير القانونية (20)، والتدابير التقنية (17.45)، والتدابير التنظيمية (20)، وتنمية القدرات (19.12)، والتدابير التعاونية (18.91). وبذلك فمجالات القوى بموجب المؤشر هي التدابير القانونية والتنظيمية وسيتضح ذلك فيما يلي[15].

فيما يتعلق بالتدابير القانونية، فقد عُني المشرع المصري بوضع إطار قانوني حاكم في هذا الشأن، فقد نصت المادة 31 من الدستور المصري على أن "أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه، على النحو الذي ينظمه القانون". كما نصت المادة 57 على "للحياة الخاصة حرمة، وهي مصونة لا تمس. وللمراسلات البريدية، والبرقية، والإلكترونية، والمحادثات الهاتفية، وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، ولا تجوز مصادرتها، أو الاطلاع عليها، أو رقابتها إلا بأمر قضائي مسبب، ولمدة محددة، وفى الأحوال التي يبينها القانون. كما تلتزم الدولة بحماية حق المواطنين في استخدام وسائل الاتصال العامة بكافة أشكالها، ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها، بشكل تعسفي، وينظم القانون ذلك"[16].

وإضافة إلى الدستور فيوجد قانونين من المهم الإشارة إليهما: الأول هو قانون مكافحة جرائم تقنية المعلومات لعام 2018 ويُعد الإطار القانوني الحاكم لأمن الفضاء الإلكتروني المصري، والمنوط بمكافحة كافة أشكال الجرائم الإلكترونية، ويُعنى القانون بعدة أمور من بينها: مكافحة الاستخدام غير المشروع للحاسبات وشبكات المعلومات، وما يرتبط بها من جرائم، والتزام الدقة في تحديد الأفعال المعاقب عليها، وتجنب التعبيرات الغامضة بوضع تعاريف

دقيقة لها، وتحديد عناصر الأفعال المجرمة بكثير من العناية، وكذلك مراعاة الاعتبارات الشخصية للمجنى عليهم، والاعتبارات المتعلقة بالمصلحة العامة وحماية الأمن والاقتصاد القومي[17].

حيث يسعى القانون إلى تحقيق عدة أهداف هي:

-حفظ وتخزين سجل النظام المعلوماتي أو أي وسيلة لتقنية المعلومات لمدة 180 يوما متصلة.

-مكافحة الاستخدام غير المشروع للحاسبات وشبكات المعلومات وتقنيات المعلومات، وما يرتبط بها من جرائم، مع التزام الدقة في تحديد الأفعال المعاقب عليها، وتجنب التعبيرات الغامضة بوضع تعاريف دقيقة لها.

-ضبط الأحكام الخاصة بجمع الأدلة الإلكترونية وتحديد حجيتها في الإثبات.

-وضع القواعد والأحكام والتدابير اللازم اتباعها من قبل مقدمي الخدمة لتأمين خدمة تزويد المستخدمين بخدمات التواصل بواسطة تقنيات المعلومات، وتحديد التزاماتهم في هذا الشأن.

-حماية البيانات والمعلومات الحكومية، والأنظمة والشبكات المعلوماتية الخاصة بالدولة، أو أحد الأشخاص الاعتبارية العامة، من الاعتراض أو الاختراق أو العبث بها، أو إتلافها أو تعطيلها بأي صورة كانت.

-حماية البيانات والمعلومات الشخصية، من استغلالها استغلالاً يسيء إلى أصحابها، وخاصة في ظل عدم كفاية النصوص التجريمية التقليدية المتعلقة بحماية خصوصيات الأفراد.

-وضع تنظيم إجرائي دقيق ينظم إجراءات الضبط والتحقيق والمحاكمة المتعلقة بتلك الجرائم، بالإضافة إلى تحديد حالات التصالح وإجراءاته، وتنظيم عمل الخبراء المتخصصين العاملين في مجال جرائم مكافحة تقنية المعلومات.

أما القانون الثاني المهم فهو قانون حماية البيانات الشخصية لعام 2020، ويعنى القانون بما يلي[18]:

-الحفاظ على الخصوصية الإلكترونية للمواطن بما يضمن حماية بياناته الشخصية من الاعتداء عليها من الشركات الدولية ومنصات التواصل الاجتماعي بدون موافقته.

-وضع إطار تنظيمي لحماية المعلومات ورفع مستويات أمن البيانات في مصر، ويتواكب مع القوانين والاتفاقيات الدولية في حماية الأنشطة الاستثمارية الحالية، وأنشطة الشركات في كل القطاعات الاقتصادية سواء السلعية أو الخدمية أو الاجتماعية والتي تتعامل مع بيانات

لمواطنين أوروبيين، بما يضمن استمرار هذه الأنشطة وعدم تعرضها لعقوبات مالية أو إدارية من قبل الاتحاد الأوروبي.

-إيجاد فرص استثمارية جديدة، وخاصة في مجالي صناعة مراكز البيانات العملاقة، ومجال صناعة التعهيد، والتي تسهم في خلق مزيد من فرص العمل وتشجع على جذب الاستثمارات في قطاعات الدولة المختلفة.

-تحسين المؤشرات الدولية الخاصة بأداء الأعمال، وتحسين وضعية مصر في التقارير الدولية الخاصة باحترام حقوق الإنسان.

-حماية الأنشطة الاستثمارية الحالية، وأنشطة الشركات في كل القطاعات الاقتصادية سواءً السلعية أو الخدمية أو الاجتماعية والتي تتعامل مع بيانات لمواطنين أوروبيين، بما يضمن استمرار هذه الأنشطة وعدم تعرضها لعقوبات مالية أو إدارية من قبل الاتحاد الأوروبي.

وبذلك فقد عمل المشرع المصري على مسارين الأول هو تجريم الجاني والثاني خاص بفرض الضوابط والمعايير المناسبة من أجل تنظيم المجال السيبراني. كما يجرى العمل على تطوير قانون للأمن السيبراني.

وإضافة إلى الجانب التشريعي فقد تم وضع استراتيجية وطنية للأمن السيبراني؛ وذلك بهدف التصدي للتهديدات السيبرانية الآخذة في التزايد من حيث العدد والمصادر، وكذلك المساهمة في بناء كوادر بشرية وتطوير صناعة وطنية يمكنها أن تُسهم في زيادة نصيب هذا القطاع من الناتج المحلي الإجمالي.

وقد صدرت نسختها الأولى للفترة (2017-2021) في مايو 2017، وتضمنت أهم التحديات والأخطار الفضاء الإلكتروني، وأهم القطاعات الحيوية المستهدفة وركائز التوجه الاستراتيجي لمواجهة أخطار الفضاء الإلكتروني. حيث حددت 6 محاور أساسية هي: تطوير الإطار التشريعي الملائم لأمن الفضاء السيبراني ومكافحة الجرائم السيبرانية وحماية الخصوصية والهوية الرقمية، وتطوير منظومة وطنية متكاملة لحماية أمن الفضاء السيبراني وتأمين البنية التحتية للاتصالات وتكنولوجيا المعلومات، وحماية الهوية الرقمية (برنامج المواطنة الرقمية) وتفعيل البنى التحتية اللازمة لدعم الثقة وخاصة في الخدمات الحكومية، وإعداد الكوادر البشرية والخبرات اللازمة لتفعيل منظومة الأمن السيبراني في مختلف القطاعات، ودعم البحث العلمي

والتطوير وتنمية صناعة الأمن السيبراني، والتوعية المجتمعية بالفرص والمزايا التي تقدمها الخدمات الالكترونية للأفراد والمؤسسات والجهات الحكومية[19].

ومع انتهاء الاستراتيجية، فقد صدرت نسختها الحديثة (2023- 2027) والتي حددت ست مجالات رئيسة هي: بناء إطار تشريعي متكامل، وتغيير ثقافة المجتمع حول الأمن السيبراني، وتعزيز الشراكة الوطنية، وبناء دفاعات سيبرانية قوية وقادرة على الصمود، وتشجيع البحث العلمي وتعزيز الابتكار والنمو، وأخيرًا تعزيز التعاون الدولي[20].

وفيما يتعلق بتعزيز الشراكة الوطنية فقد حددت الاستراتيجية الوطنية للأمن السيبراني (2023-2027) برنامج لتعزيز الشراكة الوطنية من خلال تطوير إطار حوكمة للأمن السيبراني، وإيجاد لجنة استشارية لصناعة الأمن السيبراني، مع التحرك نحو إبرام اتفاقيات للتعاون الثنائي وكذلك إنشاء صندوق تطوير الأمن السيبراني وكذلك إيجاد قاعدة مركزية لسوق الأمن السيبراني.

وفي ضوء التطور المستمر في طبيعة التهديدات فقد أكدت الاستراتيجية على العمل على برامج من شأنها بناء دفاعات سيبرانية قوية وقادرة على الصمود، وقد حددت الاستراتيجية عدد من البرامج تتدرج في إطار برامج المشروعات القومية، والبرامج الموجهة إلى البيئة التحتية الحرجة، والبرامج الموجهة للقطاع الخاص، وبرامج المعايير والسياسات، وكذلك البرامج الخاصة برفع مستوى الخدمات.

وعلى المستوى التنظيمي يمكن الإشارة إلى الدور المهم للمجلس الأعلى للأمن السيبراني، الذي تأسس كسلطة عليا في مجال الأمن السيبراني على المستوى الوطني.

كما تم إنشاء المركز الوطني للاستعداد لطوارئ الحاسب والشبكات EG-CERT، حيث تم تشكيل المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات (بالجهاز القومي لتنظيم الاتصالات في أبريل 2009، ويقدم المركز الدعم اللازم لحماية البنية التحتية القومية للمعلومات الهامة خاصة في قطاع تكنولوجيا المعلومات والاتصالات والقطاع المالي. ويتمثل الهدف الرئيسي للمركز في تعزيز أمن البنية التحتية المصرية للاتصالات والمعلومات من خلال اتخاذ إجراءات استباقية، وجمع وتحليل المعلومات الخاصة بالحوادث الأمنية، والتنسيق والوساطة بين الأطراف المعنية في حل تلك الحوادث الأمنية والتعاون الدولي مع غيرها من فرق الاستجابة لطوارئ الحاسبات والشبكات في الدول الأخرى.

وفي مجال رفع الوعي، خلال السنوات الأخيرة عمل EG-Certمن خلال العمل على رفع الوعي بالتحديات التي تفرضها التهديدات السيبرانية عبر مجموعة من الندوات وورش العمل وذلك لتمكين المجتمع بالمعرفة الأساسية والتدريب على أفضل الممارسات في تأمين الأصول الرقمية. بلغ عدد تلك الندوات في عام 2023 وحده نحو 66 ورشة عمل.

خاتمة:

مع أهمية الجهود المبذولة في مصر خلال السنوات الأخيرة في مواجهة التهديدات السيبرانية وخاصة في المجالات التشريعية والتنظيمية، فإن التطور في طبيعة التهديدات السيبرانية مع صعوبة التنبؤ بها يتطلب التعاون بشكل أكثف فيما بين دول المنطقة للاستعداد لتلك التهديدات.

كما أنه رغم الوضع الجيد نسبيا لبعض الدول العربية وفقا للمؤشرات الدولية المعنية بقياس درجة التهديدات السيبرانية في الدول المختلفة، فما زالت هناك فجوة كبيرة فيما بين الدول العربية فيما يتعلق بالقدرة على مواجهة التهديدات السيبرانية.

ومع ما قامت به العديد من دول المنطقة من وضع استراتيجيات لمواجهة الجرائم الالكترونية وكذلك تبني بعض الآليات المؤسسية والتنظيمية لمواجهة الجرائم الالكترونية والحد من مخاطرها. إلا أنه ما زالت هناك حاجة للمراجعة المستمرة لتلك الجهود في ظل ما تُشير إليه الأرقام من تزايد معدلات الجرائم الالكترونية والتوقعات باستمرار هذا التزايد بمعدلات أكبر.

وفيما يتعلق بدولة العراق، فوفقًا لمؤشر الأمن السيبراني لعام 2020، فقد جاءت في الترتيب رقم129 على مستوى العالم وفقًا لمؤشر الأمن السيبراني بقيمة للمؤشر بلغت 20.71 نقطة. كما جاءت في الترتيب 17 عربيًا.

ولو نظرنا إلى المؤشرات الفرعية المكونة للمؤشر فقد حصلت العراق على التقييم التالي: التدابير القانونية (صفر)، التدابير التقنية (6.56)، والتدابير التنظيمية (7.75)، وتنمية القدرات (2.14)، والتدابير التعاونية (4.26).

وبذلك يتضح أهمية البدء الفوري بالإطار القانوني الخاص بالأمن السيبراني في البلاد، مع التحرك بالتوازي على المسارات الأخرى. ومن المهم الاستفادة من الخبرات المتميزة لبعض الدول العربية في هذا الشأن ومن بينها السعودية والإمارات ومصر وسلطنة عمان. من

خلال المشاركة في التدريب المشترك وتبادل الخبرات والاستفادة من الخبرة القانونية بما يُسهم في وضع الإطار الأولى للبناء عليه.

المصادر والمراجع:

[1] إيمان جابر، مفهوم الأمن القومي وتطوراته وأهم القضايا والنقاشات في حقل السياسة العالمية، جامعة الإسكندرية، كلية الدراسات والاقتصادية العلوم السياسية، 23 ديسمبر 2019.
http://arabprf.com/?p=2431

[2] عباس أبو شامة، "التعريف بالظواهر الإجرامية المستحدثة: حجمها، أبعادها ونشاطها في الدول العربية"، في: **الظواهر الإجرامية المستحدثة وسبل مواجهتها**، أعمال الندوة العلمية التي عقدت في تونس في الفترة من 28-30 يونيو 1999، الرياض: جامعة نايف العربية للعلوم الأمنية، ص9-11.

[3] Transnational organized crime threat assessments, United Nations, Office on Drug and Crime, 2010.
https://www.unodc.org/unodc/data-and-analysis/TOC-threat-assessments.html

[4] إسراء مرعي، "الجرائم الإلكترونية: الأهداف - الأسباب - طرق الجريمة ومعالجتها", المركز الديمقراطي العربي، 2016.
https://bit.ly/2yvvciH.

[5] تركي بن عبدالرحمن المويشير، بناء نموذج أمني لمكافحة المعلوماتية وقياس فاعليته، رسالة دكتوراه، الرياض جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، 2009.

[6] Niv DavidPur, Which Countries are Most Dangerous? Cyber Attack Origin – by Country, Cyber Proof, 2022 https://blog.cyberproof.com/blog/which-countries-are-most-dangerous

[7] The Latest 2024 Cyber Crime Statistics, AAG, 1 March 2024.
https://aag-it.com/the-latest-cyber-crime-statistics/

[8] Cybersecurity: Economic Growth and Trade (EGAT), USAID, 2023.
https://www.usaid.gov/sites/default/files/2023-10/Cybersecurity%20Briefer_Economic%20Growth.pdf

[9] Morgan. Steve, 2022. Cybercrime To Cost the World 8 Trillion Annually In 2023, Cyber Crime Magazine,
https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

[10]The Latest 2024 Cyber Crime Statistics, Op. Cit

[11] Ibid

[12] Ibid

[13] GovTech Maturity Index,
https://www.worldbank.org/en/programs/govtech/gtmi

[14] Global Cybersecurity Index, ITU,
https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

[15] Ibid

[16] دستور مصر لعام 2014
https://manshurat.org/node/4256

[17] قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018
https://manshurat.org/node/31487

[18] قانون رقم 151 لسنة 2020 بشأن حماية البيانات الشخصية
https://manshurat.org/node/66932

[19] الاستراتيجية الوطنية للأمن السيبراني (2017- 2022)، وزارة الاتصالات وتكنولوجيا المعلومات
https://mcit.gov.eg/Upcont/Documents/swf/AR_National_Cybersecurity_Strategy_2017_2021/index.html

[20] الاستراتيجية الوطنية للأمن السيبراني 2023- 2027، وزارة الاتصالات وتكنولوجيا المعلومات
https://mcit.gov.eg/Upcont/Documents/Publications_1412024000_ar_National_Cybersecurity_Strategy_2023_2027.pdf

ملف العدد
الأمن السيبراني
درع التحول الرقمي العراقي
(بين التحديات الراهنة وضرورات المستقبل)

نحو استراتيجية للأمن السيبراني العراقي
"الفرص والتحديات"

أ.م.د. محمد ميسر فتحي
جامعة الموصل/ كلية العلوم السياسية
رئيس فرع العلاقات الدولية

يُمثل الأمن السيبراني تحدياً مستمراً في عصر الرقمنة المتسارع، ويتطلب تعاوناً شاملاً بين القطاع الخاص والعام، بالإضافة إلى الاستثمار في البحث والتطوير لمواكبة التهديدات السيبرانية المتطورة وتشكل استراتيجيات الأمن السيبراني إطاراً شاملاً لحماية الأنظمة الإلكترونية والمعلوماتية من التهديدات السيبرانية. تتضمن هذه الاستراتيجيات مجموعة من الخطوات والتقنيات التي تهدف إلى تقليل المخاطر وزيادة الوقاية والتحقق من الامتثال. وتنبثق إشكالية البحث تبعاً لشدة التهديدات السيبرانية وتأثيرها وتداعياتها على الأمن الوطني العراقي والشبكات والأنظمة الالكترونية، والتساؤل الرئيس للاشكالية هو: ماهي استراتيجية الأمن السيبرانية العراقية وكيف يتم مواجهة التهديدات السيبرانية؟ وتأتي فرضية البحث من وجود علاقة عكسية بين متغيرات البحث، إذ كلما امتلك العراق استراتيجية متكاملة وفاعلة كلما ساهم ذلك في الحد من التهديدات السيبرانية وتأثيرها وتداعياتها على الأنظمة والشبكات في المجالات كافة.

الكلمات المفتاحية: العراق، التحول الرقمي، الامن الوطني، تحديات التحول، الامن الالكتروني.

Towards a strategy for Iraqi cybersecurity
Opportunities and challenges

Dr. Muhammad Maysar Fathi
University of Mosul/College of Political Sciences

Cybersecurity represents a continuing challenge in the era of accelerating digitization, and requires comprehensive cooperation between the private and public sectors, in addition to investment in research and development to keep pace with evolving cyber threats. Cybersecurity strategies constitute a comprehensive framework to protect electronic and information systems from cyber threats. These strategies include a set of steps and techniques aimed at reducing risks, increasing prevention, and verifying compliance. The research problem arises depending on the severity of cyber threats and their impact and repercussions on Iraqi national security, electronic networks and systems. The main question of the problem is:

الاستلام 2024/05/01
الارجاع 2024/05/30
القبول 2024/06/018

What is the Iraqi cyber security strategy and how are cyber threats confronted? The research hypothesis comes from the existence of an inverse relationship between the research variables, so the more Iraq has an integrated and effective strategy, the more this will contribute to reducing cyber threats and their impact and repercussions on systems and networks in all fields.

Keywords: Iraq, digital transformation, national security, transformation challenges, electronic security.

المُقدمة

في عالمنا المعاصر المعتمد بشكل كبير على التكنولوجيا، حتى أصبح الأمن السيبراني أمراً بالغ الأهمية ومؤثراً في التفاعلات والصرعات الدولية، ويُقصد بالأمن السيبراني حماية الأنظمة الإلكترونية، بما في ذلك الشبكات والأجهزة والبرمجيات، من التهديدات السيبرانية المتنوعة. وتتنوع التهديدات السيبرانية بشكل كبير وتشمل الاختراقات الإلكترونية، والبرامج الضارة، والاحتيال الإلكتروني، والاختراقات الهجومية، والتجسس السيبراني، والهجمات الرقمية الأخرى التي تستهدف الأنظمة والبيانات الحساسة.

كما تتطلب مواجهة هذه التحديات استراتيجيات شاملة تشمل التقييم المستمر للمخاطر، وتنفيذ سياسات وإجراءات أمنية صارمة، واستخدام التكنولوجيا الحديثة لحماية الأنظمة والبيانات. فضلاً عن ذلك، يعدّ توعية المستخدمين وتدريبهم على ممارسات الأمان السيبراني جزءاً أساسياً من أي استراتيجية فعالة للأمن السيبراني، حيث يمثل الانسان أحد أهم الأصول وأيضاً أكبر نقطة ضعف قابلة للاستغلال في الأمن السيبراني.

بشكل عام، يمثل الأمن السيبراني تحدياً مستمراً في عصر الرقمنة المتسارع، ويتطلب تعاوناً شاملاً بين القطاع الخاص والعام، بالإضافة إلى الاستثمار في البحث والتطوير لمواكبة التهديدات السيبرانية المتطورة .

وتشكل استراتيجيات الأمن السيبراني إطاراً شاملاً لحماية الأنظمة الإلكترونية والمعلوماتية من التهديدات السيبرانية. تتضمن هذه الاستراتيجيات مجموعة من الخطوات والتقنيات التي تهدف إلى تقليل المخاطر وزيادة الوقاية والتحقق من الامتثال.

وتنبثق إشكالية البحث تبعاً لشدة التهديدات السيبرانية وتأثيرها وتداعياتها على الامن الوطني العراقي والشبكات والأنظمة الالكترونية، والتساؤل الرئيس للإشكالية هو: ماهي استراتيجية الامن السيبرانية العراقية وكيف يتم مواجهة التهديدات السيبرانية؟

وتأتي فرضية البحث من وجود علاقة عكسية بين متغيرات البحث، إذا كلما امتلك العراق استراتيجية متكاملة وفاعلة، كلما ساهم ذلك في الحد من التهديدات السيبرانية وتأثيرها وتداعياتها على الأنظمة والشبكات في المجالات كافة.

كما اعتمد البحث عدة مناهج لاسيما المنهج الوصفي-التحليلي فضلاً عن المنهج الوظيفي.

المحور الأول: الأمن السيبراني (المفهوم والخصائص والمفاهيم المقاربة)

أولاً: مفهوم الامن السيبراني

يعرف الأمن السيبراني* Cyber Security بأنه "عملية حماية الأنظمة والشبكات والبرامج ضد الهجمات الرقمية التي تهدف للوصول إلى المعلومات الحساسة أو تغييرها أو تدميرها، بغرض الاستيلاء على المال من المستخدمين أو مقاطعة عمليات الأعمال العادية. وبدأ الاهتمام بالأمن السيبراني عبر شبكة وكالة مشاريع الأبحاث المتقدمة (ARPANET) في عام 1972. [1]

وهناك تعريف آخر للأمن السيبراني للكاتبان (Pekka & Martti) "بأنه عبارة عن مجموعة إجراءات اتخذت في الدفاع ضد الهجمات التي تتعرض لها من قراصنة الكمبيوتر وعواقبها، ويتضمن تنفيذ التدابير المضادة المطلوبة، كما عرفت هيئة الاتصالات وتقنية المعلومات الأمن السيبراني" هو حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحتويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع".[2]

وبذلك يُعدُّ الأمن السيبراني مجموعة وسائل من شأنها الحد من خطر الهجوم على البرامجيات وأجهزة الحاسوب والشبكات، تشتمل على الأدوات المستخدمة في مواجهة القرصنة الإلكترونيَّة، وكشف الفيروسات وتوفير الاتصالات المشفّرة، وينظر إليه الاتحاد الدولي للاتصالات على أنه "مجموعة من المهمات مثل تجميع وسائل وسياسات وإجراءات أمنيَّة ومبادئ توجيهيَّة ومقاربات لإدارة المخاطر وتدريبات وممارسات فضلى وتقنيات يمكن استخدامها لحماية البيئة السيبرانيَّة وموجودات المؤسسات والمستخدمين"، بينما عدّه الإعلان الأوروبي للأمن السيبراني "قدرة النظام المعلوماتي على مقاومة محاولات الاختراق، التي تستهدف البيانات".[3]

وقد بدأ اهتمام القوى الدولية بالأمن السيبراني منذ استخدامه من قبل الرئيس الأمريكي الأسبق باراك أوباما عام 2009، وعده سببا رئيساً في تعزيز الامن القومي لبلاده وان التهديدات السيبرانية هي أكبر التحديات الأمنية والاقتصادية التي تواجهها الولايات المتحدة الامريكية. (4)

وبذلك فإن الأمن السيبراني هو مجال متخصص يركز على حماية الأنظمة الإلكترونية، بما في ذلك الشبكات، والأجهزة، والبرامج، والبيانات، من التهديدات السيبرانية. يهدف الأمن السيبراني إلى توفير سرية، وسلامة، وسلامة البيانات والمعلومات، وضمان توفر الخدمات الرقمية بشكل موثوق وآمن. يشمل الأمن السيبراني مجموعة متنوعة من التقنيات والسياسات والممارسات التي تساعد في الوقاية من الهجمات الإلكترونية والتصدي لها عند حدوثها. (5)

كما إن أهمية الأمن السيبراني تنبع من كمية البيانات الغير مسبوقة المخزنة على أجهزة الكمبيوتر والسحابة الافتراضية والشبكات المرتبطة بها، والتي تتعلق بخصوصية عمل وأداء المؤسسات الحكومية والعسكرية والاقتصادية والشركات والمالية والطبية، وقد يؤدي اختراقها الى كشف اسرار تلك المؤسسات وتعرضها الى خسائر فادحة، ومع نمو حجم وتعقيد الهجمات الإلكترونية، يتعين على الشركات والمؤسسات وخاصة تلك المكلفة بحماية المعلومات المتعلقة بالأمن القومي أو الصحة أو السجلات المالية، اتخاذ خطوات لحماية معلومات الأعمال والموظفين الحساسة الخاصة بهم، كما إن الهجمات الإلكترونية والتجسس الرقمي تشكل أكبر تهديد للأمن القومي وتتفوق حتى على الإرهاب التقليدي. (6)

ثانيًا: المفاهيم المقاربة للأمن السيبراني:

1- **الفضاء السيبراني:**

يعرف بأنه "المجال الافتراضي الذي يتكون من الأنظمة الإلكترونية المترابطة والبيانات التي تنتقل عبر الشبكات الإلكترونية، كما يمثل الفضاء السيبراني بيئة تفاعلية تتألف من الأنظمة المعلوماتية والشبكات والكيانات الإلكترونية المتنوعة، بما في ذلك الأفراد والمؤسسات والحكومات والهجمات والتهديدات". كما يشمل الفضاء السيبراني جميع الأنشطة والتفاعلات التي تحدث عبر الشبكات الإلكترونية، بما في ذلك تبادل المعلومات والتواصل الإلكتروني

والتجارة الإلكترونية والأنشطة الحكومية والعسكرية والاجتماعية. كما يتضمن الفضاء السيبراني التهديدات والهجمات السيبرانية التي تستهدف الأنظمة والبيانات والمعلومات.

كما عرفته الهيئة الوطنية للأمن السيبراني "بالشبكة المترابطة من البنية التحتية لتقنية المعلومات، والتي تشمل الإنترنت وشبكات الاتصالات، وأنظمة الحاسب الآلي والأجهزة المتصلة بالإنترنت، إلى جانب المعالِجات وأجهزة التحكم المرتبطة بها، كما يمكن أن يشير المصطلح إلى عالم أو نطاق افتراضي كظاهرة مجربة أو مفهوم مجرّد".[7]

يعدّ الفضاء السيبراني بمثابة بيئة معقدة وديناميكية، حيث تتغير التهديدات والتحديات باستمرار وتتطور التكنولوجيا والتقنيات الهجومية. ولذلك، يتطلب الحفاظ على الأمان في الفضاء السيبراني جهوداً مستمرة ومتعددة الأطراف تشمل السياسات والتقنيات والتدابير الوقائية والاستجابية. وبما أن الفضاء السيبراني لا يعترف بالحدود الجغرافية ويمتد عبر العالم، فإن التعاون الدولي والتنسيق الدولي يعتبران أساسيين لمكافحة التهديدات السيبرانية وضمان الأمان والاستقرار في هذا الفضاء. [8]

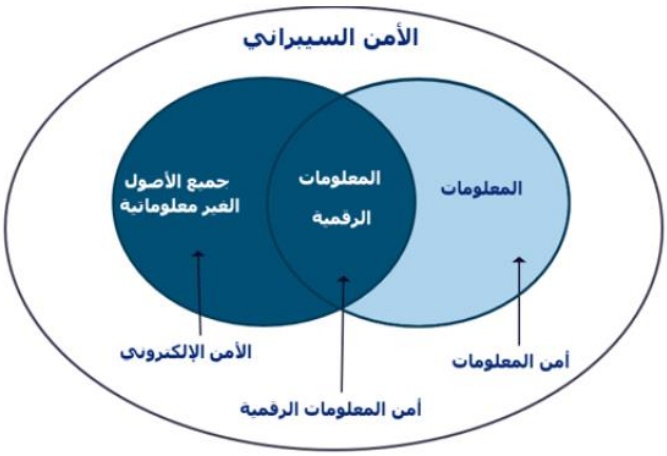
2- **الأمن الإلكتروني:**

يعرف بأنه "حماية الأنظمة الإلكترونية والبيانات والمعلومات من التهديدات والهجمات الإلكترونية، ويهدف إلى ضمان سرية وسلامة وسلامة البيانات والمعلومات، بما في ذلك حماية الأنظمة والبرمجيات من الاختراقات والاستيلاء غير المصرح به". ويمكننا التميز ين الأمن السيبراني والأمن الإلكتروني إذ يشيران إلى نفس الفكرة في الاطار العام من ناحية حماية الأنظمة الإلكترونية والبيانات، ولكن يمكن تمييز بعض الاختلافات الطفيفة بينهما وفق الآتي:- [9] (لاحظ الشكل رقم -1-)

- **مدى التطبيق:**
  - الأمن السيبراني عادة ما يكون أكثر شمولاً ويشمل جميع الجوانب المتعلقة بالحماية الإلكترونية بما في ذلك البيانات والأنظمة والشبكات والتهديدات السيبرانية.
  - الأمن الإلكتروني قد يكون محدودًا أكثر ويركز بشكل أكبر على حماية البيانات والمعلومات دون الاهتمام الكبير بالتهديدات السيبرانية الأخرى.

- **التركيز الجزئي:**
  - الأمن السيبراني يشمل جميع التهديدات الإلكترونية بما في ذلك الهجمات السيبرانية والاختراقات والبرمجيات الخبيثة والاحتيال الإلكتروني وغيرها.
  - الأمن الإلكتروني قد يتركز بشكل أساسي على حماية البيانات والمعلومات والتأكد من سلامتها وسريتها.
- **المصطلحات والاستخدامات:**
  - على الرغم من أن الكلمتين يتم استخدامهما في بعض الأحيان بشكل متبادل، إلا أن "الأمن السيبراني" غالبًا ما يشير إلى مفهوم أوسع وأكثر تعمقًا لحماية البيئة الإلكترونية.
  - بينما "الأمن الإلكتروني" قد يستخدم للإشارة بشكل أكثر تحديدًا إلى الجوانب المتعلقة بالحماية الإلكترونية للبيانات والمعلومات. بشكل عام، يمكن اعتبار الأمن السيبراني مفهومًا أوسع يشمل الأمن الإلكتروني كجزء منه، ويشير إلى الجهود الشاملة لحماية البيئة الإلكترونية بشكل عام. (10)

الشكل رقم (1) مكونات الامن السيبراني



المصدر: https://attaa.sa/library/view/868

3- **الحرب السيبرانية:**

تعرف بأنها "نوع من أنواع النزاعات القائمة على استخدام التكنولوجيا الإلكترونية والمعلوماتية في الهجوم والدفاع عن الأنظمة السيبرانية والبنية التحتية الرقمية. تختلف الحروب السيبرانية عن الحروب التقليدية في أنها تستخدم أساليب القرصنة الإلكترونية والاختراق السيبراني والبرمجيات الضارة والهجمات الموزعة للخدمة (DDoS) وغيرها من التقنيات لشن الهجمات والتأثير على الأنظمة الحيوية والبنية التحتية الرقمية للدول أو المؤسسات أو الأفراد".

فضلاً عن ذلك تشمل أهداف الحروب السيبرانية سرقة المعلومات السرية، والتجسس الصناعي، وتعطيل البنى التحتية الحيوية مثل الشبكات الكهربائية والمالية والاتصالات، وتقويض الاستقرار السياسي والاقتصادي للأعداء. قد تكون هذه الحروب مستندة إلى دوافع عسكرية، سياسية، اقتصادية، تجارية، أو حتى تكتيكية، كما تتميز الحروب السيبرانية بمرونتها وقدرتها على الخفاء، حيث يمكن للمهاجمين تنفيذ هجماتهم بشكل مجهول ومن دون أن يكشفوا عن هويتهم الحقيقية. كما أنها يمكن أن تكون غير متكافئة، حيث يمكن لهجمات صغيرة أن تتسبب في أضرار كبيرة.

لا شك تزداد أهمية الحروب السيبرانية مع تقدم التكنولوجيا وانتشار استخدام الإنترنت وتكامل الأنظمة الإلكترونية في جميع جوانب الحياة. ومع ذلك، يتطلب التصدي للحروب السيبرانية تنسيقاً دولياً وجهوداً متعددة الأطراف لتطوير السياسات والتشريعات اللازمة وتعزيز القدرات الدفاعية والاستجابة السريعة للتهديدات المتنامية في هذا المجال.[11]

4- **القوة السيبرانية:**

وتعرف بأنها "القدرة على استخدام التكنولوجيا السيبرانية والمعلوماتية بشكل فعال لتحقيق الأهداف الاستراتيجية والأمنية، تشمل القوة السيبرانية القدرة على الدفاع عن الأنظمة الإلكترونية والبنية التحتية الرقمية وحمايتها من الهجمات السيبرانية، فضلاً عن القدرة على شن هجمات سيبرانية بفعالية عند الضرورة، تتكون القوة السيبرانية من عدة عناصر أساسية، تتمثل بما يأتي:- [12]

أ. القدرات التقنية: تتضمن القدرات التقنية الخاصة بالأمان السيبراني مثل تطوير البرمجيات الأمنية، وتصميم أنظمة الشبكات المؤمنة، وتطبيق تقنيات التشفير والتحليل السيبراني.

ب. القدرات التنظيمية: تشمل هذه القدرات تنظيم الجهود والموارد لتنفيذ الأنشطة السيبرانية، وتطوير السياسات والإجراءات السيبرانية، وتوجيه الاستراتيجيات لحماية الأنظمة الحيوية والبنية التحتية.

ج. القدرات البشرية: تعتبر المهارات والخبرات الفنية للمحترفين السيبرانيين أحد العناصر الرئيسية في بناء القوة السيبرانية، حيث يتعين عليهم تحليل التهديدات والتحقق من الضعف في الأنظمة وتطبيق إجراءات الاستجابة عند الحاجة.

د. التعاون والشراكات: تتضمن القوة السيبرانية القدرة على التعاون مع الشركاء والحلفاء لمشاركة المعلومات والخبرات وتنفيذ الأنشطة السيبرانية المشتركة للحماية والدفاع عن الأنظمة والمعلومات.

ه. القدرة على التكيف والابتكار: يجب أن تكون القوة السيبرانية قادرة على التكيف مع التطورات التقنية والتهديدات السيبرانية المتغيرة بسرعة، وتطوير استراتيجيات جديدة وتقنيات مبتكرة للتعامل معها.

وبذلك فإن امتلاك هذه العناصر والقدرات، يمكن للدول والمؤسسات بناء استراتيجياتها السيبرانية وتعزيز قوتها السيبرانية لضمان الأمان والاستقرار في البيئة الرقمية المتزايدة التعقيد.

كما نجد ان الأمن السيبراني لإنترنت الأشياء ترتكز على أربع مكونات رئيسة هي: "حوكمة الأمن السيبراني، وتعزيز الأمن السيبراني، وصمود الأمن السيبراني، والأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية"، وقد تم تطوير الوثيقة والتي رُوعي فيها أفضل الممارسات العالمية للإرشادات، والمعايير، والأطر، والضوابط ذات الصلة بالأمن السيبراني، وتحليل ما تم رصده من الحوادث والهجمات السابقة، المتعلقة بإنترنت الأشياء .

المحور الثاني : تحديات وتهديدات الامن السيبراني

تشير التهديدات السيبرانية إلى أي خطر أو تهديد محتمل يمكن أن يؤثر سلباً على الأنظمة الإلكترونية والبيانات. تتنوع التهديدات السيبرانية بشكل كبير ويمكن أن تكون من مصادر مختلفة، وهناك العديد من أنواع من تهديدات للأمن السيبراني التي يواجهها الأفراد والمنظمات والدول بشكل مستمر، ويمكن أن تتراوح هذه بين هجمات التصيد الاحتيالي والبرامج الضارة وبرامج الفدية وهجمات الهندسة الاجتماعية. يجد مجرمو الإنترنت باستمرار طرقاً جديدة لاستغلال نقاط الضعف في أنظمة الكمبيوتر والشبكات، مما يجعل من الضروري للأفراد والمؤسسات مواكبة أحدث ممارسات الأمن السيبراني.

ويترتب على تهديدات الأمن السيبراني تداعيات وخيمة على الأفراد والمنظمات، ويمكن أن تشمل هذه الخسائر المالية، والإضرار بالسمعة، وفقدان المعلومات الحساسة، والتداعيات القانونية، فعلى سبيل المثال، أدى خرق بيانات Target في عام 2013 إلى سرقة 40 مليون رقم من أرقام بطاقات الائتمان والخصم، مما أدى إلى تسوية بقيمة 18. 5 مليون دولار، ومن أهم تلك التهديدات والاختراقات ما يأتي:- (13)

1- **تصيد المعلومات:** وهي عملية إرسال رسائل بريد إلكتروني احتيالية تشبه رسائل البريد الإلكتروني من المصادر الموثوقة، بهدف هو سرقة المعلومات الحساسة مثل أرقام بطاقة الائتمان ومعلومات تسجيل الدخول، ويعدّ أكثر أنواع الهجمات الإلكترونية شيوعًا.

2- **برامج الفدية:** وهي نوع من البرامج الضارة، وهي مصممة بهدف ابتزاز المال عن طريق منع الوصول إلى الملفات أو نظام الكمبيوتر حتى يتم دفع الفدية، ولا يضمن دفع الفدية استرداد الملفات أو استعادة النظام.

3- **البرامج الضارة:** وهي نوع من البرامج المصممة للوصول غير المصرح به إلى جهاز الكمبيوتر أو إلحاق الضرر به.او سرقة البيانات الخاصة والسرية، وتشمل الفيروسات وأحصنة طروادة وبرامج التجسس وأحصنة طروادة والتروجان وغيرها، والتي تصمم للدخول إلى الأنظمة وتسبب الأضرار أو سرقة البيانات.

4- **التحايل باستخدام الهندسة الاجتماعية:** ويعدّ هذا أسلوب يستخدمه الخصوم لاستدراجك إلى الكشف عن المعلومات الحساسة. يمكنهم طلب الحصول على دفع نقدي أو الوصول

إلى بياناتك السرية، ويمكن دمج الهندسة الاجتماعية مع أي من التهديدات المذكورة سابقًا لزيادة فرصتك في النقر على الروابط أو تنزيل البرامج الضارة أو الوثوق بمصدر ضار.

5- **اختراق الشبكات (Network Intrusion):** ويشمل هذا النوع من التهديدات محاولات اختراق الشبكات والأنظمة بشكل غير مصرح به، والتسلل إلى الأنظمة والسيطرة عليها أو سرقة البيانات.

6- **الهجمات الموزعة لخدمة (DDoS):** وتهدف هذه الهجمات إلى إغراق خوادم الويب أو الشبكات بحركة مرور غير مشروعة، مما يؤدي إلى تعطيل الخدمات والمواقع على الإنترنت.

7- **التهديدات الداخلية (Insider Threats):** وتشمل هذه التهديدات الهجمات أو التسريبات التي يقوم بها الموظفون أو المتعاونون الداخليون بالمؤسسة.

8- **الهجمات السيبرانية المتقدمة (Advanced Persistent Threats - APTs):** وتشير إلى هجمات متطورة ومستمرة تستهدف الأنظمة الحساسة والبيانات لفترات طويلة دون اكتشاف. (14)

9- **الذكاء الاصطناعي:** يعد الذكاء الاصطناعي تقنية سريعة التطور ويمكن استخدامها لإنشاء هجمات سيبرانية أكثر تعقيدا وقوة، مما يجعل من الصعب اكتشافها والتصدي لها، حيث يمكن استخدام الذكاء الاصطناعي لإنشاء برامج ضارة أكثر ذكاء يمكنها التهرب من تقنيات الأمان التقليدية، كما يمكن أيضا استخدام الذكاء الاصطناعي لإنشاء هجمات تستهدف البنية التحتية الحيوية، مثل شبكات الطاقة أو نظم النقل.

10- **الهجمات الهجينة:** وتَستخدم الهجمات الهجينة مزيجا من الأساليب التقليدية وغير التقليدية، وتتميز بأنها أكثر تعقيدا وصعوبة في الاكتشاف والحماية منها مقارنة بالهجمات التقليدية.

11- **التهديدات السيبرانية للصحة الرقمية:** قد تستهدف أجهزة الرعاية الصحية أو نظم السجلات الطبية، وذلك لأنها حساسة للغاية ويمكن استخدامها لأغراض ضارة، مثل الابتزاز أو التجسس أو حتى إلحاق الضرر الجسدي.

12- **هجمات اختراق التحكم في الطائرات المسيرة:** أصبح استهداف الطائرات المسيرة أو أنظمة التحكم فيها محط اهتمام متزايد، وقد تتسبب هذه الهجمات بأضرار جسيمة، بما في ذلك تعطيل الطائرات أو سرقة البيانات أو حتى إسقاطها. (15)

في هذا الصدد يمكن تحديد العوامل والمحفزات التي تزيد وتعزز من تهديدات الأمن السيبراني في عدة نقاط، أهمها الاتي:- (16)

- تطور التهديدات :يتطور مجال الهجمات السيبرانية بشكل مستمر، حيث يبتكر المهاجمون تقنيات جديدة لاختراق الأنظمة والشبكات. هذا يجعل تحديد التهديدات والتصدي لها تحدياً مستمراً.
- نقص الموارد والخبرة :قد تفتقر بعض المؤسسات إلى الموارد اللازمة لتنفيذ إستراتيجيات الأمن السيبراني بشكل كامل، كما قد تفتقر إلى الخبرة والمهارات الفنية اللازمة للتعامل مع التهديدات الحديثة.
- التوافق مع التشريعات والمعايير: قد تواجه المؤسسات تحديات في مواكبة التشريعات والمعايير الأمنية المتغيرة وضمان الامتثال بها، مما يزيد من تعقيدات تطبيق الأمن السيبراني.
- الاعتماد على التكنولوجيا المتطورة: إذ يعتمد الأمن السيبراني بشكل كبير على التكنولوجيا المتطورة مثل أنظمة الكشف عن الاختراق والحماية من الفيروسات، وهذا يتطلب استثمارات مستمرة في التحديث والتطوير.
- التحديات البشرية :يشمل الأمن السيبراني أيضاً تحديات بشرية مثل سوء الاستخدام، والتحديات الاجتماعية مثل هجمات الاحتيال الاجتماعي التي تستهدف الأفراد داخل المؤسسات.

ومما تقدم نرى ان إدراك صانع القرار للتهديدات والتصدي لها يعدّ جزءًا مهمًا من استراتيجية الأمن السيبراني لأي منظمة أو مؤسسة، حيث تساهم في حماية الأنظمة والبيانات وضمان استمرارية العمليات.

المحور الثالث: نحو استراتيجية وطنية للأمن السيبراني العراقي

تمثل استراتيجيات الأمن السيبراني إطاراً شاملاً لحماية الأنظمة الإلكترونية والمعلوماتية من التهديدات السيبرانية، وتتضمن هذه الاستراتيجيات جملة من الإجراءات والعناصر والتقنيات التي تهدف إلى تقليل المخاطر وزيادة الوقاية والتحقق من الامتثال.

- **إجراءات استراتيجية الأمن السيبراني**

تشمل إجراءات الأمن السيبراني العديد من الجوانب والتقنيات والسياسات التي تهدف إلى حماية الأصول الرقمية والتصدي لتلم التهديدات السيبرانية والتي ينبغي على الجهات الأمنية العراقية الأخذ بها، ومن بين هذه الإجراءات ما يأتي [17] :

- **حماية الشبكات والأنظمة:** تتضمن هذه الجوانب استخدام التشفير، وتطبيق الحواجز النارية وأجهزة الكشف عن التسلل، وتحديث البرمجيات بانتظام لسد الثغرات الأمنية المعروفة.
- **إدارة الهويات والوصول:** يتضمن ذلك تحديد الصلاحيات ومنح الوصول فقط للأشخاص الذين يحتاجون إليه، وتطبيق مبادئ أقل الامتياز لتقليل مخاطر الوصول غير المصرح به.
- تحليل الأمان ورصد الحوادث: يشمل ذلك استخدام أدوات رصد الحوادث لتحديد ومراقبة الأنشطة الغير معتادة على الشبكة، والتحقق من الانتهاكات الأمنية والاستجابة لها بشكل سريع.
- تطبيق السياسات الأمنية: يتضمن ذلك وضع سياسات وإجراءات أمنية صارمة وتنفيذها لضمان الامتثال القانوني والتنظيمي والتصدي للتهديدات السيبرانية.

- **عناصر استراتيجية الامن السيبراني:**

في سياق الأمن السيبراني، هناك عدة عناصر اساسية يمكن أن تشكل منطلقاً لإدراك التهديدات والتحديات وتطوير قدرات الاستجابة الاستراتيجيات الفعالة للحماية، ومن أهمها ما يأتي:- [18]

- الدفاع الشامل (Defense in Depth): هذه عصار الاستراتيجية السيبرانية، وتشير إلى استخدام مجموعة متعددة من التدابير الأمنية على مستويات متعددة داخل النظام السيبراني، بدءاً من الحماية الأولية مثل جدران الحماية وانتهاءً بالحماية على مستوى التطبيقات والبيانات، هذا يزيد من الصعوبة التي تواجه المهاجمين ويزيد من فرص اكتشاف الهجمات وإحباطها.

- مبدأ أقل الامتياز (Principle of Least Privilege): وفقاً لهذا المبدأ، يجب أن يتم منح الوصول إلى الموارد السيبرانية والبيانات فقط للأشخاص الذين يحتاجون إليها لأداء مهامهم، وهذا يقلل من فرص الوصول غير المصرح به ويقيد نطاق الأضرار في حالة التعرض لهجوم.

- التوعية والتدريب (Awareness and Training): يعدّ تعزيز التوعية بأمان المعلومات وتدريب الموظفين على ممارسات الأمان السيبراني أمراً أساسياً في بناء ثقافة أمنية قوية داخل المؤسسات. فهذا يقلل من مخاطر الاختراقات الناجمة عن أخطاء الإنسان.

- التحليل التنبؤي (Predictive Analysis): ويستخدم التحليل التنبؤي لتحليل السلوكيات والأنماط التي يمكن أن تشير إلى هجمات محتملة في المستقبل. يتيح هذا النهج اتخاذ إجراءات تصحيحية مبكرة لتقليل التأثير السلبي للهجمات المحتملة.

- الاستجابة السريعة والاستعادة (Rapid Response and Recovery): إذ يجب على المؤسسات تطوير خطط استجابة سريعة للتعامل مع الحوادث الأمنية واستعادة الأنظمة والبيانات إلى حالتها الطبيعية بأقصر وقت ممكن بعد وقوع الهجمات.

وبذلك فان هذه العناصر تساعد في بناء استراتيجيات فعالة للأمن السيبراني وتعزز قدرة الدول على التصدي للتهديدات السيبرانية بفعالية.

- **أساليب وتقنيات استراتيجية الأمن السيبراني**

تتضمن استراتيجيات الأمن السيبراني مجموعة متنوعة من الأساليب والتقنيات التي تهدف إلى حماية الأنظمة الإلكترونية والبيانات من التهديدات السيبرانية. إليك بعض الأساليب الشائعة في استراتيجيات الأمن السيبراني:- [19]

- التشفير (Encryption): ويستخدم التشفير لحماية البيانات من الوصول غير المصرح به عن طريق تحويلها إلى شكل غير قابل للقراءة دون المفتاح الصحيح. كذلك تشفير في الرسائل الإلكترونية والاتصالات عبر الإنترنت وفي حفظ البيانات على الأقراص الصلبة والأجهزة النقالة.

- تطبيق السياسات الأمنية (Security Policy Implementation): وتتضمن تحديد وتطبيق سياسات الأمن السيبراني التي تحدد السلوكيات والممارسات الأمنية المطلوبة للموظفين والمستخدمين، كما يشمل تطبيق السياسات متطلبات مثل كلمات المرور القوية وتحديد الوصول والنسخ الاحتياطي للبيانات والتحديثات الأمنية الدورية.

- إدارة الهويات والوصول (Identity and Access Management): ويتمثل في تحديد الهويات الرقمية للمستخدمين وتنظيم الوصول إلى النظام والبيانات بناءً على الصلاحيات المناسبة، فضلاً عن إدارة الهويات والوصول إنشاء وإدارة حسابات المستخدمين وتنفيذ ميزات التحقق الثنائي وتتبع النشاطات.

- رصد واستجابة الحوادث (Incident Monitoring and Response): ان رصد الأنشطة غير المعتادة على الشبكة والأنظمة بهدف اكتشاف الاختراقات المحتملة، والاستجابة لحوادث التحقيق في الاختراقات المكتشفة واتخاذ الإجراءات اللازمة للتصدي لها وتصحيح الثغرات.

- تحليل الأمان والتقارير (Security Analysis and Reporting): يتضمن تقديم تقارير دورية حول حالة الأمان السيبراني وتحليل السجلات والبيانات لتحديد الأنماط الغير معتادة أو الهجمات المحتملة، كما يساعد هذا النوع من التحليل في اتخاذ القرارات الاستباقية وتطوير السياسات الأمنية بشكل أفضل.

وماتقدم نرى ان فعالية استراتيجيات الأمن السيبراني في تكامل هذه الإجراءات والعناصر الأساليب وتنفيذها بشكل شامل لضمان حماية الأنظمة والبيانات من التهديدات السيبرانية بشكل فعال.

- **أنواع استراتيجيات الأمن السيبراني**

تتضمن استراتيجيات الامن السيبراني استراتيجيات دفاعية وهجومية، وكما يأتي:

1- **استراتيجيات الدفاع السيبراني** تهدف إلى تحقيق الأمان والحماية للأنظمة الإلكترونية والبيانات من التهديدات السيبرانية. تتضمن هذه الاستراتيجيات مجموعة من الخطوات والتدابير التي يمكن اتخاذها لتقليل مخاطر الاختراقات والهجمات السيبرانية، ومن أهم مبادئ استراتيجيات الدفاع السيبراني ما يأتي:- [20]

- **تطبيق الأمان في العمق (Defense in Depth):** يتضمن هذا النهج استخدام تدابير أمنية متعددة على عدة مستويات داخل البنية التحتية للأمان، بما في ذلك الشبكات والأجهزة والبرمجيات. يعمل هذا النهج على زيادة الصعوبة التي تواجه المهاجمين وتقليل التأثير المحتمل للهجمات.

- **تقييم المخاطر وإدارتها (Risk Assessment and Management):** يتضمن هذا النهج تحليل الثغرات والضعف في الأنظمة وتقييم المخاطر المحتملة المرتبطة بها، واتخاذ التدابير الوقائية اللازمة لتقليل هذه المخاطر إلى أدنى حد ممكن.

- **تحديث البرمجيات والأنظمة بانتظام (Regular Software and System Updates):** يتضمن هذا الإجراء تنفيذ التحديثات الأمنية والإصلاحات الضرورية للبرمجيات والأنظمة بانتظام، وذلك لسد الثغرات الأمنية المعروفة وتقليل خطر الاختراقات.

- **تحسين التحليل السيبراني (Enhanced Cyber-security Analysis):** يتمثل هذا النهج في استخدام تقنيات التحليل السيبراني المتطورة لرصد واكتشاف التهديدات بشكل فعال، وتحليل السلوكيات غير المعتادة التي قد تشير إلى هجمات محتملة.

- **تعزيز التعاون والمشاركة (Enhanced Collaboration and Sharing):** يتضمن هذا النهج التعاون مع الشركاء والجهات المعنية الأخرى لمشاركة المعلومات والخبرات حول التهديدات السيبرانية وتبادل الأفكار والأفضليات في مجال الدفاع السيبراني.

هذه المبادئ الاستراتيجية ليست بالضرورة مستقلة عن بعضها البعض، بل يمكن أن تتكامل معًا لتعزيز القدرة على التصدي للتهديدات السيبرانية بفعالية أكبر.

2- الاستراتيجية الهجومية السيبرانية: تتمثل في استخدام التكنولوجيا السيبرانية والمعلوماتية لشن هجمات واختراقات على أنظمة الخصم أو الهدف بهدف تحقيق أهداف معينة. تتنوع أهداف هذه الهجمات والاختراقات بشكل كبير وتشمل ما يلي:- (21)

- **تجسيد البنية التحتية:** يمكن للاستراتيجية الهجومية السيبرانية استهداف بنية تحتية حيوية في الدولة المعنية مثل الكهرباء أو المياه أو الاتصالات بهدف التعطيل أو التخريب.

- **التجسس وسرقة المعلومات الحساسة:** تهدف الهجمات السيبرانية الهجومية إلى سرقة المعلومات الحساسة مثل الأسرار التجارية أو البيانات الحكومية للاستفادة منها أو للتأثير على السياسات أو القرارات.

- **التدمير والتخريب:** يمكن أن تتضمن الهجمات الهجومية السيبرانية الهدف من تدمير البنية التحتية الرقمية بشكل مستمر أو تخريب الأنظمة بحيث يصعب إصلاحها.

- **التلاعب بالمعلومات والتضليل:** تستخدم بعض الهجمات الهجومية السيبرانية لتشويه البيانات أو تضليل الخصم بالمعلومات الكاذبة بهدف تشويه سمعته أو تشويه صورته.

- **الهجمات الموجهة نحو الأفراد والمؤسسات:** يمكن أن تشمل الهجمات الهجومية السيبرانية استهداف الأفراد أو المؤسسات بغية الابتزاز أو السرقة أو الضغط السياسي.
- **الهجمات المستهدفة نحو البنية التحتية العسكرية:** تتمثل في استخدام التكنولوجيا السيبرانية لاختراق وتعطيل الأنظمة العسكرية للخصم.

كما تستند الاستراتيجية الهجومية السيبرانية على استخدام التقنيات السيبرانية المتقدمة وتطوير أساليب مبتكرة للهجوم والتسلل، وتعدّ هذه الاستراتيجية جزءًا من استراتيجية أوسع للقوة السيبرانية وتستخدم كأداة لتحقيق الأهداف السياسية أو العسكرية أو الاقتصادية للقوى الدولية والمتنافسة.

- **استراتيجية الأمن السيبراني العراقي:**

أعلنت مستشاريَّة الأمن الوطني منذ 2017عن استراتيجيَّة الأمن السيبراني العراقي، لتوفير التدابير المتماسكة والإجراءات لضمان أمن وحماية الوجود العراقي في الفضاء السيبراني، وحماية البنية التحتيَّة الحيويَّة للمعلومات، وبناء ورعاية مجتمع شبكات انترنت موثوق فيه، وحدد التهديدات السيبرانيَّة الرئيسة لاسيما (الجريمة الإلكترونية، والإرهاب الإلكتروني، والصراع السيبراني، والتجسس السيبراني، الى جانب إساءة معاملة الاطفال واستغلالهم الكترونياً... وغيرها)، وشددت الاستراتيجية على ضرورة تقييم مواطن الضعف الوطنية في المجال السيبراني وقياس الآثار والفرص، بهدف الاسهام في إحداث تشريعات شاملة لمكافحة الجريمة السيبرانية والتدابير المضادة للتهديد السيبراني، وتطوير امكانات الامن السيبراني على جميع مستويات الدولة في العراق. (22)

كما وضعت الاستراتيجية خريطة طريق تفصيليَّة من ثمانية محاور، متمثلة بالآتي: (الحكومة الفعالة، والاطار التشريعي والتنظيمي، واطار تكنولوجيا الأمن السيبراني، وثقافة الامن السيبراني وبناء القدرات، والبحث والتطوير نحو الاعتماد على الذات، والامتثال والتنفيذ، والجاهزية لحوادث الأمن السيبراني، الى جانب التعاون الدول).

فضلاً عن ذلك جرى الإعلان عن فريق وطني مشترك مختص للاستجابة للحوادث السيبرانية وحماية البنية التحتية للانترنت ونشر الوعي في مجال حماية الخصوصية والحماية الذاتية للأفراد والمؤسسات على الانترنت يعمل تحت إشراف مستشارية الأمن الوطني العراقي(23).

كما يتولى الفريق مسؤولية تأمين وحماية الشبكات ومراكز البيانات الوطنية والمواقع الرسمية التي تعمل في مجال الفضاء السيبراني العراقي ويقوم بتنسيق الجهود الوطنية، ودعم المؤسسات في القطاعين العام والخاص في حماية نفسها وخدماتها في الفضاء السيبراني، وتحقيق الرصانة والموثوقية للأنظمة الالكترونية، وتعزيز ثقة المواطن بالمؤسسات والارتقاء بمستوى العراق دولياً في مجال الامن السيبراني لتشجيع تطوير الخدمات الالكترونية ودعم مشروع أتمتة الخدمات والحكومة الالكترونية. (24)

ويهدف الفريق الى الاستجابة للحوادث الأمنية والحد من آثارها وتوفير تدابير استباقية لتلافي هذه الحوادث، وبناء الأطر الوطنية للأمن السيبراني لتشجيع التعاون بين القطاعين العام والخاص وتبادل المعلومات، وزيادة الثقة في استخدام الخدمات الإلكترونية الحكومية، وتعزيز الوعي الأمني لمستخدمي انظمة تكنولوجيا المعلومات والإنترنت، وتطوير القدرات الأمنية لمدراء أنظمة تكنولوجيا المعلومات للتعامل مع الحوادث الأمنية، وتحليل التهديدات الأمنية وتأثيرها وتوفير معلومات عن آخر الحوادث وطرق تجنبها، وبناء مركز معتمد لتسلم البلاغات عن الحوادث السيبرانية، وتشجيع البحث والتطوير في مجال الأمن السيبراني، والتعاون المشترك مع فرق الاستجابة والمنظمات على الصعيدين الإقليمي والدولي . (25)

وقد صنف المؤشر العالمي للأمن السيبراني (جي سي آي) الذي أصدره الاتحاد الدولي للاتصالات التابع للأمم المتحدة أربع دول عربية فقط في (المستوى المرتفع) عام ٢٠١٨،وهي(السعودية، عمان، قطر، مصر)، أما العراق فقد احرز تقدم، اذ جاء بالمرتبة (107) عالمياً و(13) عربياً. ويرصد التقييم الذي شمل (175) دولة على مستوى العالم الممارسات والأدوات التي تستخدمها الدول لحماية الأنظمة والشبكات والبرامج من الهجمات الرقمية. ويشير الاتحاد الدولي للاتصالات إلى أن "الرقم القياسي العالمي للأمن السيبراني يقيس مدى التزام البلدان في مجال الأمن السيبراني، وفقاً للدعائم الخمس للبرنامج العالمي للأمن السيبراني، وهي (التدابير القانونية، والتدابير التقنية، والتدابير التنظيمية، وبناء القدرات، والتعاون). (26)

قطعت وزارة الداخلية أشواطاً متقدمة في مجال إرساء قواعد الأمن السيبراني في العراق، لا سيما ما يتعلق بمحوري الجريمة الإلكترونية، والإرهاب الإلكتروني، وتمكّنت من توفير عناصر متدربة على المهارات الرقميَّة المتقدمة لمواجهة تلك الجرائم، في مديرياتها بجميع المدن

العراقية، ووفرت متطلبات الإبلاغ السريع عن تلك الجرائم، فضلاً عن قيامها بحملات توعية الشرائح العراقيَّة المختلفة بمخاطرها، ووسائل تجنبها من قبل الأفراد العاديين، عن طريق الحملات الإعلاميَّة والإلكترونيَّة والندوات الحواريَّة والتثقيفيَّة. (27)

وتهدف الاستراتيجية الوطنية العراقية للأمن السيبراني وضع خارطة طريق وطنية مع آليات منسقة مختلفة؛ إطار تنفيذي؛ والإجراءات التي تضمن تحقيق الرؤية الوطنية والاهداف المتعلقة بالأمن السيبراني لاسيما أهمها ما يأتي:- (28)

- صياغة تشريعات شاملة لمكافحة الجريمة السيبرانية والتدابير المضادة للتهديد السيبراني التي يمكن اعتمادها على الصعيد الوطني والإقليمي والعالمي ذات الصلة في سياق تأمين الفضاء السيبراني للبالد.
- توفير التدابير التي تحمي البنية التحتية الحيوية للمعلومات، فضلاً عن الحد من مواطن الضعف والثغرات.
- وضع آلية فعالة للاستجابة لحالات الطوارئ والعمل على تحسين قدرة وتطوير فريق الاستجابة
- وضع آلية موثوقة لإشراك أصحاب المصلح المتعددين و الوطنيين والدوليين من أجل التصدي بشكل جماعي للتهديدات السيبرانية.
- ردع وحماية الحكومة من جميع أشكال الهجمات السيبرانية

الخاتمة

لاشك واقع الأمن السيبراني العراقي، لازال يتعرض لمخاطر وتهديدات مستمرة، وهذا يتطلب استحداث هيئة وطنية موحدة للعمل المشترك بين جميع التشكيلات والفرق الإلكترونية للأجهزة العراقية، التي يمكن أنْ تشكّل البنية التحتيَّة والأساس لذلك، ضمن مسار الاستراتيجية الوطنية للأمن السيبراني، وبصلاحيات متوازنة مع مهامها وأهدافها، وبما يساهم في تأمين البلاد في البعد الخامس للحروب السيبرانية المعاصرة، إلى جانب تشريع القوانين المناسبة لمواجهة الجرائم السيبرانيَّة، وفقاً للمتغيرات المعاصرة، وإرساء ثقافة تعزيز الأمن السيبراني على صعيدي المؤسسات الحكومية وغير الحكومية والأفراد، وتشجيع البحث العلمي المتعلق بتطوير هذه المجالات، فضلاً عن تدريب وتنمية المهارات الرقميَّة بشكلٍ مستمر، لمواكبة المستجدات الإلكترونيَّة، على المستويين الداخلي والخارجي.

المصادر والمراجع:

* تعرف كلمة سايبر Cyber بانها مشتقة من Cybernetic وأصلها يوناني وتعني التوجيه والسيطرة، وعرفها Norbert Wiener في عام 1984م "الدراسة العلمية للسيطرة على الأحياء والآلات وآلية التواصل بينها.

1 See in: Chen, Thomas M. Jarvis, Lee, Cyber terrorism: Understanding, Assessment, and Respons, New York: Springer, June 2014, P 21.

2 الهيئة الوطنية للأمن السيبراني،الضوابط الأساسية للأمن السيبراني، 2018، على الرابط https://nca.gov.sa.

3 فارس محمد إبراهيم ،الأمن السيبراني :المفهوم وتحديات العصر، دار الخليج للنشر والتوزيع ،عمان ، 2022، ص ص 8-9.

4 سمير بلي، التهديدات الأمنية السيبرانية: دراسة في انعكاسات الحرب الالكترونية على الامن القومي للدول واستراتيجيات المقاومة، مجلة الرسالة، العدد 2، الجزائر، 2023، ص 190.

5 للمزيد ينظر: البانا إيسيني، الذكاء الاصطناعي والامن السيبراني: دراسة فيما يخبئه المستقبل، مركز البيان للدراسات والتخطيط، 2014، ص5.

6 See: Chen, Thomas M.;Jarvis, Lee , Op Cit, P 23.

7See: National Institute of Standards and Technology NIST, on link : https://csrc.nist.gov/glossary /National Institute of Standards and Technology NIST.

8 للمزيد ينظر: ياسمين وعمروش الحسين، التهديدات الالكترونية والامن السيبراني في الوطن العربي، مجلة نوميروس الاكاديمية، العدد الثاني، الجزائر، 2021، ص 165.

9 للمزيد ينظر: عبدالله جعفري، التهديدات السيبرانية وتأثيرها على الامن القومي الجزائري، المجلة الافريقية للدراسات القانونية والسياسية، العدد 2، جامعة احمد دراية، الجزائر، 2022، ص 246.

10 خالد محمد الربيش، أمن المعلومات مجال حيوي يمسّ فئات المجتمع كافة.. والأمن السيبراني جزء من السيادة الوطنية، صحيفة الرياض، الأربعاء 5 ربيع الآ خر 1440هـ -12 ديسمبر 2018، ص 8.

11 سمير بلي، مصدر سبق ذكره، 196.

12 حنان عباس سلمان و ابتسام كاظم جاسم، مصدر سبق ذكره، ص ص 624-625.

13 سمير بلي، مصدر سبق ذكره، 197-198. وكذلك: عبدالله جعفري، مصدر سبق ذكره، ص 246.

14 للمزيد ينظر: حورية قصعة، تداعيات التهديدات الأمنية في الفضاء الإفريقي على الأمن القومي الجزائري دراسة في تطورات الأزمة الليبية،مجلة البحث القانن و السياسية، العدد 1، الجزائر، 2022، ص 55.

15 أحمد عنتر،تقنيات الأمن السيبراني والتحديات المستقبلية، مركز الجزيرة للدراسات، 2023، على الرابط: https://www.aljazeera.net/tech/2023/12/4

16 ينظر: حورية قصعة، مصدر سبق ذكره، ص57.

17 يسرى ستار، الامن السيبراني في العراق، تقدر موقف، مركز رواق بغداد، تشرين ثاني،2022، ص6.

18 احمد بطو، عناصر الأمن السيبراني، على الرابط: https://cyberone.co

19 للمزيد ينظر: طواهير عبد الجليل، استراتيجيات الامن السيبراني كتحدي للتحول الرقمي بالمنظمات الحكومية مع الإشارة لتجربة دولة الامارات العربية المتحدة، مجلة الرسالة، العدد 1، الجزائر، 2023، ص 286.

20 سمير بلي، مصدر سبق ذكره، 199.

21 المصدر نفسه، ص 198.

22 صفد الشمري، ما واقع الأمن السيبراني في العراق؟، جريدة الصباح، 2021/06/08، على الرابط: https://alsabaah.iq/48007-.html
23 استراتيجية الامن السيبراني العراقي, مستشارية الامن الوطني, امانة سر اللجنة الفنية العليا للامن الاتصاالت والمعلومات, ص 2.
24 ينظر: يسرى ستار، مصدر سبق ذكره، ص4.
25 استراتيجية الامن السيبراني العراقي, مستشارية الامن الوطني, امانة سر اللجنة الفنية العليا للامن الاتصالات والمعلومات, ص 3.
26 محمد جبر، الهجمات السيبرانية وخطورتها على الامن الوطني العراقي والخصوصية، مركز النهرين للدراسات الاستراتيجية، 2019، على الرابط: https://alnahrain.iq/post/450
27 استراتيجية الامن السيبراني العراقي, مستشارية الامن الوطني, امانة سر اللجنة الفنية العليا للامن الاتصالات والمعلومات, ص 4.
28 المصدر نفسه, ص 6.

البحوث والدراسات الأمنية

- السياسات الاستراتيجية العراقية في مواجهة تداعيات التغيرات المناخية على الامن الوطني العراقي.

م.د. فراس عباس هاشم

- الأساس القانوني لدور مجلس الأمن والمحكمة الجنائية الدولية في مكافحة الجرائم الدولية.

العقيد انصيف جاسم محمد التكريتي

- الحرب الروسية – الأوكرانية وتداعياتها على أمن الطاقة للاتحاد الأوروبي.

م.م. عبد الرحمن عبد القادر عبد الله

- أمن المعلومات بين الضرورات الآنية والتدابير المستقبلية.

م.م. إبراهيم محمد محمود الجبوري

البحوث والدراسات الامنية

السياسات الاستراتيجية العراقية
في مواجهة تداعيات التغيرات المناخية على الأمن الوطني العراقي

م.د. فراس عباس هاشم
جامعة البصرة/ كلية القانون

تبحث هذه الدراسة في التحديات المتسارعة التي تواجها منطقة الشرق الأوسط بسبب ظاهرة التغيرات المناخية كان لها تأثيراتها على العديد من دول المنطقة. كما تناقش الدراسة سياسات العراق في إعادة صياغة مقتربات استراتيجيته الوطنية لمواجهة تنامي مخاطر تغيرات المناخ وتحييد تأثيراتها . كما تعرض الدراسة التحديات المختلفة التي تواجه العراق في مواجهة تغيرات المناخ وتداعياتها الداخلية. وتم تقسيم الدراسة إلى ثلاث محاور: يقدم الأول: التغيرات المناخية في الشرق الأوسط ودلائل تأثيراتها على العراق. ويعرض الثاني: مكونات الاستراتيجية العراقية تجاه التغيرات المناخية وديناميكياته. ويتناول الثالث: العراق وفجوة الأداء في مسارات مواجهة تغيرات المناخ وديناميته.

الكلمات المفتاحية: العراق، التغير المناخي، الشرق الأوسط، الاستراتيجية، الأمن الوطني.

Iraqi Strategic Policies
in the Confrontation of the Repercussions of Climate change on Iraqi National Security

Dr. Firas Abbas Hashem
University of Basra/College of Law

This study examines the accelerating challenges facing the Middle East region due to the phenomenon of climate change, which has had its effects on many countries in the region. The study also discusses Iraq's policies in reformulating its national strategy approaches to confront the growing risks of climate change and neutralize their effects. The study also presents the various challenges facing Iraq in confronting climate change and its internal repercussions. The study was divided into three axes: The first presents: climate changes in the Middle East and evidence of their effects on Iraq. The second presents: the components of the Iraqi strategy towards climate change and its dynamics. The third deals with: Iraq and the performance gap in ways to confront climate change and its dynamics.

Keywords: Iraq, climate change, the Middle East, strategy, national security.

الاستلام 2024/02/04
الارجاع 2024/04/12
القبول 2024/05/28

المقدمة

مما لا شك فيه أن منطقة الشرق الأوسط تواجه تحديات متسارعة بسبب ظاهرة التغيرات المناخية كان لها تأثيراتها على العديد من دول المنطقة لا سيما في المجالات المرتبطة بالتصحر والجفاف وانخفاض معدلات هطول الامطار وارتفاع درجات الحرارة وتضاعف مستويات الغازات في الغلاف الجوي، وهي بذلك تشكل مخاطر تهدد أمن دول الإقليم، وبناء عليه تجد بلدان المنطقة نفسها أمام متغير بيئي يستلزم منها اتخاذ إجراءات للحد من تلك الآثار الناجمة عن تغير المناخ.

ومن هنا أصبح الأمن الوطني العراقي يواجه تحديات ناتجة من تغيرات المناخ، تفرض عليه إعادة توجيه سياسته الاستراتيجية من أجل وضع التدابير الضرورية لمواجهة تنامي مخاطر تغيرات المناخ، والتي فاقمت من أشكال التحدي في ظل بنيته المؤسسية الهشة ومحدودية قدراته الوطنية، لذلك ومن أجل التخفيف من آثار تغيرات المناخ، سعى العراق نحو تبني مبادرات تهدف إلى إحداث تحولات بإدارة ملف التغيرات المناخية .

أضف إلى ذلك حاول العراق ضمن استراتيجيته الوطنية للطاقة لعام 2030 العمل على تنويع مصادر الطاقة عبر الاستثمار في الطاقة المتجددة من خلال بناء شراكات استراتيجية عالمية وإقليمية، بهدف الحد من آثار تغيرات المناخ، إلا أن مساعي العراق الاستراتيجية تواجه العديد من التحديات التي لها أبعاد مختلفة تضعف من قدرته على مواجهة تطورات الأزمات المتصاعدة نتيجة تغيرات المناخ وتعرضه إلى مزيد الضغوط الاجتماعية والاقتصادية والبيئة بالإضافة إلى عدم الاستقرار السياسي.

وعليه تنطلق أهمية الدراسة من كونها تبحث في حدود السياسات العراقية وتدابيرها في مواجهة آثار التغيرات المناخية وتداعياتها الأمنية والتي أصبحت تشكل محوراً مهماً من محاور التحركات الحكومية العراقية في الوقت الراهن.

وتنطلق الدراسة من إشكالية مفادها: شكلت متغيرات المناخ التي واجهها العراق دافعاً نحو توجهات الحكومة العراقية في صوغ سياساتها للتحول نحو نهج اقتصادي منخفض للانبعاثات الغازية، ويعزز تحوله بالاهتمام بالطاقة المتجددة، وبالتالي تحاول الدراسة الاجابة على مجموعة من التساؤلات: ما هي انماط التهديدات الامنية التي فرضتها تغيرات المناخ؟.

كيف استجابت الحكومة العراقية لمخاطر تغيرات المناخ . وماهي الاليات الاستراتيجية التي اعتمدتها الحكومة العراقية لمواجهة التغير المناخي ؟. وماهي التحديات التي تواجه الحكومة العراقية وتزيد من بطء اجراءاتها للحد من تغيرات المناخ.

وبالتالي تقوم الدراسة على فرضية مفادها :"تعكس سياسات التحول في الأداء الحكومي العراقي من أجل مواجهة التغير المناخي، تطوراً في إجراءاته الاستراتيجية نحو بناء قدراته على تنفيذ أهدافه الوطنية في التعامل مع تداعيات تغير المناخ وآثاره على أمنة الوطني".

ملامح التحول في الاستراتيجية الوطنية للعراق ، عبر ترسيم

واتساقاً مَع ما تقدم سيتم توزيع هيكلية الدراسة إلى ثلاث محاور. يركز المحور الأول : التغيرات المناخية في الشرق الأوسط ودلائل تأثيراتها على العراق. أما المحور الثاني يتناول: مكونات الاستراتيجية العراقية تجاه التغيرات المناخية وديناميكياتها. فيما تَناول المحور الثالث : العراق وفجوة الأداء في مسارات مواجهة تغيرات المناخ وديناميته.

المحور الأول: التغيرات المناخية في الشرق الأوسط ودلائل تأثيراتها على العراق

لا شك فيه أن قضية التغيرات المناخية أصبحت موضع الاهتمام العالمي في جميع الأقاليم الجغرافية المختلفة، لا سيما منطقة الشرق الأوسط، التي باتت تواجه تأثيرات التغيرات المناخية، ونتيجة لذلك شهد العراق اهتماماً ملحوظا في سياساته لمواجهة آثار التغيرات المناخية من حيث جعلها أولوية في سلم الاهتمامات وهو ما نشهده جارياً في وقتنا الحالي.

أولاً: التغيرات المناخية ومؤشرات التفاقم العالمي

يشهد المجتمع الدولي اهتماماً واسعاً بمسألة تغير المناخ (Climate change)، وباتت هذه القضية تحتل مكان الصدارة على جدول أعمال معظم الدول نتيجة لتأثيراتها في مناحي حياتنا البشرية، ووفقا للاتفاقية الإطارية للأمم المتحدة المعنية بتغير المناخ، تعزى تلك الظاهرة بصورة مباشرة أو غير مباشرة إلى النشاط البشري الذي يفضي إلى تغير في تكوين الغلاف الجوي (Atmosphere) العالمي، بالإضافة إلى تقلب المناخ الطبيعي على مدى فترات زمنية متباينة، وأكدت الاتفاقية على أن تغير المناخ ينتج عنه تضاؤل المساحات المغطاة بالثلوج، وتقلص الجليد البحري، وارتفاع مستويات البحار، ودرجات حرارة المياه، وزيادة تواتر

درجات الحر القصوى وموجات الحر، والأمطار الغزيرة وزيادة المساحات المتأثرة بالجفاف، واشتداد الأعاصير المدارية [1].

إضافة إلى ذلك زيادة الانبعاثات الكربونية(أنظر الرسم البياني رقم (1)) وارتفاع معدلات التلوث وهو ما أدى لأثار وتداعيات سلبية كثيرة على الحياة على وجه الأرض وعلى كثير من المجالات مثل تأثر الأمن الغذائي وتزايد الكوارث الطبيعية. وفى هذا الإطار تبرز التداعيات الأمنية للتغيرات المناخية ومنها تهديد الأمن الوطني[*] (National Security) للدول وكذلك تهديد السلم والأمن الدوليين, فضلاً عن تزايد الصراعات وظاهرة الإرهاب(Terrorism) في الكثير من مناطق العالم[2].

وإزاء ذلك تسهم التغيرات في النظم المناخية في تغيير مكونات الغلاف الجوي، ويتمثل الناتج الرئيسي لتلك الأنشطة في انبعاثات الغازات المسببة لظاهرة الاحتباس الحراري، وكما يلاحظ انتجت هذه الظاهرة أشكالاً جديدة من الآثار السلبية المترتبة على تلك التغيرات، وتنقسم إلى آثار وقتية مثل (الأمطار الغزيرة، والفيضانات، والأعاصير، وموجات الحرارة)، وآثار متوسطة وبعيدة المدى مثل (ارتفاع مستوى سطح البحر، والتصحر، وتدهور الأراضي والمصايد السمكية، وغيرها من الظواهر المناخية القاسية). فضلًا عن ارتفاع متوسط درجات الحرارة، بما لها من آثار مباشرة على المجتمعات البشرية، والأنشطة الاقتصادية، والنظم البيئية والايكولوجية، بالإضافة إلى تهديد الجزر الصغيرة، والمناطق الساحلية بالغرق، بما يتسبب في تفاقم الأزمات الاقتصادية، والاجتماعية، والأمنية، مثل زيادة تدفق اللاجئين وغيرها[3].

من خلال ذلك نلاحظ ارتفاع في مستوي الانبعاثات لغاز ثاني أكسيد الكربون (CO_2) في الغلاف الجوي ، والتي يتسبب بها حرق البشر كميات متزايدة من الوقود الأحفوري. حيث شهد شهر أيار /مايو عام 2023 أعلى مستوى يسجله ثاني أكسيد الكربون على الإطلاق، إذ بلغ 424 جزءاً في المليون، مكللاً اتجاهاً متواصلاً من مستويات الكربون المتزايدة المرصودة في الغلاف الجوي سنوياً منذ ستينيات القرن العشرين[4].

الرسم البياني(1) مستويات ثاني أكسيد الكربون في الغلاف الجوي

المصدر: نيك فيريس، "رسوم بيانية تثير قلق العلماء من أزمة المناخ"، **موقع صحيفة اندبندنت عربية**، 28 /2023/8، شوهد في 2024/4/1، في: https://www.independentarabia.com/node/489516

ومن ثم تتجاوز آثار تغير المناخ البعد البيئي لتؤثر بصورة مباشرة في مختلف قطاعات التنمية، والنشاط البشري فهي تؤثر على قطاعات مثل الزراعة والموارد المائية بصورة مباشرة، وقطاع إنتاج الطاقة بصورة غير مباشرة، كما تؤثر على النماذج المستقرة للإنتاج في قطاعات أخرى مثل الطاقة والنقل والصناعة، وحتى التجارة[5]. في هذا الشأن صرح الأمين العام للأمم المتحدة السابق " بان كي مون"(Ban Ki-moon) قائلاً: "إن خطر التغيرات المناخية على البشرية شبيهة بخطر الحروب"، مضيفا "إن تغير المناخ بات أمرا لا يمكن تجاهله، وأن تدهور البيئة على الصعيد العالمي لم يجد من يوقفه كما أننا نستغل الموارد الطبيعية بشكل يخلف ضرراً كبيراً"[6].

وهكذا أضحت ظاهرة التغير المناخي ظاهرة طبيعية تحدث كل عدة آلاف من السنين، لكن نظرا للنشاطات البشرية المتزايدة ، فقد أدى ذلك إلى تسارع حدوث التغيرات المناخية التي عرفتها اتفاقية الأمم المتَحدة الإطارية بشأن تغُّير المناخ في مادتها الأولى بأنها :" تغيراً في المناخ يعزى بصورة مباشرة أو غير مباشرة إلى النشاط البشري، الذي يفضي إلى تغير في تكوين الغلاف الجوي العالمي، بالإضافة إلى التقلب الطبيعي للمناخ على مدى فترات زمنية مماثلة"[7].

أما الهيئة الحكومية الدولية المعنية بتغير المناخ (IPCC) فقد عرفت التغير المناخي بأنه : "تغير في حالة المناخ والذي يمكن معرفته عبر تغييرات في المعدل أو المتغيِرات في خصائصها والتي تدوم لفترة طويلة، عادة لعقود أو أكثر، ويشير إلى أي تغير في المناخ على مر الزمن، سواء كان ذلك نتيجة للتغيرات الطبيعية أو الناجمة عن النشاط البشري". كما تعرِف "اتفاقية الأمم المتحدة الإطارية بشأن تغير المناخ" (UNFCCC) التغير المناخي على أنه " تغير في المناخ يعزى بصورة مباشرة أو غير مباشرة إلى النشاط البشري، والذي يفضي إلى تغير في تكوين الغلاف الجوي للأرض" [8].

علاوة على ما سبق، تطرح الزيادة الأخيرة في الكوارث المناخية قضايا إضافية خاصة بتهديد اقتصادات تلك الدول، التي تدفع السكان إلى الفقر، وتوضح الأدبيات أن خسائر الكوارث، بما في ذلك الخسائر الاقتصادية والبشرية، استمرت بنسب متزايدة في البلدان النامية ومن المرجح أن تكون قضية الخسائر والأضرار التي لا يمكن تجنبها من خلال جهود التكيف[*] (Adaptation) والتخفيف[**](Mitigation) من التأثيرات السلبية من تغير المناخ على البلدان النامية[9]، الواقع، إن التكيف والتخفيف استراتيجيتان مناخيتان متكاملتان، ومن مصلحة الفاعلين الجمع بينهما لتحسين فعاليتهما وتجنب عدم التناسق والتداخلات، ما دام الهدف يتجلى في مكافحة تغرير المناخ وآثاره، لكن بوسائل مختلفة [10].وفي هذا إشارة واضحة إلى الأدراك الدولي لطبيعة التحديات التي تمثلها الآثار السلبية لتغيرات المناخ على الدول، في ظل تقاسمها تلك الآثار المناخية، خاصة في مجالات انخفاض كميات الامطار وتلوث الهواء والتصحر ..الخ، وبما تنطوي عليه هذه الظاهرة من تداعيات لها انعكاسات داخلية مختلفة، مما يفرض على صانعي القرار بإيجاد الحلول العملية للمشاكل التي انتجتها تغيرات المناخ.

وفي ضوء ما تقدم يمكننا القول أن التغير المناخي عبارة عن تغيرات في الخصائص المناخية للكرة الأرضية نتيجة للزيادات الحالية في نسبة تركيز الغازات المتولدة عن عمليات الاحتراق في الغلاف الجوي، بسبب الأنشطة البشرية التي ترفع من حرارة الجو، ومن هذه الغازات: ثاني أكسيد الكربون والميثان(CH4)،وأكاسيد النيتروجين(NO2)، والكلورو فلوروكربون (CFCs) ومن أهم التغيرات المناخية: ارتفاع حرارة الجو، واختلاف في كمية وأوقات سقوط الأمطار، وما يتبع ذلك من تغير في الدورة المائية وعملياتها المُختلفة [11].

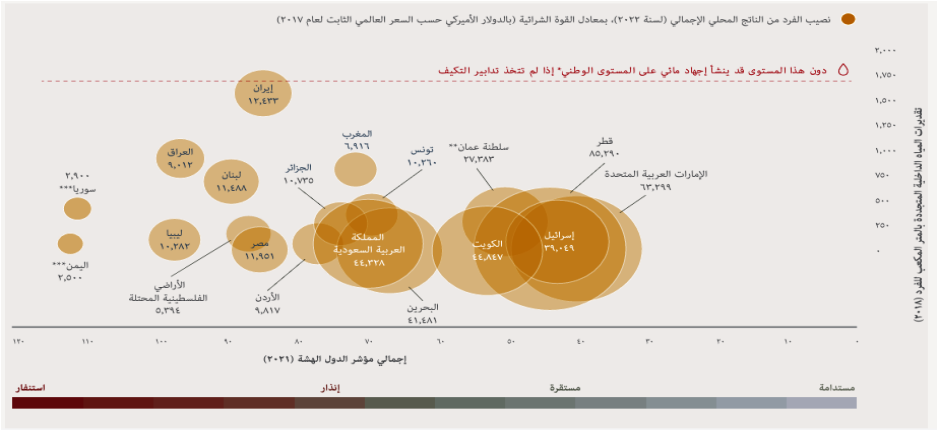
ثانيا: الشرق الأوسط واتساع تأثيرات التغير المناخي في الإقليم

حريا بنا القول، كما اسلفنا سابقاً أن تغير المناخ وما يرتبط به من ظواهر مثل الاحتباس الحراري أو الاحترار العالمي(*) (Global warming) يؤثر بشكل سلبي على بلدان العالم ككل، إذا تشكل تحدياً كبيراً لما لها من آثار تهدد مستقبل البشرية، وهذا ما يفسر تأثر دول منطقة الشرق الأوسط بالتغيرات المناخية، فهذه الظواهر تؤدي إلى موجات من الجفاف، وارتفاع في درجات الحرارة؛ حيث تشهد المنطقة انخفاضاً كبيراً في موارده وبالأخص موارد المياه، نتيجة ظاهرة عدم انتظام هطول الأمطار، والتي شهدت انخفاضاً كبيراً في دول المنطقة[12].

وفي الوقت نفسه، ستؤدي طبيعة استجابة المجتمعات والحكومات للظروف المناخية المتغيرة تأثيرها على شدة الآثار العابرة للحدود الجغرافية، فقد شهدت منطقة الشرق الأوسط حرائق الغابات في لبنان عام 2019 ، فضلا عن شح المياه مؤخراً في العراق وإيران والجزائر، فإن عجز الحكومات عن التعامل مع الإجهاد البيئي يمكن أن يؤدي إلى تحديات تهدد الأمن الوطني للدول(انظر الرسم البياني (2)) الذي يوضح التباين في القدرة على مواجهة التهديدات المناخية والتكيف معها: ففي حين تواجه جميع البلدان تحديات نتيجة انخفاض مستويات المياه العذبة مقارنة بعدد السكان، ولا يتم تصنيف أي منها على أنها مستدامة سياسياً، فإن بعضها يتميز عن غيره بثروة اقتصادية كبيرة تمكّنه من التكيف، بينما يندرج البعض الآخر في عداد البلدان المتضررة من الحروب والأزمات الاقتصادية [13].

وبحسب تقرير "المبادرة الإقليمية لتقييم أثر تغير المناخ على الموارد المائية وقابلية تأثر القطاعات الاجتماعية والاقتصادية في المنطقة العربية-ريكار" (RICCAR) أشار إلى أن درجات الحرارة سترتفع في منطقة الشرق الأوسط خلال القرن الجاري بسرعة تزيد بمعدل الضعف مقارنة بأجزاء أخرى من العالم. ويظهر متوسط التغير في درجات الحرارة بالنسبة لمسار التركيز النموذجي (مسار تركيز غازات الدفيئة وليس الانبعاثات) عند مستوى 4.5، زيادةً متوقعة بنحو 1.2-1.9 درجة مئوية منتصف القرن، و1.5-2.3 درجة مئوية بحلول نهاية القرن. أما بالنسبة لمسار التركيز النموذجي عند مستوى 8.5، فإن الزيادة في درجة الحرارة ستبلغ 1.7-2.6 درجة مئوية منتصف القرن، و3.2-4.8 درجة مئوية بحلول نهاية القرن[14].

رسم البياني (2) التباين بين دول الشرق الأوسط في مجالات توافر المياه العذبة والاستقرار الداخلي



المصدر: غلايدا لان ، وغريغ شابلاند ، **المخاطر المناخية المتعاقبة وخيارات تعزيز المنعة والتكيف في الشرق الأوسط وشمال أفريقيا** ، ترجمة : أشرف إبراهيم ، (بلا بلد، المفوضية الأوروبية ،2022)، ص 3.

وعليه تضاف التأثيرات السلبية من تغير المناخ في منطقة الشرق الأوسط ؛ إلى سلسلة التأثيرات التي تضرب العالم منذ العقود الأخيرة ، ولكن نظراً لطبيعة موقعها الجغرافي، ولضعف الدعم المالي المتاح لها من الدول المتقدمة، فإن ذلك يجعلها معرضة للخطر بشكل أكبر دون غيرها، حيث مازال الدعم ضئيلاً مقارنة بتكاليف التكيف السنوية التي تقدر بنحو 70 مليار دولار، ومن المتوقع، أن تصل إلى 160-340 مليار دولار بحلول عام2030 [15].

واتساقاً مع ما تقدم يرى "باري بوزان" (Barry Buzan) في ما يتعلق بالتحولات المتصلة بميدان التغيرات المناخية أنه يمكننا إضفاء الطابع الأمني على قضية معينة من خلال اللجوء إلى سلسلة من العمليات المترابطة، تتمثل الحلقة الأولى من السلسلة في مرحلة "اللاتسييس (Nonpoliticised ") أي أن هذه القضية لا تعتبر قضية سياسية، قد تكون ، قضية اجتماعية، ثقافية أو بيئية...، أما الحلقة الثانية فتعبر عن عملية "التسييس" (Politicised) والتي تعني أن تصبح تلك القضية حاضرة في نقاشات السياسة العامة، لنصل في الحلقة الثالثة إلى عملية "الأمننة" (Securitization) وفيها تنتقل القضية من مجال السياسة الدنيا إلى مجال السياسة العليا، لأن القضية تصبح بمثابة تهديد حقيقي للأمن [16].

وفي السياق ذاته يصبح التغير المناخي أحد المصادر غير التقليدية التي تمثل تهديداً حقيقيا للأمن الوطني للدول وكذلك تهديداً للسلم والأمن الدوليين، إضافة إلى المصادر التقليدية مثل

الحروب بين الدول والنزاعات المسلحة والحروب الأهلية داخل الدول والإرهاب وانتشار الأسلحة النووية، فضحايا التغيرات المناخية أضحت تفوق ضحايا الحروب والنزاعات، كما أنها تهدد كل الدول والشعوب على عكس النزاعات التي تهدد الدول التي تندلع فيها فقط ويمكن اعتبار التغير المناخي تهديدا للأمن الوطني والسلم الدولي[17].

وهكذا تشكل هذه الموضوعات إشارة واضحة على وجود صلة وثيقة ومباشرة وغير مباشرة بين تغير المناخ والأمن الوطني للدول، حيث أنها تعتبر من العوامل المضاعفة للتهديدات التي قد تؤدي إلى تفاقم المشاكل القائمة وزيادة عدم الاستقرار: يمكن أن يؤدي ارتفاع درجات الحرارة ونقص المياه والغذاء إلى توسيع الفجوات الاجتماعية والاقتصادية، مما يؤدي إلى الهجرة الجماعية وموجات اللاجئين، ويخلق ظروفًا مواتية لظهور الجهات الفاعلة الإرهابية وشبه الحكومية التي تستغل الفئات الضعيفة من السكان. إذ ترتبط الزيادة في درجات الحرارة بزيادة العنف بين الجماعات[18]. ففيما يتعلق بدرجات الحرارة حيث تشير التقارير والبيانات الى إن درجة الحرارة شهدت ارتفاعاً مُطرداً في جميع انحاء البلاد منذ خمسينات القرن الماضي وبمتوسط بلغ 0.7 درجة مئوية بالمقارنة مع ما كانت عليه قبل 100 عام، ومن المتوقع أن يرتفع متوسط درجات الحرارة بنحو 2-3 درجة مئوية على مدار الـ 100 عام القادمة، وقد ارتفع متوسط درجات الحرارة خلال المدة 1901-2021 بنحو درجتين مئوية وهي أعلى حتى من المتوسط العالمي[19].

ووفقاً لذلك فإن العراق يواجه تحديات بيئية مختلفة فبحسب التقرير السادس لتوقعات حالة البيئة العالمية لمنطقة غرب آسيا (GeO – 6) صنف بالمرتبة الخامسة كونه من أكثر الدول المتضررة من أزمة التغييرات المناخية، اذ تعرض البلاد في العقود الأخيرة إلى الظواهر المناخية العنيفة مثل درجات الحرارة العالية، وعدم كفاية الامطار ونقص هطولها، والجفاف، وندرة المياه.

وتكرار العواصف الرملية والترابية والفيضانات [20]. ومن خلال مقاربات التحرك العراقي يتضح أنه أصبح مدركاً للتغيرات التي تستظهرها خرائط التغيرات المناخية على تضاريس البيئة العراقية، مما يهدد أمنة الوطني من تلك التغيرات كالتغير الحراري واختلاف كميات سقوط الامطار وما يتبعها من تأثيرات على انخفاض منسوب المياه في الأنهر، فضلاً عن اتساع الأراضي غير الصالحة للزراعة والتي تعد شأن آخر أيضاً من ظاهرة تغير المناخ.

وفي هذا الإطار يسلط التقرير الصادر عن البنك الدولي عام 2022 الضوء على التغيرات المناخية وآثارها على بيئة الأمن الوطني العراقي، لاسيما في ظل تفاقم شح المياه، الذي ساهم في تراجع الإنتاج الزراعي في العراق من ناحية [21]، ومن ناحية أخرى تكشف الإحصاءات أن المياه السطحية تعد المورد المائي الرئيسي في العراق وتتكون من مياه نهري دجلة والفرات وروافدهما وشط العرب وقد حدث تناقص كبير للموارد المائية للعراق بسبب السدود الكثيرة والمشاريع الأروائية والتنموية التي أنشئت على هذه الأنهار في دول الجوار لتأمين حصصها المائية واستخدامها لتوليد الطاقة الكهرومائية مما أثر على حصة العراق المائية ونوعيتها، كما أن تأثيرات التغيرات المناخية قد سببت نقصان كميات المياه الواردة إلى أنهاره, حيثُ يعتبر قطاع المياه من أكثر القطاعات هشاشة في مواجهة التغيرات المناخية[22].

علاوة على ذلك، ازدياد انبعاثات غاز ثاني أوكسيد الكربون في العراق إلى أكثر من الضِعف على مدار العقد الماضي وسجل العراق واحداً من أعلى معدلات كثافة انبعاثات الكربون (نسبة الانبعاثات إلى إجمالي الناتج المحلي) بالمقارنة مع نظرائه من حيث الدخل من البلدان الأخرى في المنطقة وتساهم قطاعات الكهرباء، والنفط والغاز، والنقل في نحو ثلاثة أرباع الانبعاثات في البلاد ويمكِن أن يؤدي اتخاذ المسارات الملائمة في خفض انبعاثات الكربون في قطاع الكهرباء إلى مكاسب إضافية كبيرة في مستويات النمو والإنتاجية[23].

المحور الثاني: مكونات الاستراتيجية العراقية تجاه التغيرات المناخية وديناميكياتها

اتخذ العراق سياسات متعددة الأبعاد تعبر في جوهرها عن أهداف استراتيجية، في سياق مواجهة تغيرات المناخ، تشمل المجالات التنموية والبيئية ، وهذا ما جعل الحكومة العراقية تتخذ مجموعة من القرارات المناسبة في العديد من المشاريع التنموية بالتزامن مع زيادة الاجراءات التعاونية الدولية والإقليمية.

أولاً: الإطار الاستراتيجي كوسيلة ملائمة السياسات التنظيمية

تشير الأدبيات الاستراتيجية (Strategy) إلى أن المفهوم الحديث للاستراتيجية يتصف بالهرمية والنسقية ،أي توجد استراتيجية عليا للدولة، ومنها تتفرع استراتيجيات فرعية كالاستراتيجية السياسية والاستراتيجية الاقتصادية والاستراتيجية العسكرية ومنها أيضاً تتفرع استراتيجيات أخرى كالاستراتيجية التعليمية والاستراتيجية الصحية والاستراتيجية الإعلامية

والاستراتيجية البيئة وغير ذلك من الاستخدامات الأخرى في مختلف الجوانب حتى ضمن أدنى المستويات، لذا يعرفها البعض بأنها :" تعني مجموعة الخطط والتدابير اللازمة لتحقيق هدف او مجموعة من الأهداف بغض النظر عن طبيعة تلك الأهداف سواء كانت عسكرية أو سياسية أو اقتصادية أو اجتماعية ويمكن استخدامها بدءا من أعلى مستوى في الدولة نزولاً إلى أدنى مستوى وحتى على مستوى الأفراد أيضاً وغالباً لا يمكن تحقيق النجاح في عمل ما دون أعداد استراتيجية مسبقة لذلك العمل" [24].

وتأسيسا على ما سبق، فأن الاستراتيجية بمفهومها الحديث هي خطة لإدارة قطاعات الدولة وفق رؤية مسبقة ومدروسة تتضمن أهدافها واضحة ومن ثم فهي إحدى الأدوات التي يعتمد عليها المختص في الجغرافية السياسية في أدارة مقومات الدولة وتطويرها من ناحية، ومن ناحية أخرى فهي تمثل الوجه الأخر لعلم الجيوبوليتيك(Geopolitic) الذي من شأنه وضع تصورات لمستقبل الدولة وفق خطط دقيقة. وبما أن المناخ هو أحد المقومات الطبيعية للدولة بل يمثل عنصر رئيس في قوتها كونه ينعكس على النشاط الاقتصادي وطبيعة سلوك الإنسان وفعالياته اليومية ومن ثم فإن تحديد طبيعة مناخ الدولة ضرورة ملحة بالنسبة إلى المختص بالجغرافية السياسية، لذا فإن قضية التغيرات المناخية تحولت إلى قضية استراتيجية لها وجهين محلي يتمثل بالأخطار المحتملة التي تمس كيان الدولة وأمنها الوطني، والثاني دولي يتمثل بمدى تفاعل الدولة مع المجتمع الدولي لمواجهة الخطر المشترك وهو ما يتطلب وضع استراتيجيات واضحة لهذا العمل[25].

ومن هنا تصبح التصورات الاستراتيجية جزءاً أساسياً من البحث عن السياسات المختلفة، التي تشكل مدخلاً مهما تتحرك الدول من خلاله للحد من تأثيرات التغيرات المناخية بكل الوسائل الممكنة، وتعد التكنولوجية إحدى أهم تلك الوسائل، حيث لعبت التكنولوجيا دوراً مثيرا للاهتمام عبر التاريخ فيما يتعلق بتغير المناخ، إذ أصبحت التطورات التكنولوجية الحالية أكثر اخضراراً ووعيا بالتأثيرات البيئية مما كانت عليه في العقود الماضية، وأصبح المجتمع في وضع افضل بكثير لزيادة انتاج الطاقة واستهلاكها بطريقة موفرة للطاقة، ولكن لا تزال الآثار السلبية التي خلفتها الثورات الصناعية المتتابعة قائمة ومتمثلة في زيادة انبعاثات الكربون، على الجانب الآخر يساعد تطبيق التكنولوجيات الحديثة مثل النقل الكهربائي في التخفيف من تأثير وسائل النقل التي ينبعث منها الكربون، كما تقلل التكنولوجيات الرقمية على

المدى البعيد من الانبعاثات الكربونية بنسبة 15% طبقا لتقرير نشره المنتدى الاقتصادي العالمي[26].

وهكذا تحظى قضية تغير المناخ بالمزيد من الاهتمام بين مختلف الجهات الحكومية، حيث أن تأثيرات تغير المناخ عالمية النطاق وغير مسبوقة من حيث الحجم، وبدون اتخاذ إجراءات صارمة في الوقت الراهن، سيكون التكيف مع هذه الآثار في المستقبل أكثر صعوبة ومكلفة، حيث أصاب التلوث كل عناصر البيئة المحيطة بالإنسان بعد أن ضل الطريق من أجل ما يصبو إليه من مكاسب، فدمر الأرض التي نأكل من نتاجها والهواء الذي لا نحيا بغيره والماء الذي يعد من أهم مقومات الحياة [27].في جوهر الأمر، تتيح الاستراتيجية اختيار الوسائل والأدوات التي يمكن من خلالها تنظيم ممارسات أنشطة الدول في مواجهة تحديات تغيرات المناخ، عبر تطوير القطاعات التنموية والبيئة المختلفة، من أجل زيادة فاعلية قدراتها للتخفيف من تأثيرات تغير المناخ.

وبناء على ذلك، في ظل هذا الجدل حول المسئولية عن ظاهرة تغير المناخ العالمي، تطورت الاتفاقيات العالمية لمواجهة هذه الظاهرة فيما يخص كيفية سعيها لخفض الانبعاثات المتسببة في ارتفاع درجة حرارة الأرض. فبعد أن كان بروتوكول "كيوتو" يطالب الدول المتقدمة فقط بخفض هذه الانبعاثات، أقرت اتفاقية "باريس" مبدأ "المسئولية المشتركة ولكن متباينة الأعباء" بين الدول المتقدمة والنامية لمواجهة تغير المناخ العالمي، ودعت جميع الدول إلى تحديد الأهداف الخاصة بانخفاض الانبعاثات[28].

وفي المقابل، أصبحت الدول تعمل على توسيع سياسات التكيف وتخفيف آثار تغير المناخ الموضوعة حاليا على حد سواء مع العمل على تعزيزها. ويجب أن تمنح البلدان الأولوية للاستراتيجيات الشاملة التي لا تقتصر على معالجة الأزمات المباشرة وإنما هي أيضا تعد للعواقب الأطول أجلا من تغير المناخ ويجب أن يمنح صناع السياسات الأولوية في استراتيجياتهم للاستثمار في إجراءات تعكس الطريقة التي تتعامل بها الدولة مع قضية تغير المناخ، على نحو يأخذ في الحسبان تعزيز البنية التحتية والزراعة القادرتين على تحمل تغير المناخ، فضلاً على إدارة مخاطر الكوارث، والحماية الاجتماعية[29]. وبطبيعة الحال فإن اتخاذ مزيد من الإجراءات لتلك السياسات من قبل الدول يقتضي الحصول على مزيد من الدعم متعدد الأطراف. ويمكن أن يساعد ذلك في الحفز على اتخاذ إجراء حيث تكون الحاجة ماسة إلى ذلك، ونقل

المعرفة الفنية القيمة وتبادل الخبرات في مجال السياسات، وتحفيز مصادر التمويل الأخرى لتلبية الاحتياجات التمويلية الكبيرة في المنطقة بغرض التكيف وتخفيف آثار تغير المناخ وتكتسب كلها أهمية خاصة في البلدان منخفضة الدخل والبلدان في الشريحة الأدنى من فئة الدخل المتوسط [30].

وأجمالا يمكننا القول أن قضية التغير المناخي ذات طابع عالمي، فإن أي جهود لصيانة البيئة داخل إقليم الدولة سوف تبقى محدودة الفاعلية، ولذلك فإن عملية حماية البيئة تتطلب مجهودات دولية من خلال التعاون بين كافة الدول، فضلاً عن المجهودات الوطنية فهي جزء لا يتجزأ من المجهودات الدولية [31].

ثانيا : مجهودات العراق في تنمية آليات مواجهة التغيرات المناخية

تعتبر السياسات الحكومية للدول فاعلية محورية في بحث عن التغيرات المناخية وكيفية الحد من آثارها السلبية، حيث تعمل على توجيه الجهود الوطنية والدولية نحو "التنمية المستدامة" [*]،(Sustainable Development) تلعب الحكومات دورًا حاسمًا في وضع الأطر التشريعية والتنظيمية التي توجه الحفاظ على البيئة والتنمية الاقتصادية والرفاه الاجتماعي في سياق التخفيف من تغير المناخ، يمكن أن تؤثر سياسات الحكومة بشكل كبير على جهود التخفيف من تغير المناخ من خلال تحديد أهداف خفض الانبعاثات وتعزيز الطاقة المتجددة[**] (Renewable Energy) ووضع معايير لكفاءة الطاقة وتعزيز ممارسات استخدام الأراضي المستدامة [32].

وهنا في ظل تصاعد تحديات التغيرات المناخية، تسعى الحكومات من خلال أهدافها الوطنية لمواجهة التغيرات المناخية، رسم ملامح استراتيجية تقدم الحلول المبتكرة في بحث عن التغيرات المناخية وكيفية الحد من آثارها السلبية بصيص أمل للتخفيف من الآثار الضارة لتغير المناخ، تهدف هذه الحلول، التي تستفيد من التكنولوجيا المتطورة والنهج الإبداعية، إلى معالجة الأسباب الجذرية لتغير المناخ مع تعزيز النمو المستدام والقدرة على الصمود. من خلال تنفيذ استراتيجيات مبتكرة، يمكن للمجتمعات تقليل انبعاثات غازات الاحتباس الحراري وتعزيز كفاءة الطاقة وزيادة قدرة عزل الكربون، وبالتالي المساهمة في الجهود العالمية لمواجهة تأثيرات المناخ [33].

وتوافقاً مع ما سبق بيانه سابقاً من أن مناخ العراق شهد تغيرات مناخية كبيرة على مر التاريخ تمثلت بالعصور الجليدية والفترات الدفيئة في مختلف الأزمنة، إلا أن تلك التغيرات لم تكن مفاجئة بل استغرقت وقتاً طوياً استمر آلاف السنين، امتازت الفترات الدفيئة في ذلك الوقت بكونها أقل حرارة من الآن وكانت جل أسبابها طبيعية. أما ما يحدث في الوقت الحاضر من تغيرات مناخية فمعظمها يعود إلى الأنشطة البشرية الصناعية وما يترتب عليها من زيادة في استهلاك الوقود الأحفوري وما ينتج عنه من زيادة في انبعاث الغازات الدفيئة وتزايد تركيز غاز ثاني أوكسيد الكاربون الموجود في الغلاف الجوي والذي سجل رقماً قياسياً عالياً مقارنة بالنصف مليون سنة الماضية مسجلاً بذلك معدلات سريعة واستثنائية، والذي أنعكس بدوره على الزيادة في درجات الحرارة السنوية إذ سجل تزايداً ملحوظاً خلال الألف سنة الماضية. ويتضح أن الاتجاه العام لمعدلات درجة الحرارة السنوي في العراق يسير نحو الارتفاع بمقدار (0,5)مْ[34].

وضمن هذا النطاق، جاءت التوجهات الاستراتيجية للحكومة العراقية الجديدة على مستوى التحولات في مسار التصدي لملف التغير المناخي من اجل تجاوز الارهاصات التي نشأت بفعل أزمات داخلية أسهمت بخلق عقبات لمواجهة التغير المناخي ،لا سيما في ضوء صياغة آخر استراتيجية وطنية عراقية تتناول خطة عمل بيئية لمواجهة تحديات التغيرات المناخية في العراق جرت في عام 2013، وكانت تهدف حينها إلى تأطير العمل البيئي في البلاد جغرافياً وسياسياً وأمنيا. وخلال السنوات الأربع التالية، تعذر تنفيذ هذه الخطة في ظل الحرب التي خاضها العراق لمواجهة خطر التنظيمات الإرهابية المتطرفة وخاصة تنظيم داعش الإرهابي. حيث لم تعالج تلك التحديات بشكل معمق، ومع استقرار الأوضاع نسبياً، وفي ظل الالتزامات المناخية والبيئية التي تعهد بها العراق أمام المنظمات الدولية(International organizations)، جرى أخيراً إطلاق خطة عمل وطنية جديدة بدعم من برنامج الأمم المتحدة الإنمائي (UNDP)، بالتعاون مع برنامج الأمم المتحدة للبيئة (UNEP) من خلال طرح الحلول والسياسات الوطنية لمواجهة تغير المناخ [35].

وفي السياق ذاته شكلت "رؤية العراق 2030" الاستراتيجية الوطنية العراقية التي أعلن عنها رئيس مجلس الوزراء العراقي "محمد شياع السوداني" في مؤتمر العراق في محافظة البصرة في آذار/ مارس عام 2023، إطاراً يعزز البناء المؤسساتي والقانوني للدولة للحد من التلوث البيئي

حتى عام 2030، من خلال حماية وتحسين جودة الهواء والمياه والتربة، وتطوير وتحسين إدارة النفايات الصلبة، والحد من التلوث في قطاعي الصناعة والطاقة، والبحث عن مصادر أخرى جديدة للطاقة نظيفة ومستدامة لا تتسبب بالتلوث، فضلاً عن [36].

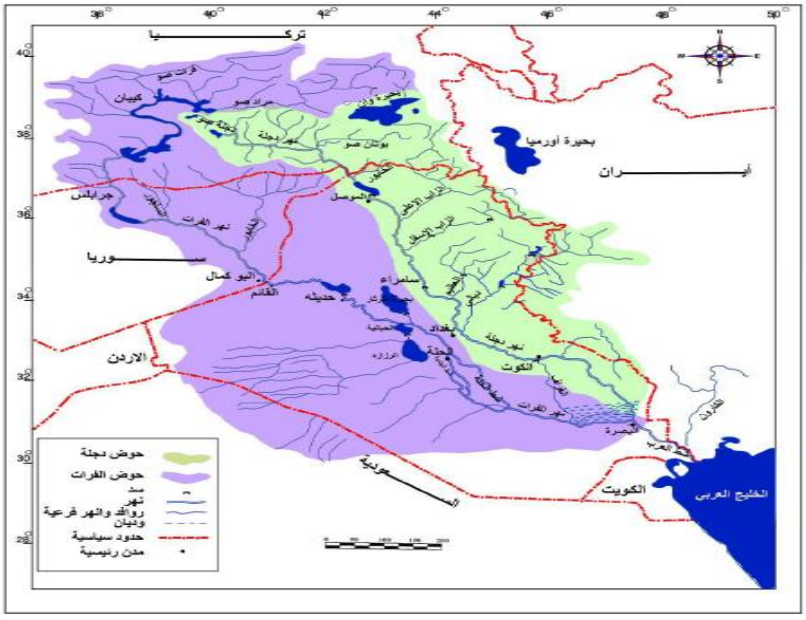
إلى جانب ذلك، تسعى رؤية العراق (2030) إلى إقامة مؤسسات إدارية فاعلة تضمن الحقوق السياسية والمدنية والإنسانية والعدالة والمساواة لجميع المواطنين أمام القانون، فضلاً عن تحقيق الحكم الرشيد ومواجهة تردي مؤشرات الحكم في البلد وخاصة تلك المرتبطة بالفساد والدولة الهشة من أجل ضمان تقديم الخدمات العامة بطريقة شاملة وشفافة وخاضعة للمساءلة من قبل الدولة وسيقوي الحكم الرشيد العلاقة بين الدولة والمواطن وبين الحكومة المركزية والحكومات المحلية بما يضمن مساراً تنموياً وطنياً ومحلياً مستداماً، وقد حددت رؤية العراق آليات ضمان الحكم الرشيد بالآتي: تعزيز ثقافة التسامح والحوار والسلم المجتمعي، وتعزيز قيم المواطنة والحد من أوجه عدم المساواة، حلول مستدامة للهجرة الداخلية والنزوح والهجرة إلى الخارج[37].

ومن ناحية أخرى من بين المعالجات الأخرى التي سلطت الحكومة العراقية تركزيها، عودة الاهتمام بقضية الرقابة البيئية واشتراط حصول أصحاب النشاطات الصناعية والخدمية على الموافقات البيئية التي تعتمدها وزارة البيئة، والتي تشترط التزامهم بالمحددات والضوابط البيئية قبل منحهم إجازة إنشاء المصانع أو ممارسة عملهم، وتنفيذ بعض البرامج التي تسهم في دعم الوعي وتعزيز الثقافة البيئية لدى أصحاب هذه النشاطات بما ينعكس بشكل إيجابي في الحفاظ على البيئة وتحسينها. وفي الوقت نفسه تعتزم وزارة الموارد المائيَّة، تشييد 36 سداً صغيراً لحصاد المياه موزعة بين المناطق الصحراويَّة، ضمن خططها للاستفادة من مياه الأمطار وتخزينها ، متوقعةً هطولاً جيداً للأمطار خلال فصلي الخريف والشتاء، بحسب تأكيد "عون ذياب عبدالله" وزير الموارد المائية العراقي، الذي أعلن على إكمال أعمال الدراسات والتصاميم والتحريات الأولية الخاصة بتلك السدود في المستقبل القريب، موضحاً أن مواقع السدود المزمع تشييدها ستتوزع بين الصحراء الغربية ووادي السماوة والمناطق الشمالية والجنوبية والشرقية من البلاد[38].

يضاف إلى ذلك أيضاً الممارسات التي تقوم بها "منظمات المجتمع المدني"(Civil society organizations) في شمال العراق، تركّيز ناشطين من عدة منظمات بيئية على

الحفاظ على المياه من خلال تشجيع مشاريع إعادة التغذية الاصطناعية للمياه الجوفية، وإعادة التشجير، وإزالة التلوث عن المناطق الملوثة. وجاءت الخطط والمبادرات العراقية لمواجهة الآثار السلبية للتغيرات المناخية، وفي المقدمة منها مخاطر الجفاف، ونقص الغطاء النباتي، وانتشار التصحر، ونقص الحصص المائية، وارتفاع التلوث، وانتقال مياه البحر إلى أعلى النهر في جنوب العراق، لتدمر 60 ألف فدان من الأراضي الزراعية و 30 ألف شجرة في العام 2022 فقط، ما تسبب في تلاشي المخزون المائي في البحيرات(انظر الخريطة رقم (1)) والمسطحات المائية، فيما انخفضت مستويات المياه في بحيرات كبيرة كانت تساهم في تعزيز المخزون المائي على المستوى الوطني مثل بحيرتي "الحبانية" في الغرب "وساوة" في الجنوب، وأيضاً انخفضت مستويات المخزون في منخفض الثرثار الذي يمثل أكبر مساحة لتخزين المياه في وسط العراق، فضلاً عن جفاف ما يزيد على 80 % من الأهوار في الجنوب [39].

خارطة (1) الموقع الجغرافي للبحيرات في العراق



المصدر: ضحى جواد كاظم ، أمير هايد جدوع، "الامكانات المائية المتاحة للعراق (دراسة جغرافية العراق)"، **مجلة كلية التربية الأساسية للعلوم التربوية والإنسانية**، العدد(30)،(العراق : 2016)، ص 676.

إضافة إلى ذلك على المستوى الدبلوماسي سعى العراق إلى الاستفادة من مخرجات أعمال مؤتمر الأطراف المناخي " كوب 28 " الذي عقد في "اكسبو" في مدينة (دبي) للفترة الممتدة من 30 تشرين الثاني/ نوفمبر ولغاية 13 كانون الأول/ ديسمبر عام 2023، وتطويعها لصالحة

من خلال دعم سياقات العراق للتخفيف والتكيف مع التغير المناخي وتأثيراته وبما ينسجم مع الخطة الوطنية العراقية من خلال عدة اهداف رئيسية وكالآتي:

أولاً: على صعيد التمويل والدعم المالي لمشاريع التخفيف والتكيف ومتطلبات حماية البشر والطبيعة وتعزيز أنماط العيش المستدامة وصولاً إلى العدالة المناخية فمن النتائج المهمة هو تفعيل صندوق "الخسائر والأضرار" بقيمة 725 مليون دولار قابلة للزيادة على شكل منح مالية من الدول المتقدمة صناعياً للدول النامية ومنها العراق.

ثانياً: بشأن الانتقال من الوقود الأحفوري(الفحم، النفط، الغاز الطبيعي) إلى مصادر نظيفة خضراء ومتجددة صديقة للبيئة بهدف إزالة الكاربون من النظم الطاقوية عبر إقامة شراكات للانتقال العادل، فعلى المستوى العراقي هناك جوانب مهمة آنية جاذبة للاستثمار والتمويل وبشكل خاص معالجة المياه الملوثة نتيجة استخدامها في إنتاج النفط عبر استخدام التقنيات الحديثة وتبقى المساهمة الأكبر هو إنهاء حالة حرق الغاز المصاحب الذي شرعت فيه الحكومة العراقية الحالية ورصدت لها التمويل في ميزانية الثلاث سنوات القادمة وعن طريق الاستثمار.

ثالثاً: خصص يوم حول تأثير التغير المناخي في الصحة العامة (Public Health) تعتمد استراتيجية ثلاثية الأبعاد (الوقاية، والتأهب، والاستجابة) والتغطية الصحية الشاملة وبمشاركة واسعة توجت باتفاق دولي وقع عليه 123 بلداً من ضمنها العراق لدعم الاستثمار وتمويل البرامج الصحية الوطنية لمعالجة الأضرار الناجمة عن تلوث الهواء وارتفاع نسبة الملوثات الكيمياوية والبايولوجية [40].

خلاصة لما تقدم، يمكننا القول يسعى العراق إلى توظيف مجالات التعاون مع الأطراف الأخرى على نطاق واسع من أجل توفير بيئة دولية وإقليمية مساهمة لاستراتيجيته الوطنية تمزج بين تحقيق أهدافه في اتخاذ تدابير تحد من تفاقم التهديدات والمخاطر على أمنة الوطني بفعل انعكاسات تغيرات المناخ على الوضع الداخلي من جهة، ومن ناحية أخرى أشراك تلك الأطراف في تحقيق سياساته التنموية.

المحور الثالث: العراق وفجوة الأداء في مسارات مواجهة تغيرات المناخ وديناميته

مما لا شك فيه رغم كل الجهود التي تقوم بها المؤسسات الحكومية العراقية لمواجهة تأثيرات المتغيرات المناخية على العراق إلا أنها تواجه العديد من التحديات في الوقت الراهن، مما يجعل العراق أكثر عرضة للأثار المرتبطة بتقلبات المناخ وتغيراته.

أولا: اتساع نطاق أشكال التحدي ودلالاته المختلفة

تشير لفظة التحدي عند "أرنولد توينبي" (Arnold Toynbee) إلى وجود (واقع مشكلة موقف ازمة خطر تهديد) يقابله استجابة والتي تتضمن(الرد المجابهة الفعل التجاوز التمرد التخلص ... الخ) ويؤمن "توينبي" أنه كلما زاد التحدي تصاعدت قوة الاستجابة حتى تصل بأصحابها إلى ما يسميه الوسيلة الذهبية والتي تأتي من خلالها سلسلة الاستجابات الناجحة أو شبه الناجحة أو الفاشلة، ولقد عد "توينبي" التحديات الخاصة بالطبيعة وتحدي البيئة البشرية من ضمن أنواع التحديات التي تواجه الحضارات ويعتقد أن العلاقة بين التحدي والاستجابة علاقة طردية فكلما زاد التحدي تصاعدت الاستجابة حتى نصل إلى الوسيلة الذهبية وصنفها إلى استجابات فاشلة وهي التي تؤدي إلى التخبط والفوضى والاعتماد على الغير والاستجابة الناجحة والتي يصنفها إلى ثلاث مراحل هي الصحوة أي مرحلة الاحساس بالخطر واليقظة وهي مرحلة تعقب الصحوة وتتضمن العمل المدروس والمخطط تعقبها النهضة التي تتضمن الإبداع والتميز في مواجهة التحديات الماثلة أمامها [41].

أضف إلى ما سبق، إن التغيرات المناخية هنا ستمثل تحدياً خطيراً ينعكس على أمن الدولة البيئي وبناءها الجاري كونها تهدد قطاعات مهمة ومنها القطاع الاقتصادي بمستوياته المختلفة كقطاع الزراعة وقطاع المياه واللذان يشكلان جانبان مهمان من جوانب سيادة الدولة كونهما يجعلان الدولة تعتمد على الخارج في سد احتياجاتها [42].

وعليه دفعت تلك الآثار المستمرة لتغير المناخ في جميع انحاه العالم إلى أن تواجه الدول مجموعة من التحديات أو العقبات المتنوعة على كافة الأصعدة السياسية والاقتصادية والأمنية، والتي قد تعرقل جهودها لمواجهة آثار التغيرات المناخية، فالتحديات التي تواجهها الدول في مكافحة الظواهر المصاحبة للتغيرات المناخية أصبحت أكبر من أي وقت مضى، وفي هذا السياق، يمكن الإشارة إلى تعاني الكثير من الدول من ضعف حاد في قدراتها الذاتية التي يمكن الاعتماد عليها لوضع سياسات واستراتيجيات تمكنها من مواجهة آثار التغيرات المناخية،

ورغم تبني بعض الدول خطابات سياسية تُشير فيها إلى عملها على وضع تدابير لمواجهة هذه الآثار، فإن غياب مُؤسسات حكومية قادرة على صياغة استراتيجيات وطنية تتضمن إجراءات محددة ورؤية شاملة يؤثر بشكل كبير في هذه المواجهة[43]، أضف إلى ذلك هشاشة وضعف البنية التحتية المؤهلة والتي تساعد الدولة على تعزيز قدرتها على الصمود في مواجهة التغيرات المناخية وآثارها، وحتى قدرتها على مواجهة الكوارث الطبيعية كما حدث في الفيضانات المدمرة التي ضربت كل من شمال شرق ليبيا عام 2023، وباكستان عام 2022، وكذا الزلازل المدمرة التي ضربت كل من تركيا وسوريا والمغرب عام 2023، وحرائق الغابات في الجزائر ومدينة (كانغ نونغ) الساحلية الشمالية شرق عاصمة كوريا الجنوبية في العام 2023[44].وفي السياق ذاته مع استمرار اتجاهات الضغوط التي تواجه سياسات الدول بإدائها لمواجهة الظواهر المناخية، فأنها في الوقت نفسه تضع مزيد من التحديات على مقارباتها في مسارات مشاريع التنمية، إضافة إلى ذلك قد يعطل نهجها في مضمار العمل بشأن رؤاها وخططها الاستراتيجية ذات الصلة بالتغيرات المناخية .

إضافة إلى ذلك يفرض تنفيذ النموذج الاقتصادي المعد للالتزامات المُناخية تحدياتٍ جديدةً على بلدان المنطقة، مع عواقب متفاوتة، بحسب كل بلد؛ فتطبيق سياسات التخفيف، يعني اتخاذ تدابير الترشيد والاستدامة في قطاعات محددة وكثيفة الاستخدام للطاقة، مثل الكهرباء والمباني والزراعة والصناعة والنقل. ومع ذلك، فإن المضي قدما في التحولات العميقة لاقتصادات البلدان المصدرة للنفط والغاز، قد ينطوي على صعوبات عديدة. فمنطقة الخليج معرضة لتأثيرات تغرير المناخ، نظراً إلى موقعها الجغرافي ومُناخها الجاف واعتمادها على الوقود الأحفوري، وبحلول عام 2075، من المتوقع أن تصبح غير صالحة للسكن بسبب ارتفاع درجة الحرارة بمقدار 4 درجات مئوية[45]. كما أن البحرين وقطر والإمارات والعراق واليمن، هي من الدول المعرضة بشكل خاص لموجات الحر وارتفاع درجات الحرارة. ومن شأن إعادة النظر في النموذج الاقتصادي الأحفوري، أن تهز أركان العقد الاجتماعي القائم على الريع، والمترسخ منذ عقود. ويفرض هذا الوضع على دول الخليج والجزائر والعراق وليبيا إيجاد مصادر أخرى للدخل. وقد شرعت دول الخليج بالفعل في الاستثمار في إنتاج الطاقة الخضراء والترويج للقطاعات الاقتصادية الأخرى، مثل السياحة، في حين تبدو الجزائر وليبيا والعراق أقل استعدادًا لتحمل خسارة عائداتها من النفط والغاز، وعموما، تبقى للمنطقة

إمكانيات عالية لتخفيف ذلك، سواء من حيث آفاق الطاقة الخضراء أم من حيث تحقيق الكفاءة في استخدام الطاقة[46].

ومن هنا تتجلى إجراءات إصلاح وترسيخ مؤسسات حكم متماسكة، وآليات فعالة لتنسيق الحلول الإقليمية للتحديات المشتركة، تمثل خطوة أساسية في هذا المسار، وسيقود إلى استجابة مبكرة وفاعلة لتداعيات التغيرات المناخية والكوارث والصراعات وتأثيراتها على الأمن الوطني للدول. مع الاعتراف بأن توجهاً كهذا لن يكون تحقيقه سهلاً؛ فحتى في حال وجود رغبة لدى حكومات المنطقة في تطبيق "الحكم الرشيد"[*](Good Governance) ، من الصعب ضمان استجلاب دعم الشركاء الدوليين في ظل عدم القدرة على التحقق من أن هذا الدعم ينفق في الاتجاه الصحيح ولنفس الغرض تعزيز الحوكمة، فضلاً عن وجود تعقيدات موضوعية عديدة ومتداخلة، يتعلق معظمها بطبيعة سياسات المنطقة والتركيبة الديمغرافية فيها، حيث يؤدي العاملان القبلي والإثني دوراً في تشكيل النخب والمنظومات السياسية وتصعيدها، على نحو يُعيق -في بعض الأحيان- خطط بناء الدولة وعمل مؤسساتها، في إطار مشروعات التعامل مع آثار التغيرات المناخية [47].

ثانيا: معضلة ضعف القدرات وغياب الفاعلية

على الرغم من الاجراءات التي يقوم بها العراق في مواجهة آثار تغيرات المناخ كتحدي يواجه الأمن الوطني العراقي للحد من تزايد الانبعاثات الغازية، فضلاً عن تحقيق أهداف التنمية في التحول نحو الطاقة النظيفة(Clean Energy) وحماية البيئة، إلا أنه على المستوى التنفيذي يلاحظ هنالك ضعف في مواجهة التغير المناخي بعد أن تعرضت البيئة في العراق إلى ضغوطات عديدة، منها زيادة النمو السكاني وتأثير ثلاث حروب وسوء استخدام الأراضي الزراعية، مما أدى إلى تدهور نوعية المياه وجودتها بسبب ارتفاع نسبة الملوحة في التربة وتلوث الهواء، كما أدت النزاعات والاضطرابات إلى غياب اتفاقيات مائية تنظم استخدام الموارد المائية للزراعة وتربية المواشي، وزادت من حدة الهجرة من الريف إلى المدينة، فضلاً عن ذلك يعاني العراق من مشاكل جودة الهواء وارتفاع درجات الحرارة بسبب التغيرات المناخية وضعف الغطاء النباتي نتيجة ضعف الوعي والاستثمار في المساحات الخضراء(Green spaces) [48].

بالإضافة إلى ذلك أثر التغير المناخي في العراق بشكل كبري على الجوانب الاجتماعية أيضاً واحد الظواهر الناجمة عنه هو ظاهرة الهجرة المناخية. إذ شهدت بعض المناطق في العراق تغيرات مناخية جعلتها غير صالحة للعيش، مما دفع السكان إلى التحرك نحو مناطق أخرى توفر ظروفاً أكثر ملائمة تسببت دوافع الهجرة المناخية في العراق في زيادة حالات ندرة المياه وارتفاع درجات الحرارة والعواصف الرملية والجفاف وزيادة نسبة الملوحة في المياه وانخفاض الأمن الغذائي(*)(Food Security) نتيجة لزيادة التصحر وتقليص المساحات الزراعية. هذه الظروف القاسية تجبر الناس على مغادرة منازلهم ومناطقهم الأصلية بحثاً عن بيئة أفضل وفرص أفضل للعيش والعمل، تؤدي هذه الهجرة المناخية إلى تغيرات ديموغرافية خطيرة في المناطق المعنية، حيث يمكن أن تتسبب في زيادة الضغط الاجتماعي والاقتصادي على المناطق المستقبلة، بالإضافة إلى التحديات التي يواجهها النازحون في بدء حياة جديدة. ومنذ مطلع عام 2022 هناك حوالي 11 ألف عائلة أي ما يعادل 68 ألف فرد نزحت بسبب التغيرات المناخية خصوصاً في مناطق وسط وجنوب العراق(49).

وإزاء ما تقدم، يمكن القول يعد التغير المناخي أخطر عامل مؤثر في مفاقمة الهشاشة للصراعات الداخلية والإقليمية كما يساهم في هيجان "الاضطراب الاجتماعي"(Social unrest) ، ويشمل ذلك الصراعات العنيفة المسلحة. إذ إن السياسات والبرامج التكاملية في ثلاث قطاعات مفتاحية -التغير المناخي مع التكيف، والتنمية والمساعدة الإنسانية وبناء السلام- هي عوامل
حاسمة للمساعدة في تقوية المرونة اتجاه أخطار الهشاشة، وتحقيق المنافع المشتركة (50).

علاوة على ما سبق، فرضت سمة الاعتماد على القطاع النفطي مخاطر وتحديات تشكل عقبة امام تحقيق التنمية المستدامة في مجالات مشاريع معالجة ارتفاع مشكلة البطالة، إذ يعزز الاعتماد الكلي أو شبه الكلي على رؤوس الأموال الكبيرة الناتجة عن القطاع النفطي، إلى اهمال القطاعات التي تستقطب الايدي العاملة كالزراعة والصناعة، إذ أن الاعتماد المتزايد على القطاع النفطي بشكل مفرط حال دون تنمية الصناعات والنشاطات الاقتصادية التي تستقطب ايدي عاملة كبيرة (51).وهذا ما أكدته العديد من التقارير التي تشير إلى اعتماد العراق على نموذجٍ للنمو يعتمد بدرجة أساسية على النفط الذي أنتج تقلباتٍ اقتصادية. والذي من شأنه إحداث آثار سلبية على البيئة الداخلية للعراق، لا سيما فيما يتعلق بعدم قدرته على بناء اقتصادٍ

أكثر تنوعاً يقوده القطاع الخاص ويتميز بقدرته على خلق فرص العمل وتنمية رأس المال البشري، وفي الوقت نفسه بناء القدرة على الصمود لمواجهة آثار تغير المناخ[52]. يتضح من خلال ذلك أن مؤشرات الأداء المؤسساتي تظهر أن بطء السياسيات العراقية تجاه قضية المناخ، يعود إلى غياب التعاون التنظيمي ما بين القطاعات الحكومية المختلفة في المواضيع المتعلقة بتعزيز الاستجابة لمخاطر تغيرات المناخ .

من هذا المنطلق، من شأن الافتقار إلى الاستعداد لمواجهة آثار التغرير المناخي والفشل في تنويع اقتصادات البلدان العربية الهشة، أن يؤدي حتماً إلى الإفلاس. ومع انهيار ريع النفط، سيتعرض النمو الاقتصادي والتماسك الاجتماعي للخطر، وسيصيب الفشل المرافق والخدمات العامة. فقد أفاد تقرير صادر عن البنك الدولي في عام 2022 حول العراق، أن "الاعتماد على النفط وحده يمكن أن يضر بالدوافع المحلية لتنفيذ الإصلاحات الاقتصادية، مما من شأنه أن يعمق التحديات الاقتصادية الهيكلية في البلاد [53].

إضافة إلى ما تقدم، تبرز أهمية مواجهة المشكلات البيئية وايقاف تفاقمها من تشريع القوانين وفرض الإجراءات التي تحد من تلوث الماء والهواء والتربة ومعالجة النفايات والمخلفات على وفق نظمٍ متطورة للطمر الصحي وإعادة التدوير، فضلاً عن أهمية التوسع في سياسة الاعتماد على مصادر الطاقة المتجددة والنظيفة. وفي أثناء ذلك لا بد من تعزيز اسهام القطاع الخاص في معالجة القضايا البيئية[54].

إجمالاً، وعلى الرغم من كل الخطوات والإجراءات التي اتخذتها الحكومة لمواجهة التغير المناخي إلا هناك الكثير من العمل الذي يجب القيام به من أجل التخفيف من حدة التغيرات المناخية منها:[55]

أولاً: بناء الوعي المجتمعي لدى افراد الشعب بخطورة التغيرات المناخية وانعكاساتها على المجتمع من خلال تبني استراتيجيات خاصة بهذا الشأن، واشراك المجتمع المدني(Civil society) لا سيما الناشطين في مجال البيئة والمناخ في هذه الاستراتيجيات.

ثانياً: إن العامل الأبرز والمهم هو ضرورة بناء نظام مالي اخضر والاستفادة من الاتجاهات الحديثة في تمويل المشاريع المراعية للبيئة والمنخفضة الانبعاثات مثل (السندات الخضراء والأسهم الخضراء والاستثمارات المراعية للبيئة) ووضع اللوائح والتنظيمات المنظمة للعمل بها، وعلى سوق العراق للأوراق المالية تشجيع المستثمرين على الاستثمار في المجالات

والمشاريع الخضراء وإدراج الشركات التي تتداول بالأسهم الخضراء، والاستفادة من المؤسسات المالية الدولية والمؤسسات المانحة للتمويل الأخضر، ومحاكاة التجارب الناجحة في هذا المجال وتطبيقها في العراق.

الخاتمة

لقد شكلت مواجهة التغيرات المناخية أحد أهم الأولويات الاستراتيجية للحكومية العراقية ، بسبب التأثير الواضح التي اظهرته تغيرات المناخ بما تحمله من عبء وتداعيات على الوضع الداخلي، وبالتالي سيؤدي تفاقمها إلى مزيد من التهديدات والمخاطر على الأمن الوطني العراقي، إضافة إلى انعكاسات آثارها البيئية، لا سيما في ظل ارتفاع معدلات الجفاف والتصحر والغازات ... الخ، ولذلك عمل العراق على اتخاذ مجموعة من الإجراءات والسياسات المتعددة والتي تهدف إلى تعزيز جهوده للتعامل مع تلك التحديات، وهذا ما نجده في نهج الحكومة من خلال إبرام العديد من الاتفاقيات الدولية بهذا الخصوص، إلى جانب تعزيز تعاونه الإقليمي والدولي من أجل تحقيق أهدافه الاستراتيجية في التخفيف من آثار تغيرات المناخ من جهة، ومن ناحية أخرى التركيز على الطاقة المتجددة والنظيفة التي يمكن من خلالها أن تتضاءل مخاطر تغيرات المناخ، أضف إلى ذلك يسعى العراق من خلال تعاونه الخارجي ضمان فاعلية الأداء لمؤسساته المختلفة، كما سيكون العراق أكثر قدرة في تنفيذ التزاماته الدولية.

المصادر والمراجع:

---

(1) زينب مجدي ،" تغير المناخ في الدول العربية : الاثار والسياسات" ، **المجلة الدولية للسياسات العامة في مصر** ، المجلد (2)، العدد (4)،(مصر: 2023)، ص 94. وللمزيد حول هذا الموضوع ينظر: أندرو دسلر ، إدوارد أ. باسون ، **تغير المناخ العالمي بين العلم والسياسية : دليل للمناقشة** ، ترجمة: عبد المقصود عبد الكريم، (القاهرة: المركز القومي للترجمة ، 2014).

(*) يعرف "عدلي حسن سعيد" مفهوم الأمن الوطني بأنه :" يهدف إلى تأمين الدولة من الداخل ودفع التهديد الخارجي عنها بما يكفل لشعبها حياة مستقرة توفر له استغلال أقصى طاقاته للنهوض والتقدم والازدهار". نقلاً عن : علي عباس مراد، **الأمن والأمن القومي : مقاربات نظرية**،(الجزائر : أبن النديم للنشر والتوزيع، 2017)، ص 33.

(2) احمد سيد احمد ،التغير المناخي وتهديد الأمن الوطني والسلم الدولي، **موقع مجلة درع الوطن** ، 2023/12/3، شوهد في 2024/4/7، في: https://www.nationshield.ae/index.php/home/detail

(3) محمد نصر، "op27 ومحددات الموقف التفاوضي المصري"، **دورية الملف المصري**، العدد (99) ،(مصر: 2022)، ص6 .

(4) نيك فيريس، "رسوم بيانية تثير قلق العلماء من أزمة المناخ"، **موقع صحيفة اندبندنت عربية**، 28 /2023/8، شوهد في 2024/4/1، في: https://www.independentarabia.com/node/489516

(5) محمد نصر، **مصدر سابق** ، ص 6.

(6) منى طواهرية ، "التغيرات المناخية ورهانات السياسة البيئية الدولية" ، **مجلة اقتصاديات شمال أفريقيا**، المجلد (16)، العدد (22)،(الجزائر:2020)،ص354.

(7) المصدر نفسه ، ص 352.

[8] انجي احمد عبد الغني مصطفى ،" الإدارة الدولية لقضية التغيرات المناخية"، **مجلة كلية السياسة والاقتصاد** ، العدد(3)،(مصر:2019)، ص 152.

[9] حازم محفوظ ، "أزمة التغير المناخي وتأثيراتها على الدول النامية" ، **دورية الملف المصري**، العدد (99) ،(مصر: 2022)، ص 32.

[*]يعرف مفهوم التكيف بأنه :" السياسات، والاستراتيجيات، والإجراءات، والعمليات، التي تسمح لبلد أو منطقة ما، بالتصدي للظروف المناخية المتغيرة، وإدارتها، والتأقلم معها . ويمكن للتكيف أن يكون إما تفاعلياً أو تلقائياً فقد يحدث التكيف بعد أن تصبح آثار تغير المناخ واضحة، أو قد يكون استباقياً عندما يحصل التكيف قبل أن تظهر الآثار". نقلا عن: الشيماء عبد السلام إبراهيم ، "آليات القيادة السياسية في التعامل مع قضية التغيرات المناخية : دراسة الحالة المصرية خلال الفترة (2014-2024)"،**مجلة كلية السياسة والاقتصاد**، المجلد(23)،العدد(22)،(مصر:2024)،ص 305.

[**] يشير مفهوم التخفيف بأنه :" أي إجراء تتخذه الحكومات والمجتمعات والشركات والأفراد لتقليل انبعاثات غازات الاحتباس الحراري أو منعها، وتشمل أمثله التخفيف كلمن الانتقال إلى الطاقة المتجددة مثل (الرياح والطاقة الشمسية)، والاستثمار في وسائل النقل الخالي من الكربون، وتعزيز الزراعة المستدامة واستخدام الأراضي، وزراعة الغابات حيث تعتبر مصارف للكربون، وتغيير ممارسات الاستهلاك وسلوكيات النظام الغذائي". نقلا عن : المصدر نفسه، ص 305.

[10] رشيد البزيم ، "مستقبلات سياسات التخفيف من آثار التغيرات المناخية في المنطقة العربية" ، **مجلة استشراف للدراسات المستقبلية** ، العدد (8)، (قطر: 2023)،ص 46.

[11] انجي احمد عبد الغني مصطفى ، **مصدر سابق** ، ص 152.

[*] يشير مفهوم الاحترار العالمي إلى :" زيادة في متوسط درة حرارة سطح الأرض، بسبب زيادة تركيز الغازات الدفيئة في الغلاف الجوي وهي (غاز ثاني أكسيد الكربون، وغاز الميثان، وغازات ثاني أكسيد النتيروز، والهيدروفوركربون، والبيروفلوروكربون، وسادس فلوريد الكبريت)تمتص هذه الغازات المزيد من الإشعاع الشمسي وتحول دون خروج الطاقة مما يؤدي الى حبس المزيد من الطاقة داخل الغلاف الجوي، ومن ثم يحدث ارتفاع معدل درجات الحرارة". نقلا عن : الشيماء عبد السلام إبراهيم ، **مصدر سابق**، 305.

[12] زينب مجدي ، مصدر سابق ، ص 98.

[13] غلايدا لان ، وغريغ شابلاند ، **المخاطر المناخية المتعاقبة وخيارات تعزيز المنعة والتكيف في الشرق الأوسط وشمال أفريقيا** ، ترجمة : أشرف إبراهيم ، (بلا بلد، المفوضية الأوروبية ،2022)، ص 3.

[14] عائشة السريحي ، "إدارة تغير المناخ في منطقة الخليج العربي: السياسات والتحديات والآفاق"، **مركز الامارات للدراسات** ، 3 /8/ 2023، شوهد في 2024/4/7، في: https://epc.ae/ar/details/featured/idarat-t

[15] حازم محفوظ ، مصدر سابق، ص 32.

[16] منى طواهرية ، **مصدر سابق** ، ص 355.

[17] احمد سيد احمد ، **مصدر سابق** .

[18] عبدالله رشيد مجيد ، "التغيرات المناخية واستراتيجية الأمن القومي العراقي: درجات حرارة متصاعدة ومخاطر متزايدة" ، **مجلة حوار الفكر** ، العدد (64)،(العراق: 2022)، ص 7.

[19] سلطان جاسم النصراوي،" التغير المناخي في العراق: مشكلة مركبة بحاجة إلى حل"، **جامعة كربلاء -كلية الإدارة والاقتصاد** ، 2022/10/4، شوهد في 2024/4/11، في: https://business.uokerbala.edu.iq/

[20] شيماء محمد ناصر العبدالي، "المرأة العراقية في ظل التغير المناخي: التحديات والمعوقات واستراتيجيات التمكين" ، **مجلة قضايا سياسية** ، العدد (76)،(العراق:2024)، ص 242.

[21] "عدم التصدي لتغير المناخ في العراق يعرِض الاستقرار الاجتماعي وآفاق التنمية الاقتصادية للخطر" ، **موقع البنك الدولي** ، 2022/9/11، شوهد في 2024/4/1، في: https://www.albankaldawli.org/ar/n

[22] محمد صادق اسماعيل، "العمل العربي الجماعي وجهود جامعة الدول العربية في الحد من التأثيرات المناخية" ، **مجلة آفاق عربية وإقليمية** ، المجلد (6) ، العدد (11)، (مصر:2022)، ص59.

[23] المصدر نفسه.

[24] علي ضاري محمد ، فراس عبد الجبار الربيعي ، "استراتيجيات مواجهة التغيرات المناخية في العراق"، **مجلة ديالى للبحوث الإنسانية** ، العدد (84)،(العراق: 2020)، ص 472.

[25]علي ضاري محمد ، فراس عبد الجبار الربيعي ، **مصدر سابق** ، ص 473.

[26] محمد خليف، "نقل التكنولوجيا وحلول مواجهة تغير المناخ ... التحديات والفرص"، **مجلة السياسة الدولية** ، العدد (230)،(مصر:2022)، ص72.

[27] انجي احمد عبد الغني مصطفى، **مصدر سابق،** ص 155.

[28] احمد قنديل، "الاتفاقيات العالمية لمواجهة التغير المناخي وحدود فعاليتها"، **مركز الاهرام للدراسات السياسية والاستراتيجية** ، 2022/1/19، شوهد في 2024/4/5، في: https://acpss.ahram.org.eg/News/176

[29] جهاد أزعور, حسن دودو, لينغ زو ، "كيف يمكن لمنطقة الشرق الأوسط وآسيا الوسطى معالجة التحديات المناخية على نحو أفضل" ، **صندوق النقد الدولي** ، 29 /11/ 2023، شوهد في 2024/4/8، في: https://www.imf.org/ar/Blogs/Articles/2023/11/29/how-the-middle-east-and-centr

[30] المصدر نفسه.

[31] انجي احمد عبد الغني مصطفى ، **مصدر سابق،** ص 155.

[*] **تعرف التنمية المستدامة على أنها :**" التنمية التي تلبي احتياجات الجيل الحاضر دون التضحية أو الإضرار بقدرة الأجيال القادمة على تلبية احتياجاتها". نقلا عن: نزار عوني اللبدي ، التنمية المستدامة : استغلال الموارد الطبيعية والطاقة المتجددة ،) الأردن : دار دجلة ناشرون وموزعون ، 2015)، ص 52.

[**] يعرف مفهوم الطاقة المتجددة بأنه:" الطاقات التي نحصل عليها من خلال تيارات الطاقة التي يتكرر وجودها في الطبيعة على نحو تلقائي ودوري وهي بذلك على عكس الطاقات غير المتجددة الموجودة غالباً في مخزون جامد في الأرض يمكن الإفادة منها إلا بعد تدخل الإنسان لإخراجها". نقلا عن : أبو تراب تغريد قاسم ، "الطاقة المتجددة وأثارها البيئية والاقتصادية في العراق" ، **مجلة الدراسات التجارية والاقتصادية المعاصرة** ، المجلد (4)، العدد(2)،(الجزائر:2021)،ص243.

[32] "التغيرات المناخية وكيفية الحد من آثارها السلبية"، **موقع Eduhub 2021 ،** شوهد في 2024/4/3، في: https://eduhub21.com/%D8%A8%D8%AD%D8%AB-%D8%B9%D9%86

[33] المصدر نفسه .

[34] محمد صادق اسماعيل، **مصدر سابق ،** ص 57.

[35] "هل تنجح الاستراتيجية الجديدة في حل مشكلات البيئة العراقية المزمنة" ، **موقع صحيفة الشرق الأوسط** ، 2 /2/2024،شوهد في 2024/4/10، في: https://aawsat.com/%D8%A8%D9%8A%D8%A. وللمزيد من المعلومات حول تنظيم داعش الإرهابي انظر : هشام الهاشمي، **عالم داعش : تنظيم الدولة الإسلامية في العراق والشام،** (لندن : دار الحكمة ، 2015). وأيضاً انظر : مازن شندب ، **داعش : ماهيته ، نشأته ، إرهابه ، أهدافة ، استراتيجيته،** (بيروت : الدار العربية للعلوم ناشرون ، 2014).

[36]هل تنجح الاستراتيجية الجديدة في حل مشكلات البيئة العراقية المزمنة"، **مصدر سابق.**

[37] التقرير الطوعي الوطني الثاني للمتحقق من أهداف التنمية المستدامة 2021، (العراق : وزارة التخطيط ، 2021)،ص 77.

[38] "العراق.. خطط طموحة لمواجهة الآثار السلبية للتغير المناخي" ، **مركز الاتحاد للأخبار** ، 9 /11/ 2023،شوهد في 2024/4/1، في: https://www.aletihad.ae/news/%D8%BB9%D8%B1%8A

[39] "العراق.. خطط طموحة لمواجهة الآثار السلبية للتغير المناخي" ، **مصدر سابق** .

[40] جيهان بابان، "تفاقم ظاهرة التغير المناخي وأولويات العراق في الاستدامة البيئية"، **موقع صحيفة الصباح** ، 2024/1/24، شوهد في 2024/4/10، في : https://alsabaah.iq/90989-.html

[41] علي ضاري محمد ، فراس عبد الجبار الربيعي، **مصدر سابق** ، ص ص 481-482.

[42] المصدر نفسه ، ص 482.

[43] "رهانات صعبة: تغيُّر المناخ.. تحديات تواجه الدول في سبيل مجابهة آثاره "، **المستقبل للأبحاث والدراسات المتقدمة** ، 12/8 /2023، https://futureuae.com/ar-AE/Mainpage/Item/8835

[44]"رهانات صعبة: تغيُّر المناخ.. تحديات تواجه الدول في سبيل مجابهة آثاره "، **مصدر سابق** .

[*] **يعرف الحكم الرشيد بأنه:**" الحكم الذي تقوم به قيادات سياسية منتخبة ،واطارات إدارية ملتزمة بتطوير افراد المجتمع برضاهم وعبر مشاركتهم في مختلف القنوات السياسية للمساهمة في تحسين نوعية حياتهم ورفاهيتهم ". نقلا عن : ابتسام حاتم علوان ،" ترشيد الحكم في التجربة العراقية ... الأبعاد والمعالجات"، **المجلة السياسية والدولية** ، المجلد (1)، العدد (43)،(العراق: 2020)،ص 26.

[45] رشيد البزيم ، مصدر سابق ، ص 49.

[46] رشيد البزيم ، مصدر سابق ، ص 49.

[47] "تحديات المرونة والتكيُّف: حدود الاستجابة للتغيُّر المناخي في منطقة القرن الأفريقي" ، **مركز الإمارات للسياسات** ، 13/ 4/2023، شوهد في 2024/4/14، في: https://epc.ae/ar/details/featured/taha

[48] مروان محمد عبود، "سياسات المناصرة المناخية في العراق : الواقع والطموح"، **مركز البيان للدراسات والتخطيط**،2023/8/26، شوهد في 2024/15، ص ص 3-4. متاح للتحميل على الرابط: https://www.bayancenter.org/2023/08/10148

[*] يعرف الأمن الغذائي بأنه:" توفير احتياجات جميع سكان الدولة من السلع، والمواد الغذائية بالقدر المطلوب ، والأنواع المختلفة من الطعام، والشراب، والمواد الغذائية اللازمة بالقدر الذي يحتاجه الناس، وفي الوقت نفسه مع عدم توقع وقوع نقص الغذاء في المستقبل". أما منظمة الأغذية والزراعة التابعة للأمم المتحدة تعرف الأمن الغذائي بأنه:" ضمان حصول كل الأفراد وفي كل الأوقات على كفايتهم من الغذاء الذي يجمع بين النوعية الجيدة والسلامة، كي يعيشوا حياة نشطة موفورة الصحة ولا يأتي ذلك إلا بتوفير امدادات غذائية مستقرة تكون متاحة مادياً واقتصادياً للجميع". نقلا عن : عبد الجبار محسن ذياب الكبيسي، **تحديات الأمن الغذائي في الوطن العربي وآفاقه المستقبلية: خلال العقد الأول من القرن الحادي والعشرين**، (عمان: آمنة للنشر والتوزيع، 2014)،ص ص 22 - 25.

[49] مروان محمد عبود، **مصدر سابق** ، ص ص 4-5.

[50] علي كريم كاظم، معن عبد الكاظم رشيد، "تحديات التغير المناخي في العراق والمنطقة"، **مركز البيان للدراسات والتخطيط**، 2022/11/26، شوهد في 2024/4/15، ص8. متاح للتحميل على الرابط:
https://www.bayancenter.org/2022/11/9058

[51] احمد عبدالله ناهي، محمد ارمين كربيت، "التنمية المستدامة في العراق : التحديات والمعالجات" ، **مجلة قضايا سياسية** ، العدد (65)،(العراق: 2021)، ص 20.

[52]"عدم التصدي لتغير المناخ في العراق يعرِض الاستقرار الاجتماعي وآفاق التنمية الاقتصادية للخطر"، **مصدر سابق**.

[53] رشيد البزيم ، **مصدر سابق** ، ص 64.

[54] مجموعة باحثين، **المستقبل الذي تصبوا اليه : رؤية العراق للتنمية المستدامة 2023** ، (بغداد : وزارة التخطيط ، 2019)، ص 53.

[55] سلطان جاسم النصراوي، مصدر سابق .

البحوث والدراسات الأمنية

الأساس القانوني
لدور مجلس الأمن والمحكمة الجنائية الدولية في مكافحة الجرائم الدولية

العقيد م. الحقوقي. انصيف جاسم محمد التكريتي
مقدم اللواء الخامس/ قيادة فرقة الرد السريع

يُعدَّ إنشاء المَحْكَمَة الجِنائِيَّة الدوْلِيَّة، أمرا غايةً في الأهمية على مستوى القَانُون الجنائي الدَّولي، لا سيما في الجانب الذي يتعلق بتدوين وتقنين عدَّة قوانين دوْلِيَّة جديدة، لأن ما توصل إليه مشرعو النِظَام الأساس للمَحْكَمَة، قد وصلوا إليه بعد جهودٍ متوازنة وكبيرة امتدت لما يزيد عن قرن كاملٍ من الزمان، حيث جاءت هذه الجهود لمعالجة موضوع الجَرِيمة الدوْلِيَّة، وخصوصاً بعد الحَرْب العالمية الأولى والثانية، وما تمخض عنهما من الويلات التي أدت إلى تشكيل محاكم عديدة لتنظر في الجَرَائِم الدوْلِيَّة التي جرى ارتكابها في تلك الفترة بحق بعض الشعوب، عليه يتخصص هذا البحث في بيان الأساس القانوني لمجلس الأمن والمحكمة الجنائية الدولية في مكافحة الجرائم الدوليَّة.

الكلمات المفتاحية: الأساس القانوني، مجلس الأمن، المحكمة الجنائية الدولية، الجرائم الدولية.

Legal basis The role of the Security Council
and the International Criminal Court in combating international crimes

Colonel Ansif Jassim Muhammad Al-Tikriti
Lieutenant Colonel of the Fifth Brigade / Rapid Response Division Command

This establishment of the International Criminal Court is considered an extremely important matter at the level of international criminal law, especially in the aspect that relates to the codification and codification of several new international laws, because what the legislators of the basic system of the Court have achieved, they have achieved after balanced and significant efforts spanning more than a century. A whole period of time, as these efforts came to address the issue of international crime, especially after the First and Second World Wars, and the calamities that resulted from them, which led to the formation of many courts to look into the international crimes that were committed during that period against some peoples. Therefore, this research specializes in Statement of the legal basis of the Security Council and the International Criminal Court in combating international crimes.

Keywords: legal basis, Security Council, International Criminal Court, international crimes.

الاستلام 2024/04/20
الارجاع 2024/05/12
القبول 2024/06/05

المقدمة

كان الشغل الشاغل للجماعة الدوْلِيَّة في مكافحة ومعالجة الجَرَائِم الدوْلِيَّة الماسة بأمِنْهَا وسلامتها منذ بداية العصر الحديث، فقد عالجت دراستها وبحوثها على مراحل زمنية متعاقبة، وكان لدور تلك الجهود أن يظهر إلى العلن النِظَام الأساسي للمَحْكَمَة الجِنائِيَّة الدوْلِيَّة عام 2002، متمخض عن محاكم دوْلِيَّة مؤقتة، ابتدأت في عام 1919 عقب انتهاء الحَرْب العالمية الأولى، وكذلك عقب انتهاء الحَرْب العالمية الثانية في محكمتي نورمبورغ وطوكيو عام 1946، ومن ثم بعد الانتهاكات الجسيمة التي طالت الجماعة في يوغسلافيا ورواندا عام 1994، ألا أنَّ ذلك تخلله محاكم جِنائِيَّة مشتركة كَمَحْكَمَة كمبوديا عام 1975، وتلك اعتبرت لبنة بناء قضاء دوْلِيَّة.

إلا إنَّه وعلى وفق مبدأ استقلالية القضاء، فقد اقرت الْجَمْعِيَّة الْعَامَّة للأمم المتحدة استقلالية المَحْكَمَة الدوْلِيَّة الخاصة بالنظر في جرائمِ الحَرْبِ، وجَرَائِم الإبادةِ، والجرائم التي تحدث ضد الإنسانية، وجرائم العدوان، بيد أن تحريك الشكوى بخصوص انتهاكات الجَرَائِم المذكورة، اقتصر في المادة 12 من النِظَام الأساسي على المنظمة إليها، لكن المادة 13 منه، أعطت دور لمجلس الأمن الدولي تحريك الشكوى، وفق إجراءات رسمتها تلك المادة، وبالاستناد الى صلاحياته المنصوص عليها في الفصل السابع من مِيثَاق الأمم المتحدة في حفظ السلم والأمن الدوليين.

وعليه سيتطرق هذا البحث الى الأساس القَانُوني لدور مجلس الأمن والمَحْكَمَة الجِنائِيَّة الدوْلِيَّة، كذلك سنتطرق لدور مجلس الأمن والمَحْكَمَة الجِنائِيَّة الدوْلِيَّة في إيجابيات وسلبياته، في المحاكم المؤقتة والمَحْكَمَة الدائمة، وتسلط الدول الكبرى على قَرَاراته واثر حق الفيتو على دور مجلس الامن في حفظ الامن والسلم الدولي، وعليه يطرح هذا البحث التساؤل الرئيس الآتي: ما اهم الانتقادات في الأساس القَانُوني لدور مجلس الأمن والمَحْكَمَة الجِنائِيَّة الدوْلِيَّة في مكافحة الجَرَائِم الدوْلِيَّة؟ ، ويندرج ضمن هذا التساؤل الرئيس حزمة من التساؤلات الآتية:

1- ما الجريمة والجريمة الدولية وما أركان الجريمة الدولية وأنواعها؟

2- ما الأساس القانوني لسلطة مجلس الأمن والمحكمة الجنائية الدولية في مكافحة الجرائم الدولية؟

من أجل الوصول إلى هدف البحث، سيتبع المنهج "الكيفي والتحليلي" بمنهجية علمية قَانُونية رصينة مبنية على أساس البحث والتقصي واستخلاص الحقائق، وتنظيمها وفقاً لأسس علمية قَانُونية رصينة، ويقوم على العلمية النقدية البناءة، من خلال جمع الأدلة والتتابع الزمني لدراسة الجَرِيمة وتطورها، والجهود الدوْلِيَّة للحد مِنْهَا ومعاقبة مرتكبيها، وبعض المحاكم المؤقتة السابقة.

المحور الأول: مفهوم الجريمة الدولية

إنَّ فكرة الجَرِيمة الدوْلِيَّة، بالمفهوم الدَّولي والقانوني، تعدُّ فكرةً حديثةً نسبياً، وارتباطها بتطور قواعد القَانُون الدَّولي والمعاصر هو ارتباطٌ كبيرٌ إلى حدٍ ما، لأن القاعدة السائدة في ظل القَانُون الدولي التقليدي تؤكد على أنْ تتضمن معاهدات السلام والتي تبرم على أثر الحروب نصوصاً خاصة عن العفو العام، و الذي يكونُ متبادلاً عن الأفعال التي أحدثتْ ضرراً، والتي حدثت من المتحاربين، أو من أفراد من القوات المسلحة، أو من الرعايا أثناء الحَرْب بسبب دوافعَ سياسيةً، مثل التسبب بإشعال فتيل الحَرْب، أو أعمال العنف والقتل، أو إلحاق الضرر بالممتلكات، وأفعالاً أخرى مشابهة لهذه الأفعال، ونجد أنَّ معظم معاهدات السلام قد تضمنته، خصوصاً ما أبرمَ منها في زمن القَانُون الدَّولي التقليدي.[1]

وهنا ارتفعت المطالبات التي تذهب إلى ضرورة إنزال العقوبات بمرتكبي الجرائم الدَّولية، وذلك لفداحة الأضرار والخسائر الناتجة، ومعاقبة كل من يرتكب فعلاً أو عملاً يخالفُ قواعدَ الحروب وعاداتها، وخاصة معاقبة مجرمي الحرب، وبسبب حدة الاستياء وصل الأمر إلى المطالبة بمحاكمة رؤساء الدُّول الذين ساعدوا على إشعال الحرب، أو كانوا سبباً بها، أو بارتكاب جرائمها[2]. وتعززت هذه المطالب بعد أن اندلعتْ الحَرْب العالمية الثانية، والتي انتهت بنسبة خسائر بَشَرِيَّة كبيرة أيضاً، وارتكبت فيها جَرَائِم وحشيةً عديدةً بين الدُّول المتحالفة، بشكلٍ مُخالفٍ لجميع القواعد التي يتضمنها القَانُون الدولي، والاتفاقيات الدوْلِيَّة السائدة آنذاك، فقد قُتل خلال هذه الحَرْب (54) مليونَ إنسانٍ، وجُرِحَ (90) مليوناً آخرين، وتَعُّوقَ (28) مليونَ إنسانٍ، وكل هذا أدى إلى دعواتٍ متتالية ومتزايدة بشكلٍ مبكرٍ سبقَ انتهاء أعمال الحَرْب، وذلك من أجل محاكمة كل مَن تسبب وارتكبَ الجرائمَ البشعة، والانتهاكات الدوْلِيَّة، وعلى هذا توافق المنتصرون من الحلفاء على أنَّه يجب محاكمة المتهمين بارتكاب الجَرَائِم، وانتهاكات حقوق الإنسان، ومرتكبي أعمالَ الإبادةِ، والمخالفين لعادات

الحروب وقوانينها، وهذا ما تجسدَ في محكمة (نورمبرغ)، ومحكمة (طوكيو)، وهاتانِ المحكمتانِ شكلتا البداية الحقيقية، بالرغم من كل ما شابها من العيوب والانتقائية، لتقوم بترسيخ مفهوم (الجَريمة الدوْلِيَّة)، ووجوب معاقبة من يرتكبها، وهو ما تعزز فيما بعد، خلال الممارسات الدوْلِيَّة[3].

عرفها "فتوح عبدُالله الشاذلي" بأنها" سلوك إنساني غير مَشْرُوع صادر عن إرادة إجرامية يرتكبها الفرد باسم الدولة، أو برضاء مِنْهَا، وينطوي على انتهاك للمصلحة الدوْلِيَّة يقرر القَانُون الدولي حمايتها عن طريق الجزاء الجنائي"[4].

كما عرفها "عبد الواحد محمد الفار" بانها: "فعل أو امتناع يعد مخالفة جسيمة لأحكام ومَبَادِئ القَانُون الدولي، ويكون من شأنه إحداث الاضطراب في الأمن والنِظَام العام الدولي، والمساس بالمصالح الأساسية والإنسانية للجماعة الدوْلِيَّة، وافراد الجنس البشري، مما يستوجب معه المسؤولية الدوْلِيَّة وضرورة توقيع العقاب الجنائي على مرتكب تلك المخالفة"[5].

وعرفها الفقيه "كرافن Krafin" بانها: "تلك الأفعال التي تتعارض مع احكام القَانُون الدولي ويترتب عليها المسؤولية الدوْلِيَّة، وهي لا تكون الا بالنسبة لأفعال ذات الجسامة الخاصة التي تحدث اضطراباً واخلالاً بالأمن العام للمجموعات الدوْلِيَّة"[6].

في حين عرفها الفقيه "لومبواز Loumbios": الجَرِيمة الدوْلِيَّة هي (عُدْوَانٌ) على المصلحة الأساس في المجتمع الدولي، والتي تتمتع بحمايةٍ من النِظَام القَانُوني، وذلك من خلال القواعد الخاصّة بالقَانُون الدولي الجنائي، أو هي (تصرفات) لقواعد القَانُون الدولي، تنتهك مصلحة مهمةً الجماعة الدَّوْلِيَّة، والتي قررت أنْ تحميها بقواعد القَانُون الدَّولي"[7].

وقد عرفها الفقيه "بلاوسكي Plawski" بأن الجَرِيمة الدوْلِيَّة هي "تصرف غير مَشْرُوع معاقب عليه بمقتضى القَانُون الدولي لاضراره بالعلاقات الإنسانية للجماعة الدوْلِيَّة"[8].

ومن خلال التعريفات السابقة نرى بأن لا يوحد تعريف محدد متفق عليه للجَرِيمة الدوْلِيَّة، وبالرغم من ذلك هنالك تقارب بين التعريفات العربية والغربية، وهذا التقارب يتفق على انها: الأفعال التي تتخالف مع أحكام القَانُون الدَّولي، وتترتب عليها مسؤولية دوْلِيَّة، وتكون للأفعال الجسيمة الخاصَّة، والتي تؤدي إلى اضطرابٍ وإخلالٍ بأمنِ المجموعات الدَّوليةِ العام.

المحور الثاني: أنواع الجَرَائم الدوْلِيَّة

وتحت هذا الإطار نجد بأنَّ أهمية إنشاء مَحْكَمَة جِنائِيَّة دوْلِيَّة يكمن في إنَّها تتجاوز بالنِظَام الأساسي الخاص بها الإطار التقليدي، فهو يضع للجرائِم المختلفة تعريفاً شاملاً، طبقاً لما جاء في البنود القَانُونية الدوْلِيَّة ونصوصها[9]، فلم يقتصر توصيف الجَرَائِم الحَرْبية على ما تضمنته الحروب من تجاوزات قانونية وجرائم -وهذا بموجب المادة (8) من نِظَام المَحْكَمَة الجِنائِيَّة الدوْلِيَّة الأساس، بل اشتمل على تجاوزات أُخر، تظهر عند حدوث حروب أهلية أو نزاعات داخليَّة، إضافة لتجاوزات الحرب، ويُعدُّ هذا تطويراً ملحوظاً، وتوسيعاً شاملاً لمفهوم (جرائم الحرب) بحسب ما سبق من النصوص، وهذا يعني أنَّ القَانُون الدولي الإنساني في تطورٍ حديث.

وقد ابدعت اللجان التحضيرية عندما قامت بتعْداد كل ما يشكل جَرائماً ضد الإنسانية، فقد ذكرت إضافةً إلى القتل المتعمد، أو الاغتصاب، أو التعذيب أو (وهي عناصر إجرامية معروفة) عدة جَرَائِم : كجريمة الاستبداد الجنسي، والإكراه على الحمل، أو البغاء، أو التعنيف الجنسي، والاختفاء القسري. وهكذا وبعد وضع هذه المادة، نضمن محاكمة هذه الجَرَائِم والتي هي خارج نطاق جرائم الحَرْب، سواءً في حالة الحرب أو حالة السلام، وعند النظر لهذه المادة، فإننا لا نستغرَب من تهرّب (إسرائيل) من القبول بهكذا معاهدة؛ أنَّها توفّر الفرصة للضحايا الذين اعتدت عليهم بأن يطالبوا بإعادة النظر في جَرَائِم قادتها وجرائم مواطنيها، ممّا قد يؤدي ذلك إلى محاكمتهم؛ ولذا فإنَّ اسرائيل لم تقدّم على التوقيع على النِظَام الأساسي، إلا بعد تقديم الضمانات لحمايتها من قِبل الولايات المتحدة الأمريكية[10].

وجاء نص المادة "5" من نِظَام (رُومَا) الأساسي،[11] عن المَحْكَمَة الجِنائِيَّة الدوْلِيَّة واختصاصها بشكلٍ حصريٍّ، وهو ما سنتناوله تفصيلاً، مع التركيز على اخطر الجَرَائِم الدوْلِيَّة والتي تتمثل بـ : " وجَرائِم الإبادة الجماعية، وجرائم العدوان، والجَرَائِم الحربية، وجَرَائِم ضدَّ الانسانيَّة" ونبينها على النحو الآتي:

اولاً: جَرِيمَة الإبادة الجماعية

إنَّ الجَرَائِم الدوْلِيَّة التي تمس الجنس البشري تعدُّ من أكثر الجَرَائِم شدَّةً وخطورة ضد البشر، إذ أنها تذهب إلى المساس بحياة الشخص، أو مجموعةَ الأشخاص، أو مساس حرياتهم،

أو أبسط حقوقهم، أو ادميتهم، وإن تلك الجَرَائِم في مجموعها تشكلُ ما يطلق عليه بـ (الجَرَائِم الإنسانية).

تعدُّ جَرِائم الإبادة من الجرائم التي امتدت جذورها عبر تاريخٍ طويل، وكَانَتْ تتمثل في إغارة المجتمعات والقبائل على بعضها البعض، وإبادة بعضهم بعضاً، من أجل الحصول على الثروات والنفوذ والغنائم، إنَّ الظهور الأول لمصطلح (الإبادة الجماعية) كان باستخدام الفقيه (ليميكن) في دراسة كان قد أعدَّها عام 1944م، من أجل توضيح خصوصية الجَرَائِم التي ترتكب من قبل النازية، والفظائع التي يمارسونها ضد الإنسانية، وبالأخص الأفعال التي تهدف إلى تدمير دول أوربا، والتي تقع تحت الاحتلال النَّازي، وجرمنة هذه الدَّول، وقد أورد (ليميكن) تعريفاً لهذه الجَرِيمة ويذهب إلى أنَّ : "كل من اشترك أو تآمر من أجل القضاء على جماعة وطنية، بسببٍ متعلق باللغة، أو الجنس، أو حرية وملكية أعضاءِ هذه الجماعة يعد مرتكباً لجَرِيمة إبادة جنس بشري"[12].

كانت سلسلة جَرَائِم بشعة تلك التي ارتكبت خلال الحَرْب العالمية الثانية، ضدَّ الجنس البشري، وما رافقها من هدرٍ لحقوقِ الإنسانِ، وانتهاك حرياته، وحقه في الحياة، واستعمال وسائل وحشية مختلفة في التعذيب، والقتل، والاعتداء على حرية الافراد، وكان لسلسلة الجرائم هذه أثرها على اتجاه الدول قاطبة، نحو إقَرَار المَبَادِئ التي تختص بمواجهة جَرِيمة الإبادة الجماعية بكافة أشكالها، والتي تشمل الإبادة المادية، أو المعنوية، أو الثقافية، ومن صور جَرِائم الإبادة الجماعية اثناء الحَرْب العالمية الثانية؛ القنبلة النووية التي تمَّ إلقاؤها على (هيروشيما) و(ناجازاكي) عام 1945م، والتي أبادت سكان هذه المدن بالكامل، بغض النظر عن انتمائهم الى أي جماعة، فقط لكونهم رعايا دولة من دول الأعداء[13].

وبذلك تعْد جَرِيمة الإبادة الجماعية من اخطر الجَرَائِم التي تهدد الجنس البشري وتمثل اعتداء يصيب الانسان بصفته الشخصية إذا كان منتمياً الى جماعة معينة، في كرامته وصته وحياته، وتعتبر جَرِيمة الإبادة الجماعية من الجَرَائِم القديمة[14] ، واخذ المجتمع الدولي يتنبه الى خطورة هذه الجَرَائِم على المستوى الدولي، خصوصاً بدايات القرن العشرين لمساسها الحقوق الإنسانية حق الحياة، في 11 ديسمبر 1946 أصدرت الْجَمْعِيَّة الْعَامَّة للأمم المتحدة قَرَاراً يتضمن اعلانا باعتبار إبادة الجنس البشري جَرِيمة ولية لتعارضها مع مقاصد الأمم المتحدة ويستنكرها الضمير الإنساني، ثم جاءت مرحلة اخرى من مراحل تعريف إبادة الجنس

البشري وهي المحلة التي مهدت لإقَرَار اتفاقية منع الإبادة الجماعية والمعاقبة عليها لعام 1948، وقد أقرت الْجَمْعِيَّة الْعَامَّة هذه الاتفاقية في 1948/12/9م[15].

وقد ورد في نِظَام رُومَا الأساسي تجريم الإبادة الجماعية في المادة السادسة منه وعند اطلاعنا عليه وجدناه مطابقا الى حد بعيد لما ورد في المادة الثانية من اتفاقية الإبادة الجماعية لعام 1948.

وقد نصت المادة "6" من النِظَام الأساسي للمَحْكَمَة الجِنائِيَّة الدوْلِيَّة على: "لغرض هذا النِظَام الساسي، تعني "الإبادة الجماعية" أي فعل من الأفعال التالية يرتكب بقصد اهلاك جماعة قومية أو اثنية أو عرقية أو دينية، بصفتها هذه، اهلاكا كليا أو جزئيا: "أ" قتل افراد الجماعة. "ب" الحاق ضرر جسدي أو عقلي جسيم بأفراد الجماعة. "ج" اخضاع الجماعة عمدا لأحوال معيشية يقصد بها اهلاكها الفعلي كليا أو جزئياً. "د" فرض تدابير تستهدف منع الانجاب داخل الجماعة. "هـ" نقل أطفال الجماعة عنوة الى جماعة أخرى"

وعند امعان النظر فيما ورد أعلاه نجد أن هذه المادة لا تخلو من غموض في مصطلحاتها وذلك في تعبيرها بلفظ الجماعة والمعيار الذي على أساسه قسمت هذه الجماعة الى عرقية ودينية وقومية واثنية، وكذلك المراد بالإهلاك الكلي أو الجزئي، أما الكلي فمعروف لكن الجزئي لا يعلم المراد منه أن كان أكثر من النصف أم أقل أم يكفي قتل شخص واحد مع وجود القصد الجنائي، لكن ما اعتمدته جمعية الدول الأطراف في المذكرة التفسيرية لأركان الجَرَائِم[16] في جَرِيمة الإبادة الجماعية هو استعمالها عبارة "شخص أو أكثر " في معظم الأفعال التي تشكل جَرِيمة دوْلِيَّة.

وكذلك الفعل الثاني من أفعال الإبادة وهو الحاق الضرر الجسدي أو العقلي الجسيم بأفراد الجماعة، فقد آثار هذا الفعل بعض الإشكالات اثناء مناقشات رُومَا، وكان أبرزها بيان مدى هذا الضرر الجسدي أو العقلي الذي يعتبر إبادة وقد اتفق في الأخير على كون الفعل ينطوي على كافة صور الضرر المادي أو المعنوي التي يمكن أن تؤثر وبشكل خطر على سلامة البدن والعقل مما يهدد تدمير الجماعة[17].

وقد جرمت الاتفاقية الدوْلِيَّة فعل إبادة الأجناس البشرية هذا، في وقت الحرب والسلم على حدٍّ سواء، فهي من الجرائم التي لا يشترط وقوعها وقت الحَرْب فقط، وقد جاء بنص المادة الأولى من الاتفاقية: "تؤكد دول التعاقد على أنّ كل فعل يرمي إلى إبادة الجنس

البشري سواءً ارتكب أيام السلم، أو اثناء الحَرْب، فهو جَرِيمة في نظر القَانُون الدولي، ونتعهد بمنعه والمعاقبة عليه"، وقد أكدت الاتفاقية الخاصة بجرائم الإبادة الجماعية والصادرة عن الْجَمْعِيَّة الْعَامَّة للأمم المتحدة، المبدأ الذي كانت مُحَاكَمَات (نورمبرج) قد استقرت عليه، كما قامت مَحْكَمَة رواندا بتأكيده في قضية Rutaganda، وذهبت لجنة القَانُون الدولي للأمم المتحدة في عام 1996م على تأكيد تحديد جَرِيمة (الإبادة الجماعة) بوقت إعدادها مَشْرُوعَ قَانُونِ الجَرَائِم ضد أمن وسلم البَشَرِيَّة.

قامت جَرِيمة الجنس البشري اهتمام الرأي العام العالمي بعد الحَرْب العالمية الثانية، باعتبارها فعلاً من الأفعال الاجرامية الداخلة ضمن تصنيف الجَرَائِم ضد الإنسانية، فهي وأن كَانَتْ مستحدث من مستحدثات نِظَام نورمبيرغ، إلا أن الباعث الدافع لتقنين هذه الجَرِيمة يكمن في ملايين الضحايا الذين ابادتهم النازية أو عملت على ابادتهم، ولقد استفادت الصهيونية من هذه الجَرِيمة في لفت انتباه العالم وفي التعاطف معه، ورغم أن هذه الجَرِيمة لم يختصر ارتكابها على اليهود إذ تعرض كل سكان أوربا إلى القتل والتهجير من قبل النازيين، وما أن تمكنت الصهيونية من إنشاء دولتها في فلسطين حتى بدأت تمارس ذات الجَرِيمة وبشكل مدروس ومنظم ضد عرب فلسطين، ومثالها مذبحة دير ياسين وكفر قاسم وسواها من المجازر التي ما زالت والى يومنا هذا ترتكب في فلسطين المحتلة ضد الشعب والمقدسات[18].

1. الرُكْن المادي لجَرِيمة الإبادة الجماعية

نكون بصدد الرُكْن المادي لجَرِيمة إبادة الجنس البشري إذ توافرت أحد الأفعال التي نصت عليها المادة "2" من اتفاقية منع جَرِيمة الإبادة، ويمكن بيانها فيما يلي:

أ- **قتل أفراد أو أعضاء الجماعية:** ويقصد به قتل عدد معين من الجماعة البَشَرِيَّة وليس فرداً واحداً مِنْهَا، وكذا يستوي أن تكون الإبادة جماعية، فضلاً عن وقوع الفعل بصفة إيجابية وسلبية.

ب- **إلحاق ضرر أو اذى جسدي أو عقلي بأعضاء الجماعة:** ويشترط هنا أن يكون الفعل بدرجة من الجسامة مما يؤثر على وجود أعضاء الجماعة البَشَرِيَّة، ويتحقق هذا الفعل بكل وسيلة مادية أو معنوية لها تأثير على أعضاء الجماعة مثل الضرب او التشويه الذي يؤدي الى عاهات مستديمة أو تعذيب.

ج- **إخضاع الجماعة البَشَرِيَّة لظروف معيشية قاسية "الاهلاك، التدمير" الفعلي كلياً كان أم جزئياً:** وابرزت مثال على ذلك كالإقامة في مكان ما، يخلو من سبل العيش الكريم كلها، حيث لا ماء فيه ولا زرع، أو تحت ظروف مناخية غير يسيره تجلب الأمراض، دون تقديم أيَّ سبلٍ للحياةِ[19].

د- **فرض تدابير ترمي الى منع او إعاقة النسل داخل الجماعة:** ويتمثل هذا الفعل في خضوع أعضاء الجماعة لعمليات إعاقة النسل أو التوالد مثل أعضاء، وتعقيم نسائهم بعقاقير تفقدهم القدرة على الحمل، والإنجاب وإكراههن على الإجهاض عند تحققه[20].

ه- **نقل أطفال أو صغار الجماعية قهرا أو عنوة من جماعتهم الى جماعة أخرى:** وهو نوع من أنواع الإبادة الثقافية أو التغيير الديموغرافي القسري، إذ يمثل هؤلاء الأطفال مستقبل الجماعة الثقافي واستمرارها، وتجدر الملاحظة أن المادة "3" من إتفاقية منع الإبادة تسوي من حيث المسؤولية الجِنائِيَّة بين الجَرِيمة التامة والشروع، وقد نصت على المساهمة وكذا التآمر والتحريض.

2. الرُكْن المعنوي

نصت المادة الثانية من اتفاقية الإبادة الجماعية على "أن تكون الأفعال المكونة للجَرِيمة بقصد التدمير الكلي أو الجزئي لجماعة قومية أو اثنية أو عنصرية أو دينية"، وقد شدد نِظَام المَحْكَمَة الجِنائِيَّة الدوْلِيَّة على أهمية الرُكْن المعنوي فوفقا للمادة "30" بنصه على "مالم ينص على غير ذلك، لا يسأل الشخص جنائياً على ارتكاب جَرِيمة تدخل في اختصاص المَحْكَمَة ولا يكون عرضة للعقاب على هذه الجَرِيمة إلا إذا تحقق الرُكْن المادي مع توافر القصد والعلم، فتلك الجَرِيمة لا يتصور ارتكابها بدون علم بأن عواقب معينة يمكن أن تترتب عليها، فهي ليست من الأفعال التي قد تحدث بصورة عرضية أو حتى نتيجة لمجرد الإهمال"، ولا يكفي القصد العام لقيام الرُكْن المعنوي في هذه الجَرِيمة؛ إنما يجب توافر القصد الخاص لدى الجاني الذي يتمثل في تدمير جماعة تشكل كياناً مستقلاً، وليس مجرد بعض الافراد[21]، وفي هذا الصدد ميزت الْجَمْعِيَّة الْعَامَّة للأمم المتحدة بين جَرَائِم الإبادة وجَرَائِم القتل، إذ وصفت جَرِيمة الإبادة بانها انكار لحق وجود يكون هذا القصد موجه لتدمير أحد أنواع الجماعات التي تشملها الاتفاقية

أي جماعة قومية أو اثنية أو عرقية أو دينية، وقد ضمنت الجماعات السياسية في تعريف الاضطهاد الوارد في مِيثَاق نورمبرغ، ولكنها لم تدرج في تعريف الإبادة الجماعية[22].

3. الرُكْن الدولي:

غالبا ما تكون هذه الجَرِيمة مدبرة من قبل الحكام أو فئات اجتماعية سائدة ولها تمثيل في السلطة، أو مرتبطة بالسلطة ضد فئات اجتماعية معينة عرية كَانَتْ أم دينية أم ثقافية مقهورة، وتستمد هذه الجَرِيمة صفتها الدولة أما من كون مرتكبها صاحب سلطة فعلية قائمة أو يرتبط بالسلطة الفعلية القائمة، أو لتَحْقِيق مصلحة دوْلِيَّة متمثلة في وجوب حماية الانسان بذاته، بصرف النظر عن جنسيته أو دينه أو العنصر الذي ينتسب اليه[23].

ثانيا: الجَرَائم ضد الانسانية

إنَّ الجَرَائِم ضد الإنسانية تعْد من الجَرَائِم حديثة العهد، فلم يظهر اهتمام المجتمع الدولي بها إلّا في وقت قريب أيّ: بعد الحَرْب العالمية الثانية 1939-1945م وعلى الرغم من ظهور بشاعتها في الحَرْب العالمية الأولى إلّا أنَّ الخطوات الجدية التي بدأت بالحديث عنها وتوثيقها لم يأتِ إلّا بعد معاناة ، ونتيجة للفظائع التي ارتكبت بحق اليهود والغجر من قبل النازيين، وراح ضحيتها ما يقارب الأربع ملايين يهودي من أصل ستة ملايين في ألمانيا، فقد استخدمت طرق خاصة لإبادتهم، وبناءً على ذلك ظَهَرَتْ المناشدات بتوفير الحماية الجِنائِيَّة الدوْلِيَّة للإنسان واحترام حقوقه وحرياته ، وكيفية ممارستها بالطرق التي يراها تتوافق ومعتقداته، فانطلقت العديد من المواثيق الدوْلِيَّة التي تحمي هذه الحقوق وتعاقب من يقمعها وملاحقته ومحاسبته على ما ارتكبه، وعليه ومن ذلك انبثق القَانُون الجنائي الدولي بمصطلح "الجَرَائِم ضد الإنسانية".

تتركز الجهود المبذولة من قبل فُقَهَاء القَانُون أو من المختصين في مجال حقوق الإنسان نحو وضع تعريف محدد وأكثر شمولية للجَرَائِم ضد الإنسانية، إلّا أنّه ما زالت كل التعريفات والتوضيحات يشوبها الغموض، وحتى عند البحث في النِظَام الأساسي للمَحْكَمَة الجنائي الدوْلِيَّة "رُومَا"، الذي يعدّ من أهم ما توصلت إليه الجهود الدوْلِيَّة الحديثة من نتاج تشريعي دولي يقتص من "الجَرَائِم ضد الإنسانية" باعتبارها جَرَائِم خطرة ودوْلِيَّة، إذ لم يحدد هذا النِظَام في فقراته الجَرَائِم ضد الإنسانية على سبيل الحصر ومن الفقرة "1/ك" من المادة السابعة ، التي جعلت من هذه المادة ما يؤكد عدم حصر هذه الجَرَائِم بشكل دقيق وحاسم[24].

إذ نجد أنَّ الجَرَائِم ضد الإنسانية قد أخذت الحيز الأكبر من اهتمام الدول بعد الحَرْب العالمية الثانية، فقد ظهر هذا الأهتمام بوساطة إصدار كثير من الإعلانات التي جاء بها الحلفاء أثناء الحَرْب ، وكذلك صدور المواثيق الدوْلِيَّة التي أدانت الأفعال اللاإنسانية وجرمتها ، وكَانَتْ أولى هذه البوادر قد أنتجت مَحْكَمَة نورمبورغ العسكرية وعدد من المواثيق الدوْلِيَّة.

ثالثا: جَرَائِم الحَرْب

عدَّت بعض الدول انتهاكات معينة لبعض قوانين الحرب جرائماً، مع الحَرْب العالمية الأولى، ومعظمها قُنِّنَ في اتفاقيات لاهاي عام 1899م، وعام 1907م، وذهب مِيثَاق مَحْكَمَة (نورمبرغ) العسكرية الدوْلِيَّة عام 1945م إلى تعريف (جَرَائِم الحَرْب) بأنَّها: "انتهاكات لأعراف الحرب وقوانينها، بما فيه من قتل للمدنيين في الأرض المحتلة، أو الإساءة لهم عند معاملتهم، أو إبعادهم؛ وقتل أسرى حَرْب، وقتل الرهائن، سلب الملكية الخاصة، والتدمير العسكري الغير ضروري[25].

إنَّ اتفاقيات جنيف لعام 1949م، كانت قد قننت القَانُون الدولي الإنساني، عقب الحَرْب العالمية الثانية، وذلك كعلامةً على أولِ تضمينٍ لطقمٍ من الجَرَائِم الحربية - خروقاً قَانُونيةً جسيمةً للاتفاقيات- في معاهدة إنسانية قانونيَّة، وتشتمل الاتفاقيات الأربع لجينيف: "حول جرحى الحَرْب البرية ومرضاها، وجرحى الحَرْب البحرية ومرضاها، والمدنيين، وأسرى الحرب"، على قائمتها التي تخص الخروقَ القَانُونيةَ جسيمةَ الأضرار، والقائمة بمجموعها وهي: "قتل العمد، التعذيب، المعاملة الغير إنسانية "، بما فيها التجارب الطبية"[26]؛ والتي تعمد على إيقاع المعاناة الكبيرة، أو الأذى البدني، أو الأذى صحي، وتدمير الملكية والاستيلاء عليها، بصورةٍ لا تبررها الضرورات العسكرية، وبشكل تعسفي وغير شرعي، وكذلك إجبار أسرى الحَرْب أو المدنيين على الخدمة في القوات الخاصة بالدولة الخصم، وتعمد حرمان الأسير أو المدني المحمي من حقه في المحاكمة العادلة في مَحَاكَمَ منظمة تنظيماً قَانُونياً، ونقل أو إبعاد مدني محمي بشكل خارج عن الشرعية، واعتقال المدنيين المحميين بشكل غير شرعي، وكذلك أخذ الرهائن.

قام البروتوكول الإضافي الأول لعام 1977م بحماية اتفاقيات جنيف للنزاعات الدوْلِيَّة، فعُدَّت الانتهاكات التي تلت ذلك خروقاً قَانُونيةً جسيمة: كتجارب طبية محددة؛

مهاجمة المدنيين، المواقع المجردة من وسائل الدفاع وهذا يجعلهم حتماً ضحايا له؛ الاستعمال غير الصادق لشارة الصليب الأحمر، أو الهلال الأحمر؛ القيام بنقل قطاعات من سكان أرضٍ محتلة إلى أرض تحتلها؛ إبطاء إعادة الأسرى إلى أوطانهم دون مبرر؛ الأبارثيد؛ تدمير النصب التاريخية ولبهجوم عليها؛ وحرمان المدنيين المحميين من المحاكمة العادلة. وبحسب اتفاقيات جينيف، والبروتوكول الإضافي الأول، فإنَّ على الدُّول محاكمة الأشخاص الذين أُتهموا بإحداث خروقٍ قَانُونيةٍ جسيمة، أو أن تسلمهم إلى دولة مستعْدة لأن تحاكمهم[27].

إنَّ الأحكام المتعلقة بالخروق القَانُونية الجسيمة، تنطبق على النزاعات الدوْلِيَّة المسلحة، وعلى أي فعلٍ يوجَّهُ ضدَّ الأشخاص المحميين، أو أثناء القيام بعمليات عسكرية. وبشكلٍ عامٍ، فإنَّ الأشخاصَ المحميين هم؛ المرضى والجرحى في البر والبحر من العسكريين، المأسورين في الحَرْب، والمدنيين الذين يقعون تحت قبضة دولة ليسوا من مواطنيها[28].

ولا تعدُّ معظم انتهاكات اتفاقية جينيف، والبروتوكولين الإضافيين، خروقاً قَانُونيةً. ومما لم يدرج كخروق جسيمةٍ ، ما زال الكثير مِنْهَا يندرج تحت جَرَائِم الحَرْب، وبالرغم من أنَّ الدول في هذه الحالات لا تلتزم بالمقاضاة أو التسليم كما تفعل في حالات الخروق القانونية الجسيمة، وهناك خروقاً ليست جسيمة، هي الأخرى لا تقع ضمن جَرَائِم الحَرْب، بل تعدُّ أفعالاً غيرَ قَانُونية، ولا يُسألُ عنها طبقاً للقَانُون الدولي، سوى الدولة المنتهكة. ومثالاً على ذلك: إذا كان قائدُ معسكر لأسرى حَرْب قد اخفق في الاحتفاظ بسجل العقوبات الانضباطية، وهو "انتهاك للمادة (96) لاتفاقية جينيف الثالثة"[29]، فالراجح عدم ارتكابه جَرِيمة حَرْب، بالرغم من أن البعضُ لا يوافق على هذا، ونجد أنَّ التمييز بين الانتهاكات الغير جسيمة، من أجل تقرير أياً مِنْهَا جَرِيمةَ حَرْبٍ، لم يكن علماً مضبوطاً، فإنَّ الانتهاكات الغير جسيمة والأكثر خطراً قد تتعرّض لمسؤولية فردية، في حين "يؤكد الجيش الأمريكي بأنَّ أي انتهاك لقوانين الحَرْب، بما في ذلك انتهاكات اتفاقيات (جينيف)، جميعها جَرَائِم حَرْب"[30].

إنّ للأعمال الوحشية الغير محظورة، والتي يتم ارتكابها أثناء الحَرْب، أن تكون بمقتضى اتفاقيات جينيف، أو البروتوكول الإضافي الأول، جَرَائِم حَرْبٍ، وذلك وفقاً للعنوان الخاص بالقَانُون العرفي التالي: "انتهاكاتُ قوانينَ الحَرْبِ وأعرافَها"، "وهذه الجملة نفسها موجودة في مِيثَاقِ نورمبرغ"، أمَّا نزاعات الدُّول، فإنَّ هذه الدول توافق على أنَّ جَرَائِم الحَرْب هذه تشمل انتهاكاتٍ معينةٍ لتدابيرِ واتفاقية لاهاي للعام 1907م، كاستخدام أسلحة سامَّة، تدمير المدن

تعسفياً دونَ تبرير أو ضرورة عسكرية، الهجوم على الأماكن الغير محمية؛ الهجوم على مؤسسات الثقافة والمؤسسات الدينية؛ سرقة الممتلكات الخاصة والعامَّة، ولا يقوم نِظَام المَحْكَمَة للجنايات الدوْلِيَّة الأساسي بإدراج الخروق الجسيمة في اتفاقيات (جنيف)، كجَرَائِم حَرْبٍ في نزاعات دوْلِيَّة، إضافة إلى ستة وثلاثين انتهاكاً خطيراً آخر لأعرافِ وقوانينِ الحَرْبِ، بالرغم من أنَّ الدول تعدُّ هذه الانتهاكات جَرَائِمَ، على الأقل مذ بدء الحَرْب العالمية الثانية.

أما الحروب الأهلية؛ فلا نجد في القَانُون الدولي، إلا بضع قواعد لتنظيم سلوك النِّزاعات الداخلية، والتي الكثير من الدول تجعلها جزءاً من التشريع المحلي الخاص بها، ولذا فإنَّ قائمة جَرَائِم الحَرْب تكون فيها قصيرة؛ فالبروتوكول الإضافي الثاني لعام 1977م، والذي ينطوي على القواعد الأساس لسلوك النزاعات الداخلية، لا نجد فيه أحكاماً عن المسؤولية الجِنائِيَّة، وإنَّ مدى الجَرَائِم الحَرْب في القَانُون العرفي ليست واضحة بالنسبة لتلك الحروب، كما بالحروب الدوْلِيَّة. ويتضمن النِظَام الأساس الخاص بمَحْكَمَة الجنايات الدوْلِيَّة في يوغسلافيا السابقة؛ "انتهاكات خطيرة للمادة الثالثة، المشتركة في اتفاقيات (جينيف)، وهي المادة الوحيدة في هذه الاتفاقيات التي تناولت الحروب الأهلية"، وقواعد أخرى من أجل توفير الحماية لضحايا النزاع المسلح، والقواعد الأساسية حول الحَرْب والوسائل الخاصة بها، لقد قامتْ المَحْكَمَة بتعريف الانتهاك الخطير بأنَّه: (ذلك الانتهاك الذي تكون نتائجه جسيمة على ضحاياه، ويقوم بخرق قاعدةٍ تحمي مجموعة من القيمِ المهمة). ومن المفترض أن يشمل هذا التعريف الاعتداء الذي يقع على الصحة والحياة، مثل: " سوء المعاملة، العقوبة الجسمية والبدنية، التعذيب، البغاء قسراً، التَّشويه، الاغتصاب، الاعتداء المخل بالشرف، القتل، الإعدام فوراً، احتجاز الرَّهائن، العقوبات الجماعية، النَّهب والسلب"[31]. وبالرغم من أنَّ هذه القائمة هي الأقصر بين قوائم الخروق الجسيمة، أو جَرَائِم الحَرْب الدوْلِيَّة؛ إلا إنَّنا نجدها قد غطت أكثر الأفعال رعباً، والتي قد تحدث ويتم ارتكابها في النزاعات الراهنة.

إنَّ النِظَام الأساسي لمَحْكَمَة الجنايات الدوْلِيَّة، الخاصة براوندا، يجعل جَرَائِم الحَرْب تلك الانتهاكات الخطيرة للمادة الثالثة المشتركة، ومثلها الانتهاكات الخطيرة التي تخص البروتوكول الإضافي الثاني، ويجعل هذا النِّظَام الأساسي أربعة انتهاكات خطرة، للمادة الثالثة المشتركة، والتي يجري ارتكابها في النزاعات الداخلية، ضمنَ جَرَائِم الحَرْب، وهذه الانتهاكات الأربعة هي: "الاعتداء على السلامة البدنية للأشخاص والحياة، الاعتداء على كرامة الشخص، الإعدام

الفوري الذي يتم دون محاكمة، أخذ الرهائن"، ومثلها انتهاكات لأعرافِ وقوانينِ الحرب وتمثل باثني عشر انتهاكاً خطيراً، مثل: " النَّهب، التَّشويه، القيام بهجمات على المدنيين، الاغتصاب"[32].

فالحَرْب اذن ظاهرة اجتماعية وإنسانية ظَهَرَتْ مع بدء ظهور الخليقة على وجه هذه المعمورة، فمنذ ان بدأت الحياة والحَرْب سجال بين البشر، حتى أضحت سمة من أبرز سمات التاريخ الإنساني، والحَرْب هي: (فعل "أو الامتناع عن فعل"، يصدر عن أشخاص أو شخصٍ طبيعيٍّ، عسكريّ أو مدني سواء، وينتمي إلى أحد أطراف الصراع، ضدّ أشخاصٍ أو ممتلكاتٍ لأفرادِ العدوِّ، عَامَّة كانت أم خاصّة، يحدث في نزاع مسلّحٍ أو حرب، وأن تشكل هذه الأفعال انتهاكاً لأعراف الحَرْب، وقوانينها، التي ذكرت في اتفاقيات لاهاي، عام 1899م، و1907م، واتفاقيات جنيف 1949م، فضلاً عن البروتوكول الإضافي الأول والثاني، اللذان ألحقا بها عام 1977م، وكل ما استحدث من الاتفاقيات والمعاهدات والأعراف الدوْلِيَّة في هذا الجانب[33].

اقتصرت النظرة التقليدية على مفهوم جَرَائِم الحَرْب، بأنَّها الجَرَائِم التي يتم ارتكابها في صراعات دوْلِيَّة مسلحة، أو كَانَتْ تقصرها - بتعبير أكثر دقَّة - على "الانتهاكات الخطرة"، لاتفاقيات جنيف الأربع، والمعقودة عام 1949م، والبروتوكول الإضافي الأول، والذي تم إلحاقه بها عام 1977م[34].

ولكن التطورات الأخيرة وسعت مفهوم الجريمة هذا، حتى أصبح شاملاً الانتهاكات الخطيرة لقوانين الحَرْب وأعرافها، فيما يرتكب مِنْهَا في صراعات دوْلِيَّة مسلحة، أو صراعات داخلية مسلحةٍ على حدٍ سواء، وكما تشتمل على "الانتهاكات الجسيمة"، للبروتوكول الإضافي الأول، واتفاقيات (جينيف)، ومثال هذه الانتهاكات: (القتل المتعمد، التعذيب والمعاملة الغير إنسانية، بما فيها (التجارب البيولوجية) ؛ وتعمد على أن تحدثَ معاناةً كبيرةً، أو أذىً بالغاً بالصحة، أو الاستيلاء على الممتلكات وتدميرها، دونَ الحاجة الضرورية والعسكرية لذلك، وإحداث ذلك عمداً ودون حق، وإجبار أسرى الحَرْب أو غيرهم من يتمتع بالحماية منهم على الخدمة في قوات الدولة المعادية، حرمان أسير الحَرْب أو الشخص المحمي من حقه في المحاكمة العادلة، احتجاز الرهائن، جعل أي فرد من السكان المدنيين هدفاً للاعتداء، شن الهجومات دونَ تمييز، مع وجود العلم والوعي بأنه سوف يؤدي إلى خسائر في الأرواح أكثر

مما ينبغي، أو إصابة بالمدنيين، أو الإضرار بالأهداف المدنية، وقيام سلطات الاحتلال بنقل السكان المدنيين إلى ما تحتله من إقليم ، أو نقل سكان الإقليم المحتل (جميعهم أو بعضهم)، إلى أمكنة أخرى داخل أو خارج ذلك الإقليم. وقام النِظَام الأساس للمَحْكَمَة الجِنائِيَّة الدوْلِيَّة بضمّ عددٍ كبيرٍ من جَرَائِم الحَرْب، والتي يتم ارتكابها في الصراعات المسلحة الدوْلِيَّة، وهي لا تعدُّ "انتهاكات جسيمة"[35].

جميع الفُقَهَاء في القَانُون الدولي يتفقون على أن جَرَائِم الحَرْب، هي الجَرَائِم العمدية، والتي يتطلب رُكْنها المعنوي ضرورة أن يتوفر القصد الجنائي، "العلم مع الإرادة"، أي القائم بالفعل يعلم بحرمة ما سيقوم به من فعل، على أن يتم فعل جريمة الحرب من قبل دول متحاربة، "على سبيل المثال من أحد مواطنيها"، فيقوم به برضاه وباسم الدولة، ويكونُ ضدَّ دولةٍ معادية لها، أي مفهوم المخالفة أنَّ الجريمة إذا وقعت من مواطن ضدَّ مواطنٍ آخر فليس فيها أي دوليَّة.

رابعا: جَرِيمَة العُدْوَان

إنَّ من أخطر الجَرَائِم الدوْلِيَّة، وأكثرها فداحةً وضرراً على الإطلاق، هي جريمة العدوان، لأنّها الجَرِيمة الدوْلِيَّة الكبرى التي يمكن أن يُرتكب خلالها، وفي أثنائها، جرائم عدَّة، وتندرج تحت الجَرَائِم الدوْلِيَّة الكبرى، كالجَرَائِم التي تقع ضدَّ الانسانية، وجرائم الإبادة الجماعية[36]، وقد جاء تعرّيف الْجَمْعِيَّة الْعَامَّة للأمم المتحدة لمفهوم (العُدْوَان)، في خلال دورتها (29) في عام 1974م، بأنه: استخدامُ قوة مسلحة، من قبل دولة ضد دولة أخرى، أو ضدَّ سلامة إقليمها، أو ضدَّ استقلالها السياسي، أو بأي شكلٍ آخرَ يكون متنافياً مع مِيثَاق الأمم المتحدة، وذلك وفقاً لنص التعريف هذا، وقد عدَّت الحرب العُدْوَانية جَرِيمة ضد سلم الدُّول، والعُدْوَان يرتب المسؤولية الدوْلِيَّة وليس القَانُونية، ولا يمكن أن يُعدّ أيَّ كسبٍ إقليمي كذلك، كما لا يعدُّ أيَّ مغنمٍ خاصٍ ناتجٍ عن ارتكاب (العُدْوَان)،[37] وبالرغم من كل ذلك فإننا نلاحظ عدم تفعيل ما تختص به المحكمة الجنائية الدّولية للنظر بهذه الجريمة، ويأتي ذلك لعدم تبني أو الاتفاق على تبني أيَّ تعريف خاص بالمسؤولية عن ارتكابها. وقد كان إدراج هذه الجَرِيمة ضمن قائمة الجَرَائِم التي تدخل في اختصاص المَحْكَمَة محل جدل بين مؤيد ومعارض.

وكان جانب من الجدل يدور حول التوصل إلى تعريف لجَرِيمة العُدْوَان. وقام الرأي القائل بإدراج هذه الجَرِيمة على أساس الجسامة القصوى لهذه الجَرِيمة والآثار الدوْلِيَّة الفادحة المترتبة عليها، بينما قام الرأي المعارض على أساس عدم التوصل إلى تعريف دقيق لهذه الجَرِيمة. ومن ناحية أخرى فقد امتد النقاش إلى دور مجلس الأمن في هذا الشأن. بيان ذلك أن المادة "39" من مِيثَاق الأمم المتحدة تنص على أن مجلس الأمن يختص بتقرير قيام حالة العُدْوَان بما مفاده أن تحديد قيام هذه الحالة يتصل مباشرة بدور مجلس الأمن في الحفاظ على السلم والأمن الدوليين. وقد كان من بالغ الدقة الوصول إلى حل متوازن يحفظ لمجلس الأمن اختصاصه المقرر بمقتضى مِيثَاق الأمم المتحدة، في الوقت ذاته الذي يحافظ فيه ويضمن الاستقلال القضائي الواجب تقريره للمَحْكَمَة[38].

وقد يكون من الملائم الإشارة إلى أن مَحْكَمَة نورمبرج أدانت الحروب العُدْوَانية بأبلغ وأقسى التعبيرات، حيث انتهت إلى أن شن الحَرْب العُدْوَانية ليس وحسب جَرِيمة دوْلِيَّة، بل هو أكثر الجَرَائِم الدوْلِيَّة فحشًا؛ حيث إن هذه الجَرِيمة تتضمن في ذاتها كافة الشرور الناتجة عن جَرَائِم الحَرْب الأخرى وما يرتبط بها.

وعلى ذلك نرى بان جَرِيمة (العُدْوَان)، تتلخص في فعل عدائي، يتمثل باستخدام السلاح والقوة المفرطة، تنفيذاً لأمر صدر عن القادة البارزين، أو عن حاكم الدّولة، ضدَّ دولة أخرى، فهو أي إنَّه يتمثل بالأمر الصادر عن شخص مسؤول، سواءً كان حاكماً، أو قيادياً بالقيام بفعل عدواني ضدَّ دولة ثانية، فالفعل العدائي أو العُدْوَاني، لا يكمن أن يقع الا باستعمال قوة مسلحة وعلى هيئة هجوم لا دفاع؛ لأنَّ الدفاع يعدُّ أمراً مَشْرُوعاً في منع عدوان من جهة ما، ويمنع الدولة من المساءلة، فهو "دفاع شرعي" ، أما الهجوم فإنَّه عُدْوَان ونشاطٌ يقع ضد دولة ما، وكما يتوفر فيه (القصد الجنائي)، وهو "العلم ، الإرادة"، أي: علم الفاعل بجرم هذا الفعل، وتوجيه إرادته لارتكابه حتى بعد العلم بجرمه، وبالتالي فإنَّ علمَ الجاني بعدم مَشْرُوعية هذا العُدْوَان، ثمَّ يقوم به يجعله معرضاً للمساءلة القَانُونية، فينبغي أن يقع العُدْوَان باسم الدولة، أو بناءً على طلبها، وخطتها، ورضاها عن ما سيقع من عُدْوَان ضد الدولة الأخرى، مثال على ذلك: إذا قام طيارٌ عسكريٌ بفعلٍ فرديٍ، كشنّ غارة جوية، ضدَّ دولةٍ مجاورةٍ، دون أن يصدر بتلك الغارة أي أمر، وإنّما كانت من وليد إرادته فإنّها لا تشكل

جَرِيمة عُدْوَان، لأنَّ هذا الفعل تم دونَ أمرٍ صادرٍ من حاكمٍ، أو قياديٍّ، أو مسؤولٍ في الدّولة، وبمعنى أكثر دقة فعل الغارة هذا ما تَّم باسم الدولة، ولا بناء على خطة لها.

المحور الثاني الأساس القَانُوني لمجلس الامن والمَحْكَمَة الجِنائِيَّة الدوْلِيَّة

نقول إن المَحْكَمَة الجِنائِيَّة الدوْلِيَّة رغم ما يعاب عليها تبقى إنجاز للإنسانية ينبغي انتقاده، بغية الدفع به ليتجاوز مكامن الخلل ومنع الافلات من العقاب. ويبدو أن من أهم الأعطاب التي ولد بها نِظَام رُومَا، هو ربطها في ممارسة الاختصاص بجهاز سياسي وهو مجلس الأمن.

فالقاعدة القَانُونية كما خبرنا من أهم مميزاتها كونها عامة تسري على الجميع بدون تمييز بين القوي عن الضعيف، بينما في السياسة هناك قوي وضعيف، ومنطق القوة هو المحرك وخصوصاً إذا تعلق الأمر بالعلاقات بين الدول. يمكن القول كما بينا سابقا وسنبين لاحقا أن مجلس الأمن يكيل بمكاييل مختلفة في الأزمات والصراعات الدوْلِيَّة و غير الدوْلِيَّة، وفي علاقاته بالمَحْكَمَة الجِنائِيَّة الدوْلِيَّة نثير الفقرة "ب" من المادة 13 مجموعة من التساؤلات، خصوصا عندما ربطت بين ممارستها للاختصاص بموجب إحالة من مجلس الأمن متصرفاً بموجب الفصل السابع من مِيثَاق الأمم المتحدة، وأطلقت يده في ذلك مقابل تقييد تحريك الدعوى بالنسبة للدول الأطراف والمدعي العام للمَحْكَمَة.

وكذلك المادة 16 من النِظَام الأساسي التي تنص على أنّه " لا يمكن القيام بأي بحث أو متابعة منصوص عليها بالنِظَام طيلة الإثني عشر شهرا الموالية لتاريخ توجيه مجلس الأمن طلبا في هذا الاتجاه إلى المَحْكَمَة، بمقتضى قَرَار مؤسس على الفصل السابع من مِيثَاق الأمم المتحدة. ويمكن تجديد الطلب من طرف المجلس طبقا لنفس الشروط.

اولاً: نطاق سلطة الأمن من حيث الجرائم الدولية

إنَّ الإحالة التي قررها مجلس الأمن لم تكن مقتصرة على ارتكاب جَرِيمة العُدْوَان، بل اشتملت على الجَرَائِم الأخرى التي وردت في النِظَام الأساسي للمَحْكَمَة الجِنائِيَّة الدوْلِيَّة، وتمتلك المَحْكَمَة الجِنائِيَّة اختصاصاً للنظر فيها، ومنها: جَرائِم الإبادة الجماعية، وجَرَائِم الحَرْب، الجرائم الواقعة ضد الانسانية، وقام النِظَام الأساسي للمَحْكَمَة ببيان المقصود بالجَرَائِم الثلاث الأولى من النص ، إلاّ أنه أجّل اختصاص المَحْكَمَة في النظر في الجَرِيمة الرابعة " جَرِيمة العُدْوَان " ، بحجة

الإتفاق على تعريفها ، و ذلك من خلال نص الفقرة "2" من المادة "5" من النِظَام الأساسي للمَحْكَمَة على "تمارس المَحْكَمَة الاختصاص على جَرِيمة العُدْوَان متى اعتمد حكم بهذا الشأن وفقاً للمادتين "121، 123" يعرف جَرِيمة العُدْوَان ويضع الشروط التي بموجبها تمارس المَحْكَمَة اختصاصها فيما يتعلق بهذه الجَرِيمة"، وأيضا حول تحديد دور مجلس الأمن في تحديد وقوع العُدْوَان.

بالنسبة للحجة الأولى فإنه منذ قيام الامم المتحدة ومحاولات وضع تعريف للعُدْوَان قائمة ، لكون المِيثَاق جاء خالياً من تعريف له، وفي عام 1953 قدم الاتحاد السوفيتي الى الْجَمْعِيَّة الْعَامَّة مَشْرُوعاً لتعريف العُدْوَان وفي عام 1968 اصدرت الْجَمْعِيَّة الْعَامَّة التوصية رقم 22 / 2330 الخاص بتشكيل لجنة من 35 عضواً لدارسة مسألة تعريف العُدْوَان وقدمت اللجنة ثلاثة مشاريع في هذا الخصوص.

وفي عام 1974 أصدرت الْجَمْعِيَّة الْعَامَّة التوصية الشهيرة 3314 الخاصة بتعريف العُدْوَان والتي جاء في المادة الاولى مِنْهَا :العُدْوَان هو استخدام القوة المسلحة من قبل دولة ما ضد دولة اخرى أو سلامتها الاقليمية أو استقلالها السياسي او باية صورة اخرى تتنافى مع مِيثَاق الامم المتحدة وفقاً لنص هذا التعريف[39].

ولم تكتفي التوصية بتعريف العُدْوَان وإنما حددت افعالا تكيف على أنها أفعال عُدْوَانية، حيث نصت المادة "7" من التعريف على تكييف الافعال الآتية بانها عُدْوَانية: أ: غزو أو مهاجمة أراض دول ما عن طريق القوات المسلحة لدولة اخرى أو احتلال عسكري مهما يكن مؤقتا، ناجم عن مثل هذا الغزو او المهاجمة أو أي ضرر باستخدام القوة، لأراض دولة أخرى أو جزء مِنْهَا .ب: قصف أراضي دولة أخرى عن طريق القوات المسلحة لدولة ما او استخدام اية اسلحة من جانب دولة ما ضد اراضي دول اخرى. ج :.حصار موانئ او سواحل دولة ما عن طريق القوات المسلحة لدولة اخرى .د : اي هجوم تقوم به القوات المسلحة لدولة ما على القوات البرية او البحرية او الجوية او على الاساطيل البحرية او الجوية لدولة اخرى . ه : استخدام القوات المسلحة لدولة ما الموجودة داخل اراضي دولة اخرى بموافقة الدولة المستقبلة ، على نحو يناقض الشروط المنصوص عليها في الاتفاق او اي مد لوجودها الى ما بعد انتهاء الاتفاق.

ويمكن القول أن جَرِيمة العُدْوَان مهما اختلف حول تعريفها تعْد المدخل الأساسي لباقي الجَرَائِم التي تدخل في اختصاص المحْكَمَة، وأنها ذات علاقة وطيدة بالسياسة بل إنها تمثل امتداداً لها. وتجدر الإشارة إلى أن المحْكَمَة في موقعها الرسمي أدرجت تعريفاً غير رسمي لجَرِيمة العُدْوَان وذلك في الوثيقة .ICC-ASP/8/INF :المؤرخة في 2009/07/10 وللأسف لم يتم تبنيها في مؤتمر مراجعة مِيثَاق رُومَا الذي انعقد في كامبالا عاصمة أوغندا ماي 2010 وكَانَتْ آمال كثيرة منعقدة عليه[40].

أما الحجة الثانية التي أدت إلى تأجيل اختصاص المحْكَمَة بخصوص جَرِيمة العُدْوَان فقد كان الخلاف بين الدول حول تحديد دور مجلس الأمن في تحديد وقوع العُدْوَان، فهل أن مباشرة المحْكَمَة لاختصاصها بنظر جَرِيمة العُدْوَان يتوقف على قَرَار مسبق صادر عن مجلس الأمن الدولي يثبت فيه وقوع العُدْوَان أم أن المحْكَمَة تتمتع بسلطة تقرير ارتكاب العُدْوَان من عدمه دون أن يتوقف اختصاصها بنظر هذه الجَرِيمة على ما يقرره مجلس الأمن الدولي؟

انقسمت الدول في مؤتمر رُومَا إلى قسمين ،الأول يعارض منح المجلس بسلطة تحديد وقوع العُدْوَان والثاني يؤيد ذلك، أما الدول المعارضة فقد أكدت ضرورة الحفاظ على استقلالية المحْكَمَة في مواجهة مجلس الأمن وتحذر من إخضاعه لسلطة المجلس لاسيما إن الواقع الدولي قد اثبت فشل المجلس ذاته وفي مناسبات عديدة في التعامل مع جَرِيمة العُدْوَان أو تأكيد ارتكابها برغم وقوعها فعلا، ولذلك فان إنشاء مَحْكَمَة دوْلِيَّة جِنائِيَّة فعالة ينبغي أن يتم بصورة تجعلها مستقلة بعيدة عن الخضوع لتأثيرات مجلس الأمن وتوجهاته السياسية بصدد جَرِيمة العُدْوَان، إما الدول المؤيدة لهذه السلطة وهي الدول الدائمة العضوية وبمساندة من إسرائيل فهي ترى إن منح المحْكَمَة سلطة تحديد وقوع العُدْوَان ومباشرة اختصاصها بمعزل عما يقرره مجلس الأمن بهذا الصدد هو انتقاص لحقوقها وسلب لامتيازاتها ولذلك فهي ما تزال تعارض منح المحْكَمَة مثل هذه الصلاحية وتصر بالتالي على أن يظل مجلس الأمن هو جهة الإحالة الوحيدة لمباشرة المحْكَمَة اختصاصها بنظر جَرِيمة العُدْوَان[41].

ومن ناحية أخرى، فإن موضوع الإحالة يجب أن يكون من أكثر الجَرَائِم التي ذكرناها سالفا. وعليه، لا يسمح لمجلس الأمن بإحالة – مثلاً – أي حالة تتعلق بجَرَائِم الإرهاب، أو الاتجار غير المَشْرُوع في المخدرات، أو الهجرة غير الشرعية، أو غسل الأموال، أو الاتجار في النساء والأطفال، أو الاتجار في السلاح، أو مخالفة الحظر الدولي، المفروض بواسطة مجلس

الأمن على توريد السلاح إلى بلد معين، ولم يرد لهذه الجرائم نصاً في النِظَام الأساسي للمَحْكَمَة الجِنائِيَّة الدوْلِيَّة، وبالتالي فإنَّها لم تكن موضوعاً للإحالة التي صدرت عن مجلس الأمن إلى المدعي العام للمحكمة[42].

وهنا تجدر الإشارة إلى أن الوفد الهندي أصر على أن تضاف إلى الجَرَائِم التي تختص بها المَحْكَمَة تجريم استخدام الأسلحة النووية، وفي حين اتفقت معها معظم الدول النامية، عارضتها الولايات المتحدة بشدة[43].

1. سلطة المجلس ونطاقها من حيث الزمان

إنَّ اختصاص المحكمة بالجرائم يتعلق بما يرتكب بعد نفاذ نظامها الأساسي، وذلك تبعاً للمادة (11)، من النِظَام الأساسي للمَحْكَمَة الجِنائِيَّة الدوْلِيَّة، ومن الجدير بالذكر أنَّ هذا النظام دخل حيز النفاذ في الأول من يوليو عام 2002[44].

ولذا، فإن المَحْكَمَة يحسر اختصاصها على ما يرتكب من جرائم في الوقت اللاحق لهذا التاريخ، وتختص الدول التي صدقت على النِظَام الأساسي قبل البدء بنفاذه بهذا الحكم، فلو كانت دولة ما قد أصبحت طرفاً بعد بدء نفاذ هذا النِظَام، فلا يجوز للمَحْكَمَة بممارسة اختصاصها إلا على بالجَرَائِم التي يجري ارتكابها بعد البدء بنفاذ النِظَام بالنسبة لهذه الدولة، إلا إذا كانت هذه الدولة قد أقرت في تاريخ يسبق انضمامها اختصاص المحكمة.

وبالتطبيق العملي، نلاحظ قَرَار مجلسِ الأمنِ المرقم 1593 للعام 2005، الخاص بدارفور قد قرر صراحة – في بنده الأول – «إلى إحالة وضع دارفور القائم منذ 1 يوليوز 2002، إلى المدعي العام، إلى المَحْكَمَة الجِنائِيَّة الدوْلِيَّة»، وهذا يدل على أنَّ مجلس الأمن قام بقصر الإحالات على الوقائع التي تلحق تاريخ بدء نفاذ النِظَام، وهو تاريخ الأول من يوليو عام 2002م[45].

غير أن مسألة اختصاص المَحْكَمَة من الناحية الزمنية تثير إشكالية خصوصاً أنه قيل في تبريرها انها تطبيق للقاعدة الْعَامَّة النافذة في جميع الأنظمة القَانُونية الرئيسة في العالم، التي تقضي بعدم جواز تطبيق القوانين الجِنائِيَّة بأثر رجعي، وبالتالي فهي نتيجة طبيعية ولازمة لمبدأ شرعية الجَرَائِم والعقوبات"لاجَرِيمة ولا عقاب بدون نص"، إلا أن سريان نِظَام رُومَا الأساسي على الجَرَائِم التي وقعت قبل نفاذه لا يعتبر إخلالا بهذا المبدأ فكما هو معروف إن الغرض من "عدم الأثر الرجعي" هو عدم تطبيق نص التجريم على فعل كان غير مجرم، والأمر هنا يختلف

فالنِظَام الأساسي للمَحْكَمَة الدوْلِيَّة لم يأتي بجَرَائِم جديدة بل إن هذه الجَرَائِم معروفة ومقررة بموجب معاهدات في القَانُون الدولي، وبالتالي لم تجرم المَحْكَمَة فعلا كان مباحا في الفترة التي سبقت إنشاءها أضف إلى ذلك أن العالم وخاصة ضحايا هذه الجَرَائِم كانوا قد انتظروا لفترة طويلة وعقدوا اماالاً كبيرة لإنشاء هذه المَحْكَمَة لغرض أنصافهم من مرتكبي هذه الجَرَائِم، وكذلك يعتبر هذا النص تعطيلا لمبدأ أساسي من مَبَادِئ القَانُون الدولي الجنائي وهو مبدأ عدم تقادم الجَرَائِم الدوْلِيَّة الخطيرة التي تمس بالقيم العليا للمجتمع الدولي[46].

أجمع الباحثون على تمتع مجلس الأمن بسلطته للإحالات، أياً كانت جنسية الجاني وبأي مكان تم تنفيذ الجَرِيمة فيه، سواء تم الارتكاب في إقليم دولة طرف، أو من مواطني هذه الدولة، أو تم ارتكابها في إقليم دولة ليست طرفاً. وعلى هذا فإنَّ اختصاص المكان للمَحْكَمَة الجِنائِيَّة الدوْلِيَّة يمتد إلى أقاليم دول ليست أطرافاً في النِظَام الأساسي للمحكمة، دون النظر إلى قبول هذه الدول اختصاص المَحْكَمَة أم لا، وقد تم التأكد من ذلك خلال التطبيق العملي، فقد قام مجلس الأمن الدولي بإحالة القضية السودانية الخاصة بـ «دارفور»، إلى الادعاء العام للمَحْكَمَة الجِنائِيَّة الدوْلِيَّة، بالرغم من أن السودان لم تكن دولةً طرفاً في النِظَام الأساسي للمَحْكَمَة الجِنائِيَّة الدوْلِيَّة[47].

تختلف السلطة المخولة في النِظَام الأساسي للمَحْكَمَة بين مجلس الأمن وبين الدول الأطراف ، فهي تقتصر على الجَرَائِم التي يتم ارتكابها في إقليم دولة طرفٍ، عندما يحيل مجلس الأمن هذه القضية، أو الحالة إلى المدعي العام للمَحْكَمَة الجِنائِيَّة الدوْلِيَّة، للتصرف وفق الفصل السابع، فلا تتقيد المحكمة بالشروط المنصوص عليها في مادتها الثانية عشرة من النِظَام الأساسي، وهي: (وقوع الجَرِيمة في إقليم خاصٍ بدولةٍ طرفٍ أو عن طريق أحد مواطنيها)[48].

ونستخلص الحكم هذا، "بمفهوم المخالفة" من البند الثاني لنظام المحكمة للمادة "12"، وجاء في نصه «في حالة فقرة (أ)، أو (ج) المادة "13"، "بإمكان المَحْكَمَة ممارسة اختصاصها في حال كون واحدة أو أكثر من الدول التي تلت طرفاً في النِظَام الأساسي، أو أنَّها قابلة باختصاص المَحْكَمَة، وفقاً للفقرة 3"، ويحدد النص هذا اختصاص المحكمة المكاني، بقصر المَحْكَمَة في ممارستها لاختصاصها على ما تمَّ ارتكابه من جَرَائِم في إقليم دولة طرف في النِظَام، أو لدولة قبلت على الأقل من أن تمارس المَحْكَمَة اختصاصها بما يتعلق بالجَرِائم قيد البحث، في حال

كون هذه الإحالة إلى المَحْكَمَة تمت من دولة طرف، أو أنَّ المدعي العام كان قد بدأ بالتَحْقِيق من تلقاء نفسه.

وهذا يعني، بأنَّ هاتين الحالتين يتوقف فيهما اختصاص المحكمة على مكان الجَرِيمة، أي ارتكابها في إقليم دولة طرف في النِظَام الأساسي، أو في إقليم دولة توافق على أن تمارس المَحْكَمَة اختصاصها بشأن الجَرِيمة التي لا يزال بحثها قائماً. ولم يتم بيان الحكم عند الإحالة من مجلس الأمن، وفقاً للبند (ب) من المادة "13"، وهو الأمر المعني بمفهوم المخالفة، بممارسة المَحْكَمَة لاختصاصها في هذا الفرض، سواء أكَانَتْ هذه الجَرِيمة قد ارتكبت في إقليم الدولة الطرف في النِظَام، أو من أحد مواطنيها، أو أنّها جرى ارتكابها في إقليم دولة ليست طرفاً.

ونثير مسألة الاختصاص المكاني للمَحْكَمَة الجِنائِيَّة الدوْلِيَّة تناقضا خطيرا في القَانُون الدولي العام، ذلك انها تتناقض من حيث التطبيق مع معاهدة فيينا سنة 1969 المتضمنة لقَانُون المعاهدات، فإذا كَانَتْ معاهدة رُومَا تخضع لقَانُون المعاهدات خصوصا وأنها معاهدة عامة أو شارعة من حيث كونها أبرمت بين عدد غير محدود من الدول، والغرض مِنْهَا تسجيل قواعد معينة، فإن المفروض أن لا تلزم إلا الدول التي أبرمتها[49]، وواقع الحال أن المَحْكَمَة تحقق في جَرَائِم ارتكبت في دول ليست أطرافاً فيها مثل ليبيا والسودان.

الخاتمة

بعد أن استعرضنا مفهوم الجريمة والجريمة الدولية، وايضاً دور مجلس الأمن، والمحكمة الجنائية الدولية، نرى بضرورة ملاحقة ومحاكمة مسؤولي تلك الجرائم أمام القانون الدولي، وتقديمهم الى المحكمة الجنائية الدولية، ضمن الولاية القضائية للمحكمة، وهؤلاء المجرمين على الجرام المرتكبة في فلسطين والعراق وبقية العالم، سواءً كان عن تدخل مجلس الأمن أو القضاء بالاختصاص العالمي أمام القضاء العراقي واخيراً، يجب أن تكون وقفة في مواجهة جرائم الاحتلال الأمريكي في العراق وفلسطين، ولكن هذا يواجه برفض أمريكي لاختصاص المحكمة الجنائية الدولية أو حتى لوجودها القانوني، ويعتبر هذا الرفض دليل على عدم اكتراث أمريكا بالمجتمع الدولي، فضلاً عن ذلك ارتكب جنودها أبشع الجرائم واخطرها دولياً، بدءاً بجرائم القتل وجرائم ضد الإنسانية وجريمة العدوان جريمة الإبادة الجماعية وجريمة الحرب، ويجب أن يجري التحقيق فيها ومعاقبة مرتكبيها.

الاستنتاجات

1. قسمت الجرائم الدولية في نظام روما الأساسي حسب المادة (5)، الى (الجرائم ضد الإنسانية، وجريمة العدوان، وجريمة الإبادة الجماعية، وجريمة الحرب)، وبهذا فقد فصل النظام هذه الجرائم، وهي احدى اركان عمل المحكمة الجنائية الدولية، وان المحاكمة تجري على الأشخاص وليس على الدول.
2. إن الأساس القانوني لمجلس الامن الدولي في الفصل السادس والسابع من ميثاق الأمم المتحدة، وان الأساس القانوني للمحكمة الجنائية الدولية هو النظام الأساسي للمحكمة.
3. ان وجود المحكمة الجنائية الدولية علامة ممتازة في بنية مؤسسات المجتمع الدولي، وعامل مهم لوقاية المجتمع الإنساني من الحروب والابادات والنزاعات والاعتداءات، اذ تساهم في استتباب السلم والامن الدوليين، ويتجلى ذلك في ملاحقة ومحاكمة الأشخاص المسؤولين عن جرائم الحرب والجرائم ضد الإنسانية وجرائم الإبادة الجماعية.
4. ان الواقع الدولي ينبئ عن أزمات عديدة في القانون الدولي، وتطرح فكرة مفادها اننا نعيش في عالم يحكمه قانون القوة وليس قوة القانون، في انتظار إعادة تشكيل القانون الدولي يترجمه مجتمع دولي تحكمه توازنات دولية سلمية وسليمة وفاعلة على نحو إيجابي ومرنة.
5. لم يستطيع مجلس الامن الدولي بسبب إساءة استعمال حق النقض (الفيتو)، من معالجة الكثير من حالات النزاع الدولي المسلح، ومن الجرائم التي افتعلتها العديد من الدول، وابرزها ما ذكرناها في هذه الدراسة، ومن مثالها الصارخ هو الجرائم الإسرائيلية في فلسطين والمسكوت عنها، بسبب النقض الأمريكي المستمر لصالح إسرائيل، وكذلك عجز مجلس الامن الدولي الفاضح عن تنفيذ قرارات وقوفه عاجزا إزاء إصرار بعض الأعضاء على عدم الإذعان لقراراته.

التوصيات

1. ضرورة تعديل المادة (13) من النظام الأساسي للمحكمة الجنائية الدولية، بإضافة فقرة لها، تلزم مجلس الامن، بالقيام في الإحالة، بوجود قضايا تهدد

السلم والامن الدوليين، والحد من امتناعه وتأخره بالقيام بالإحالة بعيداً عن حق الفيتو من الدول الكبرى.

2. نقترح تعديل المادة (16) من النظام الأساسي للمحكمة الجنائية الدولية لتحديد فترة ارجاع نشاط المحكمة الى ستة اشهر، غير قابلة للتجديد مع بيان دوافع المجلس الى انتهاك هذا المسار.
3. يجب العمل على تعزيز التعاون الدولي مع المحكمة الجنائية الدولية، وان يستمد قوته من تعاون ذاتي وناشئ نتيجة لمصادقتها على النظام الأساسي وأن حسن نية الدول على التعاون يقاس بإدخال التعديلات على نظمها وقوانينها الوطنية بما ينسجم ودون تعارض مع النظام الأساسي.
4. يجب عدم التنازل أو التراجع عن محاكمة الأشخاص الدوليون الذين ارتكبوا الجرائم بمساعدة الولايات المتحدة الامريكية، وخصوصاً الجرائم التي ارتكبتها إسرائيل في فلسطين، والجرائم التي ارتكبتها القوات الامريكية اثناء احتلال العراق بعد عام 2003.

المصادر والمراجع:

[1] سالم محمد سليمان الاوجلي، أحكام المسؤولية الجِنائِيَّة عن الجَرَائِم الدوْلِيَّة في التشريعات الوطنية، الطبعة الأولى، الدار الجماهيرية للنشر والتوزيع والإعلان، مصراتة، 2000، ص189.

[2] عبد الله سليمان سليمان، المقدمات الأساسية في القَانُون الدولي الجنائي، ديوان المطبوعات الجامعية، الجزائر، 1992، ص174.

[3] حسنين إبراهيم صالح عبيد، الجَرِيمة الدوْلِيَّة، دراسة تحليلية تطبيقية، دار النهضة العربية، القاهرة، 1999، ص199.

[4] فتوح عبد الله الشاذلي، القَانُون الجنائي الدولي، اوليات القَانُون الجنائي الدولي، النظريات الْعَامَّة للجَرِيمة الدوْلِيَّة، دار المطبوعات الجامعية، الإسكندرية، 2002، ص207.

[5] عبد الواحد محمد الفار، الجَرَائِم الدوْلِيَّة وسلطة العقاب عليها، دار النهضة العربية، القاهرة، 1996، ص40.

[6] عدي طلفاح محمد خضر، الجَرِيمة الدوْلِيَّة صورها واركانها، مجلة جامعة تكريت للعلم الإنسانية، العدد 10، المجلد 14، جامعة تكريت، العراق، 2007، ص89.

[7] Lombios, driot penal international, ed dalloz, Paris, 1971, P.35.

[8] Plawski, etudes des principes fondamentaux du driot international penal, L.G.D, Paris, 1972, P.75.

[9] حسنين إبراهيم عبيد، الجَرِيمة الدوْلِيَّة، دار النهضة العربية، القاهرة، 2005، ص89.

[10] سيعيد عبد اللطيف حسن، المَحْكَمَة الجِنائِيَّة الدوْلِيَّة، انشاء المَحْكَمَة، نِظَامها الأساسي، اختصاصها التشريعي القضائي وتطبيقات القضاء الجنائي الدولي الحديث المعاصر، دار النهضة العربية، القاهرة، 2004، ص181.

[11] تنص المادة "5" من نِظَام رما الأساسي على الجَرَائِم التي تدخل في اختصاص المَحْكَمَة كالتالي: "يقتصر اختصاص المَحْكَمَة على أشد الجَرَائِم خطورة موضع اهتمام المجتمع الدولي بأسره، وللمَحْكَمَة بموجب هذا النِظَام الأساسي، اختصاص النظر في الجَرَائِم الآتية: "أ. جَرِيمة الإبادة الجماعية؛ ب. الجَرَائِم ضد الإنسانية؛ ج. جَرَائِم الحَرْب؛ جَرِيمة العُدْوَان.

[12] حسام علي الشيخة، جَرَائِم الحَرْب في البوسنة والهرسك، دار الجامعة الجديدة، الإسكندرية، 2004، ص58.
[13] زياد ربيع، جَرَائِم الإبادة الجماعية، مجلة دراسات دوْلِيَّة، العدد 59، كلية العلوم السياسية، جامعة بغداد، 2015، ص105.
[14] مثال ذلك ما فعله المغول في المسلمين وما خلفته الحروب الصليبية والحَرْبين العالميتين في القرن العشرين.
[15] ليندة معمر يشوي، المَحْكَمَة الجِنائِيَّة الدوْلِيَّة واختصاصاتها، دار الثقافة، عمان، ط1، 2008، ص183.
[16] اعتمدت من قبل جمعية الدول الأطراف في نِظَام رُومَا الأساسي للمَحْكَمَة الجِنائِيَّة الدوْلِيَّة في دورتها الأولى المنعقدة في نيويورك خلال الفترة من 3 الى 10 أيلول/ سبتمبر 2002.
[17] ليندة معمي يشوي، المرجع السابق، ص188.
[18] بلختير بومدين، المَحْكَمَة الجِنائِيَّة الدوْلِيَّة ودورها في حماية حق الحياة بين القَانُون الدولي والشريعة الإسلامية، جامعة ابي بكر بلقايد – تلمسان، كلية العلوم الإنسانية والعلوم الاجتماعية، أطروحة دكتوراه، 2010، الجزائر، ص38.
[19] عبد القادر البقيرات، العدالة الجِنائِيَّة الدوْلِيَّة، ديوان المطبوعات الجامعية، الجزائر، 2005، ص93.
[20] عبد الله سليمان سليمان، المقدمات الأساسية في القَانُون الدولي، ديوان المطبوعات الجامعية، الجزائر، 2003، ص85.
[21] Cherif Bassiouni, project de cod penal international, driot penal 2001, P.129.
[22] هناء إسماعيل، المسؤولية الجِنائِيَّة عن جَرِيمة الإبادة الجماعية، مجلة رسالة الحقوق، العدد 214، العراق، 2014، ص209.
[23] زياد محمد ربيع، جَرِيمة الإبادة الجماعية، بحث منشور في موقع المجلات العلمية العراقية، شبكة المعلومات الدوْلِيَّة "الانترنت"، على الرابط: https://www.iasj.net/
[24] جواد كاظم طراد الصريفي، الجَرَائِم ضد الإنسانية دراسة مقارنة، بحث منشور في مجلة الكلية الإسلامية الجامعة، النجف الأشرف، العدد 50، الجزء 1، ص15،، 2018.
[25] DEMOCRATIC REPUBLIC OF THE CONGO 1993-2003 UN Mapping Report, United Nations, p2.
[26] Memorandum by Hersch Lauterpacht to the Committee on Crimes Against International Public Order entitled “Punishment of War Crimes” 6 "1942", http://diginole.lib.fsu.edu/islandora/
[27] The jurisdiction of the military commissions under the 2009 Military Commissions Act extends to prosecutions “for any offense made punishable by [the Act itself]” as well as offenses under the “law of war.” Military Commissions Act of 2009, Pub. L. No. 111-84, § 948"d", 123 Stat. 2190, 2576 "2009"
[28] Brief of Appellant, United States v. Khadr, No. 07-001 "Ct. of M. Comm’n R. Nov. 8, 2013", https://www.justsecurity.org/wp-content/uploads/2013/11/khadr.cmcr_.brief_.pdf; Dean Bennet, Hearing Seeking to Ease Omar Khadr’s Bail Conditions Cancelled, THE STAR "Aug. 31, 2017", https://www.thestar.com/news/canada/2017/08/31/hearing-seeking-to-ease-omar-khadrs-bail-conditionscancelled.html.
[29] See, e.g., Supplemental Brief in Support of the Government’s Appeal at 13, United States v. Khadr, No. 07-001 "Ct. M. Comm’n R. June 4, 2007" "“Congress sought to establish an enduring process for prosecuting unlawful enemy combatants for war crimes in this and future conflicts.”".
[30] Prosecutor v. Hinga Norman, Case No. SCSL-2004-14-AR729E, Appeals Chamber Decision on Preliminary Motion Based on Lack of Jurisdiction "Child Recruitment" "Special Ct. for Sierra Leone May 31, 2004" [hereinafter Hinga Norman Appeals Chamber Decision]; see discussion infra notes 139-143.

[31] Eve La Haye, a legal advisor of the International Committee of the Red Cross, writes that "individuals could always be held criminally responsible if they breached the laws of war." EVE LA HAYE, WAR RIMES IN INTERNAL ARMED CONFLICTS 105 "2009". Yet, the legal obligations flowed through the States involved in the conflict, not directly to the individual.

[32] Paola Gaeta, War Crimes and Other International 'Core' Crimes, in THE OXFORD HANDBOOK OF INTERNATIONAL LAW IN ARMED CONFLICT 737, 738 "2014" "quoting G. Manner, The Legal Nature and Punishment of Criminal Acts of Violence Contrary to the Laws of War, 37 AM. J. INT'L L. 407 "1943""

[33] احمد عبد الحكيم عثمان، الجَرَائِم الدوْلِيَّة، في ضوء القَانُون الدولي الجنائي والشريعة الإسلامية، دار الكتب القَانُونية، القاهرة، 2009، ص149.

[34] طلال ياسين العيسى وعلي جبار الحسيناوي، المَحْكَمَة الجِنائِيَّة الدوْلِيَّة – دراسة قَانُونية، دار اليازوري، ط1، الأردن، 2009، ص48.

[35] علي عبد القادر القهوجي، القَانُون الدولي الجنائي، منشورات الحلبي الحقوقية، لبنان، ط1، 2001، ص114.

[36] نايف حامد العليمات، جَرِيمة العُدْوَان في ظل نِظَام المَحْكَمَة الجِنائِيَّة الدوْلِيَّة، ط1، دار الثقافة للنشر والتوزيع، عمان، 2007، ص23.

[37] الْجَمْعِيَّة الْعَامَّة للأمم المتحدة، شبكة المعلومات الدوْلِيَّة "الانترنت"، تم زيارة الرابط بتاريخ 2021/6/8م، https://www.unhcr.org/ar/4be7cc2727f.html

[38] جَرِيمة العُدْوَان، مجلة الإنساني، المركز الإقليمي للاعلام، اللجنة الدوْلِيَّة للصليب الأحمر، شبكة المعلومات الدوْلِيَّة "الانترنت"، على الرابط: https://blogs.icrc.org/alinsani/2020/09/30/4059/

[39] تعريف العُدْوَان، قَرَار الْجَمْعِيَّة الْعَامَّة المرقم "3314" د-29"، شبكة المعلومات الدوْلِيَّة الانترنت، على الرابط: **https://undp.com.pdf**

[40] المصدر نفسه.

[41] عبد الله علي عبو سلطان، "دور القَانُون الدولي الجنائي في حماية حقوق الإنسان" أطروحة لنيل شهادة الدكتوراه في القَانُون العام، كلية القَانُون، جامعة الموصل 2004، ص 256

[42] مسافر كاظم الياسري، سلطة مجلس الامن في الإحالة واثرها في ممارسة المَحْكَمَة الجِنائِيَّة الدوْلِيَّة لاختصاصها، رسالة ماجستير منشورة، معهد العلمين للدراسات العليا، قسم القَانُون، النجف الاشرف، 2018، ص24.

[43] محمود شريف بسيوني، مدخل لدراسة القَانُون الإنساني، منشورات زين الحقوقية، بيروت، 2016، ص204.

[44] نص المادة (11) الاختصاص الزمني: 1- ليس للمحكمة اختصاص إلا فيما يتعلق بالجرائم التي ترتكب بعد بدء نفاذ هذا النظام الأساسي. 2- إذا أصبحت دولة من الدول طرفاً في هذا النظام الأساسي بعد بدء نفاذه, لا يجوز للمحكمة أن تمارس اختصاصها إلا فيما يتعلق بالجرائم التي ترتكب بعد بدء نفاذ هذا النظام بالنسبة لتلك الدولة, ما لم تكن الدولة قد أصدرت إعلاناً بموجب الفقرة 3 من المادة 12.....للمزيد انظر المادة 11 من نِظَام رُومَا الأساسي.

[45] مسافر كاظم الياسري، مرجع سابق، ص88.

[46] إسماعيل عبد الرحمن، "الأسس الأولية للقَانُون الإنساني الدولي" دار المستقل العربي، القاهرة، الطبعة الأولى 2003- ص 15.

[47] راجع، قَرَار مجلس الأمن رقم 1593 لسنة 2005، الصادر في جلسة المجلس رقم 5158 بتاريخ 31 مارس 2005.

[48] مسافر كاظم الياسري، مرجع سابق، ص86.

[49] عبد الواحد الناصر، النِظَام القَانُوني الدولي وإشكالية ما بعد هجمات 11 سبتمبر 2001، منشورات الزمن، الرباط 2006، ص 99.

البحوث والدراسات الامنية

الحرب الروسية - الأوكرانية
وتداعياتها على أمن الطاقة للاتحاد الاوروبي

م.م. عبد الرحمن عبد القادر عبد الله
قيادة فرقة الرد السريع

حظي الأمن الطاقوي الأوروبي باهتمام بالغ من طرف دائرة صنع وتنفيذ القرار لدول الاتحاد وهذا راجع لمشكلة الندرة الطاقوية للوحدات السياسية الأوروبية ومتابعها هذا من هشاشة في أمن الطاقة نتيجة للتبعية نحو الموردين خاصة لروسيا، والتي تعتبر أكبر مورد للطاقة لأوروبا. واستنادا على ما سبق، تعالج هذه الدراسة رهانات الأمن الطاقوي الأوروبي في خوض تراكمية ديناميكية المتغيرات التي تشهدها المنطقة خاصة لما تعلق الأمر بالحرب الروسية على أوكرانيا والتحولات التي مست طبيعة العلاقات الثنائية بين روسيا والاتحاد الأوروبي وتأثيرها على تواصل الإمدادات الطاقوية نحوه، حيث أدى به هذا أن يشهد معضلة أمنية طاقوية نتج عنها ارتفاع في أسعار الطاقة الاستهلاكية مناصفة مع صدمة تضخمية لاقتصاديات دول الاتحاد

الكلمات المفتاحية: الحرب الروسية – الأوكرانية، أمن الطاقة، الاتحاد الاوروبي.

The Russian-Ukrainian war
and its repercussions on the energy security of the European Union

Assistant teacher. Abdul Rahman Abdul Qadir Abdullah
Iraqi Ministry of Interior / Rapid Response Squad

European energy security has received great attention from the decision-making and implementation department of the European Union, and this is due to the problem of energy scarcity of European political units and the consequent fragility in energy security as a result of dependence on suppliers, especially to Russia, which is the largest supplier of energy to Europe. Based on the foregoing, this study deals with the stakes of European energy security in the cumulative dynamic of the variables taking place in the region, especially with regard to the Russian war on Ukraine and the transformations that affected the nature of bilateral relations between Russia and the European Union and their impact on the continuity of energy supplies towards it. This led him to witness an energy security dilemma that resulted in a rise in consumer energy prices in parallel with an inflationary shock to the economies of the Union countries.

Keywords: The Russian-Ukrainian war, energy security, the European Union.

الاستلام 2024/04/04
الارجاع 2024/05/12
القبول 2024/06/09

المقدمة

تعد روسيا الاتحادية شريكًا رئيسيًا للاتحاد الأوروبي في الطاقة، التي تعد الدعامة الأساسية التي يقوم عليها الاقتصاد الروسي، إذ أنها ثالث أكبر دولة طاقوية في العالم، وتحتل المرتبة الثانية بين منتجي الغاز الطبيعي والنفط، والرابعة بين منتجي الكهرباء، والسادسة بين منتجي الفحم. ولعل الروس هم أيضًا المصدرون الرئيسيون للغاز الطبيعي في العالم، فضلاً عن ثاني أكبر مصدري النفط وثالث أكبر مصدري الفحم، فضلاً عن ذلك، فإن روسيا هي الشريك الرئيسي للاتحاد الأوروبي في مجال الطاقة.

كما أن الموقع الجغرافي لأوكرانيا يسمح لها أن تؤدي دور الممر في التجارة الخارجية بين روسيا وأوروبا حيث تستفيد أوكرانيا من العجز الذي تعيشه الموانئ الروسية على بحري البلطيق والأسود، ونتيجة لذلك فإن نسبة كبيرة من اجمالي الغاز الذي تستهلكه أوروبا من روسيا يمر عبر الأراضي الأوكرانية، وبذلك تعد أوكرانيا حلقة محورية مهمة في سلسلة الأمن الطاقوي الروسي والأوروبي نظراً لموقعها الاستراتيجي الذي يمثل محور العلاقة بين روسيا و أوروبا، وفي أوروبا، توجد حاليًا مشكلات صناعية كبيرة يمكن أن تعيق الإمدادات في القارة العجوز. وفي 24 فبراير 2022، وبعد عدة أسابيع من التوتر، شنت روسيا حملة عسكرية في أوكرانيا.

أدانت العديد من الدول الغربية هذه العملية، بما في ذلك الولايات المتحدة ودول الاتحاد الأوروبي. رداً على هذا الهجوم، تم فرض سلسلة من العقوبات الاقتصادية على روسيا لكن هذه الحرب لها أيضًا تداعيات على موارد الطاقة والمال الأوروبي. في الواقع، تمتلك روسيا قوة طاقة تعتمد عليها بعض الدول لذا من المؤكد أن الحرب الروسية الأوكرانية سيكون لها تأثير كبير على تكاليف الطاقة في أوروبا. وكان للحرب الروسية – الأوكرانية غير المبررة تداعيات كبيرة على أسواق الطاقة والغذاء، ما جعل دول الاتحاد الأوروبي تعمل عن كثب على إجراءات تهدف إلى مكافحة ارتفاع الأسعار وندرة الإمدادات. وبشأن أسعار الطاقة وأمن التوريد، نجد أنه منذ النصف الثاني من عام 2021 ، قد ارتفعت بشكل كبير في الاتحاد الأوروبي خاصة.

أهمية البحث

تأتي أهمية البحث من حساسية موضوع الطاقة الأوروبية الروسية، حيث أن الاتحاد الأوروبي يحتاج لاستيراد 53% مما يحتاجه من الطاقة" نفط وغاز"، وفي حالة أوروبا التي

تستورد 39% من نسبة حاجتها من روسيا الواقعة في صراعٍ مع أوكرانيا والتي هي بدورها حليفة أوروبا، ومن هنا نستطيع القول إن روسيا كانت قد استخدمت موضوع الطاقة كورقة ضغط على الاتحاد الأوروبي مقابل الموقف السياسي. وعليه يُفتح باب دراستنا الحالية لنتعرف على التحديات الطاقية "حجمها، بديلها" التي تواجه الاتحاد الأوروبي اليوم.

اهداف البحث

1. إظهار مدى حساسية أمن الطاقة الأوروبي من خلال عرض العلاقات الأوربية الروسية في مجال الطاقة قبل الحرب الروسية الأوكرانية عام 2022.
2. التعرف على تحديات أمن الطاقة بالنسبة لدول الاتحاد الأوربي وروسيا.
3. التعرف على بدائل إمدادات الطاقة الأوروبية، ودور الاتحاد الأوروبي في دعم مساهمة موارد الطاقة البديلة في توليد الطاقة.
4. إعطاء تصور عن بدائل تصدير الطاقة الروسية، بظل المعلومات المتوفرة في يومنا هذا.

إشكالية البحث

يحظى موضوع أمن الطاقة بأهمية كبيرة في العلاقات الدولية ودوره كأحد أهم العوامل التي تؤثر على العلاقات بين الدول، وقد مرت العلاقات الأوروبية_ الروسية تاريخياً بمراحل مختلفة تباينت بين الصراعات العسكرية والحروب الباردة وصولاً إلى علاقات التعاون القائمة على الاعتمادية المتبادلة الشديدة المتمثلة في سعي الطرفين الأوروبي والروسي لتحقيق أمنهم في مجال الطاقة، لذلك نثير لدينا التساؤلات التالية:

- ما طبيعة العلاقات الأوروبية_ الروسية في قطاع الطاقة وماهي التحديات التي تواجهها؟
- ما تداعيات الحرب الروسية الأوكرانية على أمن الطاقة في العلاقات الأوروبية_ الروسية؟

فرضية البحث

تنطلق الدراسة من فرضية وهي (أن للحرب الأوكرانية أثر سلبياً على واقع الطاقة الأوروبي، إذ تعد روسيا المزود الاول للاتحاد الأوروبي بالطاقة (النفط والغاز الطبيعي)، حيث يمر عبر أوكرانيا 80% من أنابيب الطاقة الروسية المتجه نحو أوروبا).

مناهج البحث

استخدم المنهج التاريخي في قراءة وعرض الأحداث التاريخية للعلاقات الأوربية الروسية ، أما بالنسبة للمنهج الوصفي التحليلي فقد أستخدم في تحليل العلاقات الأوروبية_ الروسية في مجال الطاقة، والتداعيات المحتملة للحرب الروسية الأوكرانية على هذه العلاقة ، كما تم الاستعانة بالمنهج الاستشرافي المستقبلي لاستشراف مستقبل العلاقات الأوربية الروسية في مجال الطاقة .

المحور الأول: مهددات الحرب الروسية الأوكرانية على أمن الطاقة للاتحاد الأوربي

تعد روسيا شريكًا رئيسا للاتحاد الأوروبي في الطاقة التي تُعد الدعامة الأساسية التي يقوم عليها الاقتصاد الروسي، إذ تعد روسيا ثالث أكبر قوة طاقة في العالم، وتحتل المرتبة الثانية بين منتجي الغاز الطبيعي والنفط، والرابعة بين منتجي الكهرباء، والسادسة بين منتجي الفحم. ولعل الروس هم أيضًا المصدرون الرئيسيون للغاز الطبيعي في العالم، فضلاً عن ثاني أكبر مصدري النفط وثالث أكبر مصدري الفحم، فضلاً عن ذلك، فإن روسيا هي الشريك الرئيسي للاتحاد الأوروبي في مجال الطاقة. ومن الواضح أن الدول الأوروبية تعتمد بشكل كبير على الطاقة الروسية، ومن ثم فهي تتحمل وطأة عواقب الحرب الروسية الأوكرانية على الرغم من أن ارتفاع أسعار الطاقة سيؤثر على جميع أعضاء الاتحاد الأوروبي، فمن الواضح أن التأثير لن يكون هو نفسه في كل مكان، فهو أكثر اعتدالًا في فرنسا منه في الدول الأوروبية الأخرى. في الواقع، لا تعاني جميع الدول الأوروبية من نفس الاعتماد على الطاقة الروسية، ومن المتوقع أن يعاني بعضها أكثر من غيرها. على سبيل المثال، في فنلندا 94٪ من الغاز المستورد يأتي من روسيا

تسببت التوترات والصراعات المتكررة بين روسيا وأوكرانيا في اضطرابات مؤقتة في إمدادات الطاقة الروسية إلى أوروبا وأصبح أمن الطاقة أحد الاهتمامات الرئيسية للاتحاد الأوروبي التي وافقت على صياغة استراتيجية أمن الطاقة لعام 2014 وإطار اتحاد الطاقة لعام 2015[1].

والتي تضمنت من بين أهدافها تنويع موردي الطاقة وتعزيز المرونة في مواجهة أزمات الطاقة الناتجة عن صدمة العرض. وقد ركز اتحاد الطاقة على زيادة أمن الطاقة من خلال

إنشاء سوق طاقة متكامل في الاتحاد الأوروبي وتحسين كفاءة الطاقة وتنبع سياسة أوروبا في مجال أمن الطاقة من رؤيتها للتحديات القائمة في مواجهة العالم وتتجسد في تحديين بارزين:

الأول: يتعلق بتأمين تغطية منتظمة بتكلفة معقولة من مصادر الطاقة.

الثاني: يتعلق بظاهرة التغير المناخي مما يستدعي العمل بالتوازي مع تنوع مصادر الإمداد وتعدد مسارات النقل والسعي لتحقيق المزيد من التنويع في مصادر إنتاج الطاقة [2].

مع بدء العملية العسكرية الروسية ضد أوكرانيا وفشل المحاولات الأوروبية ، خاصة الفرنسية والألمانية لمنع اندلاع الحرب واقتراب القوات الروسية من كييف وفرض عقوبات اقتصادية على روسيا جعل دول الاتحاد الأوروبي تحذو حذوها في سياسات متضاربة ، وتباين الموقف الأوروبي من التحدي الروسي وعدم قدرته على الانخراط الكامل في تنفيذ العقوبات الأمريكية ، خاصة في مجال الطاقة ، كونه يعتمد في أكثر من ثلث استهلاكه على روسيا، وهذا هو ما جعل المستشار الألماني أولاف شولتز يعلن بعد "قمة فرساي" أوروبا تعمد استبعاد إمدادات الطاقة الروسية من العقوبات، لأن ذلك سيكون له تأثير قوي على اقتصاد الدول الأوروبية[3].

لذلك تعلن دول الاتحاد الأوروبي اليوم عزمها القضاء على الاعتماد على مصادر الطاقة الروسية، وأنها تعتزم الاستغناء عنها في عام 2027، وعقد اجتماعات على أعلى المستويات لمناقشة كيفية تحقيق هذا الهدف، وإطلاق عملية جادة. لإعادة صياغة سياسة الطاقة الأوروبية على مستوى أكثر شمولاً، لكنهم يدركون جيدًا أن هذا لن يتحقق بسهولة، حيث تهيمن روسيا على حصة كبيرة من سوق الطاقة في أوروبا حيث تمتلك روسيا 39٪ من الغاز الطبيعي و33.5٪ من نفط الدول وهذا ما يجعل الاعتماد الأوروبي على إمدادات الطاقة يتركز على مورد واحد مهم تمثله روسيا [4].

يتلقى الاتحاد الأوروبي 80٪ من إمدادات الطاقة القادمة من روسيا عبر أوكرانيا، مما يجعله يواجه مخاوف مستمرة بشأن قطع إمدادات الطاقة. على خلفية الأزمات الأوكرانية المتتالية التي تؤثر على استدامة سلسلة الطاقة تجاه أوروبا. كما قررت العديد من الشركات والمؤسسات الأوروبية تجميد استثماراتها ولم تنسحب من السوق الروسية كما فعلت شركة توتال الفرنسية [5].

يمكن القول إن الاستغناء عن الغاز الروسي الذي يشكل 40٪ من إجمالي واردات الطاقة الأوروبية، غير ممكن في الوقت الحالي وسيستغرق سنوات، وبالتالي ستواجه دول الاتحاد الأوروبي أزمة وانقسام حقيقيين حول السرعة التي ستواجهها إنهاء الاعتماد على إمدادات الطاقة الروسية.

المحور الثاني: مهددات الحرب الروسية الأوكرانية على أمن الطاقة الروسي

أصبحت العقوبات الغربية والاقتصاد الروسي لا تنفصل منذ عام 2014، بعد أن أعلنت روسيا ضم شبه جزيرة القرم إليها، لكن هذه العقوبات رغم شدتها لم تحظ بالجزاءات المؤلمة التي سعت لها الولايات المتحدة الأمريكية وبريطانيا ومع بداية الحرب الروسية الأوكرانية الحالية والتي لم تكن مجرد صراع بين بلدين حيث تخوض أوكرانيا معركة أكبر من قدرتها على تحمل تبعاتها مدفوعة بدعم أوربي مذبذب والثاني خصم قوي وعنيد هدفه تغيير النظام الدولي ومنذ اليوم الأول أثر الصراع على عدة ملفات دولية متشابكة وليست روسيا هي الخاسر الوحيد بأي حال وعلى الرغم من ذلك تبدو روسيا أقل اهتمامًا من أوروبا فيما يتعلق بالعقوبات المفروضة عليها خاصة وأن روسيا خلال العام الماضي تعمدت خفض إمدادات الغاز لأوروبا وبالتالي خلق أزمة طاقة في الدول الأوروبية بهدف الضغط على مفوضية الطاقة الأوروبية في بروكسل للإسراع بالحصول على ترخيص لمشروع نورد ستريم 2 الذي يزود ألمانيا بنحو 55 مليار متر مكعب من الغاز المسال سنويًا(6).

كما لعبت روسيا نفس الورقة قبل غزوها لأوكرانيا لتقسيم صفوف الأوروبيين المحتاجين للطاقة بين مؤيد لأوكرانيا وثاني يخشى دفع ثمن هذا الدعم لاحتياجاتها من الطاقة وأن خسارة السوق الأوروبية بلا شك خسارة كبيرة لروسيا لكن روسيا لديها أسواق بديلة ضخمة من حيث الاستهلاك مثل الصين والهند ودول آسيوية أخرى وحتى دول أفريقية في المستقبل.

المحور الثالث: تحديات أمن الطاقة في العلاقات الأوربية- الروسية

في الماضي وأثناء الحقبة السوفيتية، زادت هيمنة روسيا على إمدادات الغاز إلى أوروبا. منذ بناء خط أنابيب إلى الغرب، ازدادت قبضة روسيا على هذا السوق في السنوات الأخيرة، عندما فتحت الطرق إلى الصين وبدأت في تصدير الغاز الطبيعي المسال وكما ان

الصين لم تعد تستعمل القوة الناعمة فقط لتحقيق مصالحها بل كذلك من اجل التأثير على سياسة الدول الاخرى [7]

حتى تمتلك موسكو الآن حوالي 25٪ من صادرات الغاز العالمية، وفقًا للتقرير الإحصائي السنوي لـ "BB Plc"، تسيطر روسيا الآن على 13.3٪ من إنتاج النفط العالمي، مقارنة بـ 12.3٪ مع السعودية [8]. لذلك سعى الطرفان إلى إقامة شراكة إستراتيجية لضمان أمن الإمدادات، وظهرت تحديات العلاقة المشتركة بين الاتحاد الاوربي وروسيا وأهمها:

1- أثارت الهيمنة الروسية على سوق الطاقة الأوروبية مخاوف الولايات المتحدة الأمريكية، بالنظر إلى الدور الذي تلعبه شركة غازبروم في البنية التحتية للطاقة في الاتحاد الأوروبي، من استخدام النفط والغاز الروسي كسلاح استراتيجي من قبل روسيا في الساحة الأوروبية التي ظلت ميدان النفوذ الأمريكي منذ الحرب العالمية الثانية [9].

2- شبكات أنابيب النفط والغاز والمنافسة الروسية الأمريكية في السيطرة على الأنابيب التي ستنقل النفط إلى الأسواق الغربية، ومحاولة الولايات المتحدة إنشاء مشاريع خطوط أنابيب منافسة للخطوط الروسية، مثل خط نابوكو وخط باكو- جيهان وتعتبر من أخطر التحديات التي تواجه أمن الطاقة في العلاقات الأوروبية الروسية [10].

3- الأزمات السياسية في أوكرانيا وجورجيا، حيث تعتبر أوكرانيا دولة عازلة بين روسيا وأوروبا وتعتبر نقطة العبور الرئيسية لمرور إمدادات الطاقة التي تقدر بـ 80٪ من إمدادات الطاقة الروسية إلى أوروبا [11]. وتبرز مخاطر هذا العبور من خلال مخاطر سلامة شبكة انابيب الطاقة باعتبارها قديمة ومخاطر عسكرية في حال نشوب اعمال العنف ولا سيما في شرق أوكرانيا. ففي عامي 2006 و2009، تسببت الخلافات بين روسيا وأوكرانيا بشأن سعر ونقل الغاز في اضطرابات مؤقتة في إمدادات الغاز الروسي إلى أوروبا، مما أدى إلى زيادة توريق الخطابات السياسية حول الطاقة، والحرب الروسية الجورجية عام 2008. أججت التوترات بين الطرفين، وأدت الأزمة الأوكرانية عام 2014 إلى تحول هذه التوترات إلى مواجهة مفتوحة وأثرت أيضًا على موقف الاتحاد الأوروبي وروسيا تجاه تجارة الطاقة بينهما [12].

كما يُخشى أن ينهار أمن الطاقة الأوروبي والروسي ضحية للأزمات السياسية اللاحقة.

نجد أن أمن الطاقة الأوروبي أصبح مرتبطًا بترتيبات الطاقة الروسية وفقًا للاعتماد المتبادل. حاجة أوروبا للطاقة الروسية تساوي أو تفوق رغبتها في الحد من نفوذها، وهذه التحديات تطال الطرفين بمشكلة تؤثر على أمنهما وتؤكد على اندماجهما في مجال الطاقة.

المحور الرابع: الفرص والخيارات البديلة المتاحة لإمدادات طاقة الاتحاد الأوربي والروسي

لا شك أن أزمة الغاز الأوروبية الروسية هزت الثقة بروسيا كشريك في إمداد أوروبا بالطاقة. دفع ذلك الحكومات الأوروبية إلى إعادة النظر في سياستها القائمة على الاعتماد بشكل أساسي على مصادر الطاقة الروسية والسعي للحصول عليها من مصادر بديلة غير روسية. من ناحية أخرى، تتأثر روسيا بخسارة السوق الأوروبية ومحاولاتها تسويق إنتاج إمدادات الطاقة في الأسواق الأخرى في أسرع وقت ممكن.

أولاً: البدائل المتاحة للدول الأوروبية لإمدادات الطاقة الروسية

يسعى الاتحاد الأوروبي لتقليل اعتماده على واردات الطاقة من الخارج من خلال تعزيز اعتماده على موارده الذاتية وضرورة تنويع مصادر الطاقة لأوروبا بهدف إضعاف أي احتمال للابتزاز. من قبل روسيا، وكانت هذه الاستراتيجية مطروحة على الطاولة حتى قبل بدء الحرب فيما يتعلق بالطلب على الطاقة، تشير تقديرات وكالة الطاقة الدولية إلى أن منحنى الطلب على مصادر الطاقة المختلفة، باستثناء الطاقة الذرية، سيستمر في الارتفاع حتى عام 2030، وسيرتفع معدل استهلاك النفط من (84) مليون برميل يوميا حاليا إلى 116 مليون برميل يوميا عام 2030[13].

أكد وزير الاقتصاد الفرنسي برونو لو مير أن أوروبا لديها العديد من الحلول للاستقلال عن الغاز الروسي، والتي يمكن الاعتماد عليها حتى لا تكون معظم احتياجاتها في قبضة روسيا، وذكر أنه يريد تسريع العمل وفقًا لذلك. حتى تتمكن أوروبا من مواجهة شتاء 2022_2023، وهذه الحلول كالتالي [14].

1- ضرورة تسريع تخزين الغاز بنحو 90٪ من الاحتياجات اللازمة لمواجهة الشتاء الحالي والقادم ابتداءً من الصيف الحالي.
2- تجري الدول الأوروبية عمليات شراء جماعية للحصول على أسعار مخفضة.
3- على الدول الأوروبية تنويع الإمدادات من المنتجين الآخرين.

4- تسريع نشر مشاريع الطاقة المتجددة هذا العام، والتي ستقلل من استخدام الغاز بمقدار 6 مليارات متر مكعب، وتعزز حصة الطاقة الحيوية والطاقة النووية في توليد الكهرباء، مما سيقلل من استخدام الغاز بمقدار 13 مليار متر مكعب خلال عام، بالإضافة إلى إنشاء 8 محطات طاقة نووية لتوليد الطاقة بحلول عام 2050.
5- وضع إجراءات ضريبية قصيرة المدى لحماية مستهلكي الكهرباء من ارتفاع الأسعار.
6- استبدال المضخات الحرارية بأجهزة تسخين الغاز الطبيعي وإغلاق الصناعات كثيفة الغاز.

في سياق سعي الاتحاد الأوروبي إلى التنويع في إمدادات الطاقة، ومحاولته الابتعاد عن الطاقة الروسية، اتجهت الأنظار إلى قطر على أمل أن تقدم حلولاً عاجلة للسوق الأوروبية، بعد إعلانها عن زيادة إنتاجها من الغاز الطبيعي المسال من 77 مليون طن سنويًا إلى 126 مليون طن بحلول عام 2026، رغم أن قطر لن تكون قادرة على تخصيب أوروبا بمفردها من الغاز الروسي، بسبب عدة اعتبارات مهمة. ولا يمكن لدولة واحدة أن تعوض إمدادات الغاز الروسي لأوروبا، وهذا ما صرح به وزير الطاقة القطري، إضافة إلى أن قطر لديها عقود طويلة الأجل تمتد لثلاثة عقود مع دول شرق آسيا. لا يمكنها كسرها ولا يمكنها نظريًا نقل 10-20٪ فقط من صادراتها إلى أوروبا، وآخرها أن هذا الحل يظل قصير المدى وغير مستدام نظرًا للتكلفة العالية نسبيًا لنقل الغاز المسال، الأمر الذي يتطلب مرافق خاصة لتحويله من الحالة السائلة للحالة الغازية قبل استخدامه [15].

كما أن الإتحاد الأوربي يعتمد على تدفق النفط من منطقة الشرق الاوسط ويحرص على تعزيز صادرات الغاز منها لإضعاف القبضة الروسية الخانقة لإمدادات الغاز اليها [16]. على الرغم من الجهود الحثيثة التي تبذلها واشنطن لتعويض إمدادات الطاقة الروسية إلى أوروبا إلا أنها حاولت رفع صادراتها إلى القارة العجوز مستفيدة من موقعها على رأس قائمة الدول المنتجة للغاز بنحو 914 مليار متر مكعب وهو ما يفوق حصة روسيا بنحو 300 مليار متر مكعب ومحاولة الولايات المتحدة إعادة تسعير الغاز لجعله أكثر تنافسية. مع الغاز الروسي لكن كل هذا لم يكن كافيًا لسحب يد الروس لاعتبارات اقتصادية بحتة عدة أبرزها أن الغاز الروسي يتمتع بميزة سعرية نظرًا لوصوله إلى أوروبا عبر خطوط الأنابيب بحكم القرب الجغرافي وتوافر البنية التحتية على عكس الغاز الأمريكي الذي ينقل الغاز المسال بتكلفة عالية عبر

البحار وقد بلغ إجمالي صادرات الغاز الطبيعي المسال الأمريكي إلى أوروبا في يناير 7.5 مليون طن [17].

بعد فشل جهود الاعتماد الكلي على قطر وأمريكا وأذربيجان والنرويج، لجأت أوروبا إلى الشعور بنبض الدول الأخرى وأبرزها الجزائر كواحدة من أكبر مصدري الغاز الطبيعي في العالم، بالإضافة إلى بعدها الجغرافي عن أوروبا لكن الجزائر قبل اندلاع الحرب أبلغت زبائنها الأوروبيين أنها قد تخفض صادراتها من الغاز بسبب ارتفاع الطلب المحلي وهي الآن ملزمة بموقف الحياد من الحرب في أوكرانيا، وحتى إذا قبلت الجزائر بتصدير طاقتها إلى أوروبا، قد لا تتمكن من تعويض إمدادات الغاز الروسي إلى أوروبا بسبب الاختلاف الكبير في إنتاج البلدين فالحد الأقصى الذي يمكن أن يحمله خط الأنابيب المغاربي هو 32 مليار متر مكعب مقارنة بـ 300 مليار متر مكعب من الغاز تقدمه روسيا سنويًا إلى أوروبا[18].

يفكر الغرب الى جانب النفط في بدائل أكثر موثوقية لتعويض حصة روسيا من النفط وقد دخلت الولايات المتحدة الأمريكية مؤخرًا في محادثات ومفاوضات تهدف إلى وقف تدفق النفط الروسي إلى أوروبا من أجل حرمان روسيا من أحد أكبر الأسواق المستهلكة لمنتجاتها النفطية في العالم.

ولكن كما هو الحال مع الغاز، تراهن روسيا على إمكاناتها النفطية الهائلة التي تمكنها من إلحاق الضرر بسوق النفط العالمي دون أن تتمكن دول النفط الأخرى مثل العراق والسعودية وإيران وفنزويلا من تعويض العجز لتثبت للمرة الثانية أن جميع طرق الطاقة في أوروبا تؤدي حتمًا إلى روسيا على الأقل إلى المدى القريب، تعتبر معضلة الطاقة من أبرز العناوين التي توضع على طاولة البحث الأوروبية والنقاش حول هذه القضية يشكل مادة غنية والحاجة إلى تحول سريع وتبني نموذج طاقة جديد يعتمد على الاعتماد على مصادر طاقة بديلة من الرياح والوقود الحيوي والطاقة الشمسية ففي السنوات الخمسة الاخيرة تمكنت أوروبا أن تولد ضعف كمية الكهرباء التي يوفرها الفحم بالاعتماد على مصادر الطاقة المتجددة بينما يوفر الفحم الآن حوالي 12٪ من توليد الكهرباء وأصبحت طاقة الرياح والطاقة الشمسية تمثل حوالي 21٪ من توليد الكهرباء وخلال الفترة ما بين يناير ويونيو من عام 2021 تم إنتاج حوالي 40% من الكهرباء باستخدام طاقة الرياح والطاقة الشمسية والمياه والطاقة الحيوية في دول الاتحاد الأوروبي البالغ عددها 27 دولة بينما أنتج الوقود الأحفوري 34٪ فقط مما يشير

إلى تسارع حقيقي في دول الاتحاد الأوروبي في الانتقال نحو الطاقة النظيفة لذلك يريد الاتحاد الأوروبي أن تأتي حصة الكهرباء من الطاقة المتجددة لديها أن تصل إلى حوالي 32٪ بحلول عام 2030[19].

وكما للطاقة المتجددة العديد من المزايا ولكن ما يؤخذ منها هو أنها تعتمد على الرياح أو أشعة الشمس لذلك فإن الاتجاه نحو الطاقة النووية كمكمل مفيد يوفر طاقة ميسورة التكلفة ونظيفة وصديقة للبيئة بشكل مستمر وبكفاءة عالية معظم أيام السنة وتحققت التنمية المستدامة مع نمو سكان العالم وزيادة الطلب على الطاقة ففي عام 2020 بلغ الإنتاج العالمي من الكهرباء حوالي 27 ألف تيراواط / ساعة وبلغ معدل إنتاج محطات الطاقة النووية حوالي 2500 تيراواط / ساعة ومن ثم تمثل الطاقة النووية حوالي 11٪ من الإنتاج العالمي مع وجود 450 مفاعلًا نوويًا قيد التشغيل في 30 دولة وتظهر التوقعات أن الطاقة النووية سيكون لها دور رئيسي في مزيج الطاقة في العالم لعقود قادمة في ظل حروب الطاقة[20].

لكن الطاقة النووية محدودة الانتشار بسبب النظرة القاتلة لها بعد حادثة فوكوشيما التي جعلت العالم يتخذ موقفا عدائيا تجاهها حرصا منها فألمانيا قررت التخلص التدريجي منها واعترضت على مقترحات الاتحاد الأوروبي التي من شأنها أن تجعل تقنية الذرة جزءاً من خطط الاتحاد لمستقبل طاقي آمن واسبانيا وايطاليا والنمسا ولوكسمبورغ غير معنية قدماً نحو هذه الطاقة، إذ ألغت خططاً لإضافة محطات نووية جديدة، بينما تهدف فرنسا والتي تترأس الإتحاد الأوروبي حالياً إلى تحديث المفاعلات الحالية وبناء أخرى جديدة لتلبية احتياجاتها المستقبلية من الطاقة، في ظل الظروف الحالية ونقص التوريدات المستوردة[21]. وحشد دعم واسع لاجتياز مشروع تصنيف الطاقة النووية والغاز طاقة نظيفة ومفيدة لانتقال الطاقة، أمام 27 دولة عضو في الاتحاد الأوروبي حاليًا وإدراجها في الاستثمارات الخضراء.

ثانيا : الفرص والبدائل الممكنة لتصدير الطاقة الروسية

تعد قضية أمن الطاقة الروسية وتحدياتها الحالية من أهم القضايا الأمنية في استراتيجية روسيا الاقتصادية والسياسية، لأن روسيا هي اللاعب الأكبر في مجال الطاقة في أوراسيا بفضل قدراتها الهائلة في مجال الطاقة التي تعتمد عليها بالإضافة إلى مكانتها كواحدة من أهم منتجي ومصدري الطاقة تجاه أكبر المناطق المستهلكة لهذه الموارد خاصة في أوروبا وآسيا[22].

فالطاقة هي شريان الحياة للاقتصاد الروسي وقطع الإمدادات عن مستهلكي الطاقة الرئيسيين في ظل العقوبات الحالية سيؤدي إلى انهيار الاقتصاد الروسي خاصة وأن الأسواق الأخرى لا يمكن أن تحل محل السوق الأوروبية على الرغم من أن روسيا هي العضو الدائم الوحيد في مجلس الأمن الذي لا يحتاج استيراد الطاقة بل هي الأولى في الإنتاج والتصدير والوحيدة المسيطرة على أسواق الطاقة خارج دول الأوبك [23].

وتراهن روسيا خلال محاولاتها لضمان وتعزيز أمن الطاقة لديها على مجموعة من الفرص والرهانات القائمة على الحفاظ على مكانة روسيا في سوق الطاقة الأوروبية من ناحية وفي نفس الوقت البحث عن أسواق عالمية جديدة مماثلة لتلك الأسواق الأوروبية من خلال مشاريع جديدة [24].

إن الصين متعطشة للطاقة لم تدين الحرب ولم تشارك في عقوبات غربية ضد روسيا هل ستكون من المنافذ البديلة لغازها؟

كانت العلاقات بين الصين وروسيا ولا تزال، متعددة الأبعاد وعميقة الجذور بعد أن مرت بفترات صعبة قبل الحرب الباردة حيث كانت السياسات الأمريكية والغربية حريصة على تعميق هذا الخلاف ولكن بعد الحرب الباردة تم توحدهم في خندق واحد في مواجهة المعسكر الغربي بقيادة الولايات المتحدة الأمريكية والصين هي الشريك الأكبر لروسيا اقتصادياً خاصة بعد بيان الشراكة الاستراتيجية "بلا حدود" التي تم توقيعها بين الرئيسين الصيني والروسي في 4 فبراير 2022 والتي تضمنت عدة اتفاقيات تجاوزت 15 اتفاقية أهمها توريد الغاز الروسي إلى الصين عبر خط انابيب جديد بطاقة 50 مليار متر مكعب من الغاز سنويا ونصت أهم بنود الاتفاقية على توريد 10 مليارات متر مكعب من الغاز الروسي إلى الصين سنويًا على مدى 30 عامًا تبدأ من عام 2026 وتسوية مبيعات الغاز بين الجانبين باليورو بدلًا من الدولار الامريكي [25].

ملاحظات ختامية واستنتاجات

يشكل الأمن الطاقوي للاتحاد الأوروبي إشكالية محورية، فبالرغم من أن الاتحاد الأوربي يعتبر كقوة سياسية اقتصادية دولية إلا أنه يعيش تبعية مزمنة فيما يخص أمنه الطاقوي، ولقد توصل هذا البحث إلى فهم مجموعة من الاستنتاجات ومنه تم:

1- تعد روسيا كطرف رئيسي في المعادلة الطاقوية الأوروبية فهي تؤثر بشكل مباشر على الاستقلالية الطاقوية للاتحاد بفضل إمكاناتها الكبرى في مجال الطاقة والتي تستخدمها كورقة ضغط في علاقاتها.

2- كشفت الأزمة الأوكرانية العديد من الحقائق خاصة حقيقة الاعتماد الروسي في تمويل إمداداته الطاقوية للدول الأوروبية عبر أوكرانيا، ، وكما لا يمكن إنكار أن للأزمة تأثير بالغ الخطورة على الأوضاع السائدة في العالم من أجل تحقيق الأمن والسلم الدوليين، حيث سعت روسيا بكل الطرق بعدم السماح لأوكرانيا بالتعامل مع الغرب لأنه يشكل تهديدا لمصالحها وأمنها القومي، وعليه عرفت الساحة الدولية تحولات سريعة في موازين الصراع والتنافس فظهور روسيا كلاعب إستراتيجي بين الدول جعلها من جه مقبولة بنوع من الارتياح ومن جه أخرى عدم الارتياح لهذه الأوضاع بحكم وجود مصالح خفية وكما تعتبر نقاط تحول جيوسياسية وجيو اقتصادية لروسية في المنطقة.

3- سعت روسيا إلى استعادة نفوذها على أوكرانيا عن طريق ضم شبه جزيرة القرم بعد الإطاحة بالرئيس الأوكراني فيكتور يانوكوفيتش من قبل القوات الموالية للغرب، بحيث تعتبر ذات أهمية إستراتيجية وتاريخية لروسيا، مما جعلها تسعي بكل إمكانياتها لإثبات موقعها كدولة كبرى على المستويين الإقليمي والدولي، ويظهر ذلك من خلال تصديها لتوسع إمداداتها الطاقوية، وذلك من خلال ضم شبه جزيرة القرم سنة2014.

4- عرف الإتحاد الأوروبي عجز فادح من النفط والغاز ومن أجل المحافظة علي مكانته الاقتصادية والقضاء علي التبعية الروسية ،من خلال تنويع مصادر إمداداتها جعله يتوجه نحو منطقة المتوسط، بحيث تعتبر الجزائر أحد الحلول المهمة لحل الطاقوية، مما جعلها تعقد العديدة من الاتفاقيات معها، وعليها أصبحت الجزائر الحل مشكلتها الطاقوية، مم الوحيد لدول الإتحاد الأوروبي في القضاء علي فجوة العرض والطلب لامتلاكها بنية تحتية كبيرة، ما فتح آفاقا واسعة أمام صناعة الغاز بالجزائر وكذلك توجهها نحو منطقة الشرق الأوسط، ونخص بالذكر دولة قطر التي لديها إمكانيات كبيرة في تصدير الغاز الطبيعي نحو الإتحاد الأوروبي وكما يعد الغاز القطري أيضا

حل بديلا ومثاليا ليحل محل الإمدادات الروسية، بحيث تملك قطر حجم كبيرة من احتياطيات الغاز الطبيعي الذي يمكنها من تصديره إلي تركيا، وكذلك حقل الشمال القطري الذي تريد أن تجعله الحقل الأكبر في العالم.

المصادر والمراجع:

(1) سهير الشربيني، ازمة الطاقة في أوروبا: الابعاد المحلية والتداعيات العالمية، موقع ترينذز للبحوث والاستشارات، 3 فبراير 2022 ،متاح على الرابط التالي: https://trendsresearch.org/ar/insight-، (تاريخ الزيارة: 2023/4/15 9:45pm).

(2) محمد فال ولد المجتبى، السياسة الخارجية الاوربية وتحديات جيوبوليتيكا الطاقة، مركز الخليج للابحاث، 1 نوفمبر 2008، متاح على الرابط التالي: https://araa.sa/index.php?view=article&id=1888:2014-07-16-14-57-30&Itemid=172&option=com_content، (تاريخ الزيارة 2023/4/15، 10:30pm).

(3) عمر الشوبكي، الاتحاد الاوربي والحرب في اوكرانيا، مركز الاهرام للدراسات السياسية والاستراتيجية، 2022/3/16، متاح على الرابط التالي : https://acpss.ahram.org.eg/News/17435.aspx،، (تاريخ الزيارة 2023/4/15، 11:5pm).

(4) محفوظ رسول، السياحة كبديل مستديم للريع النفطي في الجزائر، جامعة الجزائر، 2016/6/17، متاح على الرابط التالي : https://www.asjp.cerist.dz/en/article/88834، (تاريخ الزيارة 2023/4/16 9:30Am).

(5) عمر الشوبكي، الاتحاد الاوربي والحرب في اوكرانيا، مصدر سبق ذكره.

(6) نورا عبه جي، تحديات العلاقات النفطية الروسية الاوربية، المعهد المصري للدراسات، المجلد 07، العدد 27، 2022/3/18، متاح على الرابط التالي : https://eipss-eg.org-،(تاريخ الزيارة 2023/4/20، 3:45Am).

(7) صفاء حسين علي، إستراتيجية القوة الذكية وأثرها في السياسة الخارجية الصينية، مجلة الجامعة العراقية، العدد 37، (الجامعة العراقية)، ص 372.

(8) د. نهلة الخطيب، تحديات أمن الطاقة في العلاقات الأوربية الروسية: الحرب الروسية – الاوكرانية نموذجاً، المركز الديمقراطي العربي، 2022، ص 38.

(9) نورا عبه جي، تحديات العلاقات النفطية الروسية الاوربية، مصدر سبق ذكره، ص2.

(10) المصدر نفسه، ص3.

(11) محفوظ رسول، السياحة كبديل مستديم للريع النفطي في الجزائر، مصدر سبق ذكره، ص 146.

(12) سوزي رشاد، أمن الطاقة ومحاولات روسيا فرض النفوذ الدولي، مصدر سبق ذكره، ص 146.

(13) محمد فال ولد مجتبى، مصدر سبق ذكره.

(14) نجاة عبد القوي عون، أوروبا بعد الغاز الروسي الى اين؟، مركز رواق بغداد 2022/4/25، ص 6.

(15) نجاة عبد القوي عون، مصدر سبق ذكره، ص 11.

(16) صدام مرير محمد عطية، الصراع الدولي والاقليمي في الشرق الاوسط واثره على المنطقة العربية(انموذج ثورات الربيع العربي)، مجلة تكريت للعلوم السياسية، العدد11،(جامعة تكريت، 2017)، ص 317.

(17) المصدر نفسه، ص 12.

(18) نجاة عبد القوي عون، مصدر سبق ذكره، ص 13.

(19) سهير الشربيني، مصدر سبق ذكره، ص 19.

(20) ميخائيل شودا كوف، طاقة نووية من اجل المستقبل، مجلة الوكالة الدولية للطاقة الذرية، 2016/9/1، متاح على الرابط التالي: https://www.iaea.org/ar/bulletin/tq-nwwy-mn-jl-lmstqbl، تاريخ الزيارة (2023/4/19، 5:32pm).

(21) أحمد الطالب محمد، مستقبل الطاقة النووية في ظل أزمة الطاقة العالمية، مجلة الوكالة الدولية للطاقة النووية، 2022/2/3، متاح على الرابط التالي: https://attaqa.net/2022/02/03، تاريخ الزيارة (2023/4/19، 7:5pm).

(22) نورا عبه جي، مصدر سبق ذكره، ص 10.

(23) خديجة محمد عرفة، مصدر سبق ذكره، ص 95.

(24) نورا عبه جي، مصدر سبق ذكره، ص11.

(25) رضوان جمول، الاقتصاد السياسي للصين الحديثة_ قراءة في "مبادرة الحزام والطريق" وآفاقها المستقبلية، المركز الاستشاري للدراسات والتوثيق، 2016، ص56.

البحوث والدراسات الامنية

أمن المعلومات
بين الضرورات الآنية والتدابير المستقبلية

م.م. إبراهيم محمد محمود الجبوري
باحث دكتوراه في إدارة الاعمال/ قسم التسويق

ساهم التطور التكنولوجي في مجال الاتصالات وتقنيات المعلومات في سرعة انتشار المعلومات وسهولة تداولها عبر خدمات الإنترنت مما أدى إلى ظهور العديد من المخاطر والاعتداءات التي تتم في بيئة الإنترنت الأمر الذي أدى إلى ضرورة نشر الوعي بين المستخدمين لحماية أمن المعلومات، وذلك من خلال قيام العديد من الدول على وضع التشريعات التي تحمي أمن المعلومات فضلاً عن العديد من المنظمات التي تقوم بوضع مواصفات دولية لتكون بمثابة الدليل الاسترشادي الأمثل لحماية أمن المعلومات مثل منظمة الأيزو، وبذلك يتأتى هدف البحث إلى التعرف على المخاطر التي يتعرض لها أمن المعلومات الرقمية بأشكالها المختلفة والتدابير المضادة للحد من هذه المخاطر مثل التدابير التنظيمية والمادية والتقنية بالإضافة إلى التدابير التشريعية على المستويين الوطني والدولي وأهم المعايير الدولية التي تضعها منظمة الأيزو لضبط ممارسات أمن المعلومات.

الكلمات المفتاحية: الأمن، أمن المعلومات، الحوكمة الرقمية، الانترنت.

Information Security
Between immediate necessities and future measures

Assistant teacher . Ibrahim Muhammad Mahmoud
Leading the rapid response squad

Technological development in the field of communications and information technologies has contributed to the rapid spread of information and the ease of its circulation through Internet services, which has led to the emergence of many risks and attacks that take place in the Internet environment, which has led to the necessity of spreading awareness among users to protect information security, through the establishment of many countries To develop legislation that protects information security, in addition to many organizations that develop international specifications to serve as the optimal guideline for protecting information security, such as the ISO organization. Thus, the aim of the research is to identify the risks to which digital information security is exposed in its various forms and countermeasures to reduce these. Risks such as organizational, physical and technical measures, in addition to legislative measures at the national and international levels and the most important international standards set by the ISO organization to control information security practices.

Keywords: Security, information security, digital governance, the Internet.

الاستلام	الارجاع	القبول
2024/05/01	2024/06/10	2024/06/20

المقدمة

تظهر أهمية دراسة أمن المعلومات بشكلٍ خاص، في أن معلومةٍ ما، قد تحمل اكتشاف جديد يُفيد البشرية في مجالٍ ما، ومعلومة أخرى تتعلق بالاقتصاد، تكون سبباً في إفلاس دول اقتصادياً، وأخرى تساعد في بناء اقتصادها، لذا فإن أهمية المعلومة تظهر في ابتكارها وإحسان استخدامها، وإذا ما أردنا تحديد الأهمية المادية للمعلومة نجد أن علماء أمن المعلومات انقسموا إلى اتجاهين لتحديد أهميتها: الاتجاه التقليدي: وهو الاتجاه الذي لا يرى في المعلومات أي قيمة مادية بل أنها ذات طبيعة معنوية لا تندرج تحت القيم المحمية، إلا إذا كانت تنتمي إلى المصنفات الأدبية والفنية أو الصناعية. أما الاتجاه الحديث: فهو يرى أن للمعلومات قيمة مالية أشبه بالسلعة، أي أنها نتاج ذهني ولكي تكون صالحه للتملك لا بد وأن يحوز مالكها على العناصر المكونة لها بطريقة شرعية في قالب يصلح للاطلاع عليها بغض النظر عن الوسيط الذي يتضمنها، من هنا كان الاهتمام بهذه الدراسة لمعرفة الضوابط التي تحول دون انتهاك قيمة المعلومات والتدابير الأمنية المتوافرة لحمايتها وضمان وصولها بطريقة شرعية.

أهداف البحث:

يسعى البحث إلى تحقيق عدد من الأهداف التي يمكن إيجازها في النقاط التالية:

1- التعرف على مفهوم أمن المعلومات وعناصره
2- توضيح المخاطر التي تهدد أمن المعلومات.
3- بيان أساليب مواجهة الاعتداءات التي تواجه أمن المعلومات.
4- استعراض أهم التدابير المحلية والدولية الخاصة بحماية أمن المعلومات.

إشكالية البحث

أضحت عمليات حماية المعلومات امراً بالغ الأهمية في ظل البيئة الرقمية المتطورة، اذ ان التصدي للتهديدات الأمنية لنظم المعلومات أصبح تحدياً يواجه سيادة الدولة وديمومة عمل مؤسساتها، فأمن المعلومات لا يعني تأمين المعلومة والحفاظ على سرية ونزاهة المعلومات وتوافرها فقط، ولكن ايضاً تأمين البنية التحتية التي تسهل استخدامها من أجهزة وبرمجيات وعوامل بشرية ومادية.

فرضية البحث

تفاقمت المخاطر الأمنية مع التقدم التكنولوجي، وسلكت الدول مسالك عديدة في تجديد عقيدتها الأمنية وزج مؤسساتها الأمنية في العمل الرقمي، حتى تصدرت العديد من دول العالم المتقدم المشهد الرقمي، واخذت الريادة في مجال أمن المعلومات وتمتلك كبريات الشركات الأمنية في هذا المجال، على ذلك وفي ضوء إشكالية البحث يمكن صياغة الفرضية البحثية الآتية: "إن إدارة المخاطر الأمنية وفقاً للأنظمة الرقمية الأمنية المعاصرة في الفضاء الرقمي يتيح للدولة التقدم في شتى المجالات، وبناء قدراتها، فالعالم اليوم ومستقبلاً مرهون بالتقدم الرقمي لما يقدمه من ميزات فريدة تقلل الكلفة، وتستثمر الوقت، والجهد".

مناهج البحث

اعتمد الباحثون على المنهج الاستنباطي للتعرف على إدارة أمن المعلومات وحوكمتها وبيان سبل إدارة مخاطرها، فضلاً عن توضيح العديد من المفاهيم ذات العلاقة بالموضوع.

المحور الأول: الإدارة والحوكمة الأمنية للمعلومات

احتلت أبحاث ودراسات أمن المعلومات مساحة رحبة آخذة في النماء من بين أبحاث تقنية المعلومات المختلفة، فهو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها، ومن زاوية تقنية هو الوسائل والادوات والاجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية، واستخدام اصطلاح أمن المعلومات في نطاق انشطة معالجة ونقل البيانات بواسطة وسائل الحوسبة والاتصال[1]، إذ مع شيوع الوسائل التقنية لمعالجة وخزن البيانات وتداولها والتفاعل معها عبر شبكات المعلومات وتحديدًا الإنترنت.

وتضمن الإدارة والحوكمة الأمنية الوفاء بمعايير إدارة الأمن التي تم تنفيذها بالتماشي مع حاجات وأهداف المنظمة، وهذه المعايير قد تكون أفرادًا أو منتجات أو عمليات مجموعة مع بعضها، وتركز على المنتج والتقنية الى جانب تركيزها على الإدارة ودخولها في العمل وتكاملها مع دعم أمن تقنية المعلومات.

ويمكن تعريف مجال أمن المعلومات بكونه فرع من فروع العلوم التقنية الحديثة، وفيه يتم حماية المعلومات والبيانات المتداولة سواءً على الإنترانت أو المحفوظة بشكل رقمي في مركز

بيانات[2] من الهجمات الضارة أو الوصول غير المسموح لأي طرف خارجي أو التعرض للتخريب المتعمد فيها[3].

يعد مجال أمن المعلومات واحدًا من أهم المجالات المطلوبة في الوقت الحالي ولاسيما للوظائف التي تتسم بياناتها بالسرية والخصوصية التي ترتقي إلى كونها بيانات حساسة للغاية لا يجب تداولها، إذا يقوم هذا العلم على حماية هذه المعلومات من الظهور وعلى الحفاظ على خصوصيتها ضمن نطاق الأشخاص المسموح لهم فقط.

لقد ظل هذا المجال من الأمن حتى أواخر السبعينات معروفًا باسم أمن الاتصالات (Communication security) والذي حددته توصيات أمن أنظمة المعلومات والاتصالات لوكالة الأمن القومي في الولايات المتحدة بأنه: "المعايير والاجراءات المتخذة لمنع وصول المعلومات الى ايدي اشخاص غير مخولين عبر الاتصالات ولضمان أصالة وصحة هذه الاتصالات".

وفي الثمانينات مع النمو للحاسبات الشخصية بدأت حقبة جديدة من الامن سميت امن الحواسيب Computer Security، والتي حددت بكونها المعايير والاجراءات التي تضمن سرية كمال وتوافر مكونات انظمة المعلومات بما فيها التجهيزات والبرامجيات والمعلومات التي تم معالجتها وتخزينها ونقلها".

وفي التسعينات من القرن الماضي تم دمج مفهومي الأمن (أمن الاتصالات وأمن الحواسيب) لتشكل ما أصبح يعرف باسم (أمن أنظمة المعلومات) Information System security والتي عُرفت بأنها : حماية انظمة المعلومات ضد أي وصول غير مرخص أو تعديل المعلومات أثناء حفظها ومعالجتها أو نقلها ، وضد إيقاف عمل الخدمة لصالح المستخدمين المخولين أو تقديم الخدمة لاشخاص غير مخولين بما في ذلك جميع الاجراءات الضرورية لكشف، وتوثيق ، ومواجهة هذه التهديدات[4] .

إن أمن المعلومات من زاوية أكاديمية يُعرف بانه العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها من انشطة الاعتداء عليها وعرفه السالمي على أنه " العلم الذي يهتم بدراسة طرائق حماية البيانات المخزونة ضمن الحاسوب وأنظمة الاتصالات والذي يتناول سبل التصدي للمحاولات الرامية الى معرفة البيانات المخزونة ضمن

الحاسوب بصورة غير مشروعة والى تلك التي ترمي الى نقل أو تغيير أو تخريب برمجيات حماية البيانات[5].

أما من الناحية التقنية فإن أمن المعلومات يشير الى الوسائل والادوات والاجراءات اللازم توفيرها لضمان حماية المعلومات من الاخطار الداخلية والخارجية [6].

من البين اذن، ان أمن المعلومات هو مجموعة المعايير والمقاييس والاجراءات والتدابير الوقائية والدفاعية التي تستخدم لحماية انظمة المعلومات بكل مكوناته وتحقيق التكامل على كافة المستويات لضمان سرية المعلومات، وتوافرها وسلامة محتواها وتحديد مسؤولية المتصرف بها وهذا ما استخلصناه من التعريف أعلاه بسبب شموليته ولكونه تضمن الخصائص المطلوبة لأية معلومات يراد توفير الحماية لها، وهذا ما أكدته اغراض وابحاث واستراتيجيات ووسائل أمن المعلومات سواءً من الناحية التقنية أو الأدائية أو التشريعية.

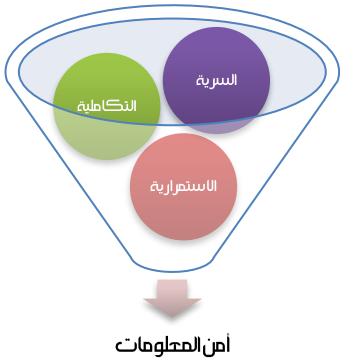
المحور الثاني: ضرورات أمن المعلومات

تنبع أهمية أمن المعلومات من أن المعلومات تستخدم من قبل الجميع بلا استثناء، وهي هدف للاختراق من قبل الجميع ، وفي بعض الأحيان تكون المعلومات هي الفيصل بين المكسب والخسارة للمنظمات وقد تكلف الفرد ثروته وربما حياته في بعض الأحيان وتزداد أهميتها في المنظمات الأمنية والعسكرية والاقتصادية ذات الطابع الاستراتيجي[7]، لذلك ارتبط عنصر السرية بالمعلومات ودرجة توافرها، في ضوء ما يترتب على فقدانها من خسائر وما يترتب على توافرها من مكاسب أن 75% من كبار المديرين في المملكة المتحدة، على سبيل المثال يدعون الآن إلى عد أمن المعلومات أولوية عليا، إذ أن متوسط أنفاق شركة بريطانية ما يقارب (4-5) من الميزانية على أمن المعلومات[8].

أصبحت المشكلة الآن ليس الحصول على المعلومات ، وإنما كيفية حماية هذه المعلومات من الأخطار التي تهددها، أما الهدف الأساسي لأمن المعلومات فهو الدقة وسلامة وأمان كل العمليات ومصادر نظام المعلومات، كما أن إدارة الأمن يمكن أن تقلل الأخطاء والاحتيال والخسائر في النظام الذي يربط كل من المنظمة وزبائنها وأصحاب المصالح فضلا عن ذلك فإن أمن وسرية المعلومات يتضمن تحديد جميع الثغرات الأمنية في المراقبة المحتملة التي قد تسمح للأفراد غير المصرح لهم الوصول إلى النظام، لذلك يجب على ادارة المنظمة إن تكون على دراية باستعمال التقنيات المعروفة جميعها لأمن النظام للتغلب على الثغرات الأمنية[9]

على ذلك يعتمد أمن المعلومات على ثلاثة عناصر أساسية لابد أن يتم توافرها في المعلومات التي تستوجب الحماية، وهي السرية Confidentiality وسلامة المعلومات وتكاملها Integrity وتوافر المعلومات Availability ، تُعرف باسم مثلث CIA أو Triangle CIA، ويمكن تناولها على النحو التالي[10]:

1. السرية



Source: Arnason, Sigurjon Thor & Willett, Keith D.(2008). How to Achieve 27001 Certification An Example of Applied Compliance Management. USA, New York: Taylor & Francis Group LLC. 3

وتعني التأكد من أن المعلومات لا تكشف ولا يطلع عليها من قبل اشخاص غير مخولين بذلك[11]، بما في ذلك الخصوصية – أي ضمان أن المعلومات الحساسة أو الخاصة يمكن الوصول إليها فقط من الأفراد المخولين بالحصول عليها وعدم اظهارها لغير الافراد المخولين قانونًا، ويوفر هذا المبدأ للمنظمة السرية التامة للمعلومات كافة، حتى لو كانت المعلومات صغيرة وبسيطة ومنها (المعلومات الشخصية والموقف المالي المنظم ما قبل إعلانه والمعلومات العسكرية وغير ذلك)[12].

2. التكاملية وسلامة المحتوى

التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله او العبث به وبشكل خاص لن يتم تدمير المحتوى أو تغيره او العبث به في أية مرحلة من مراحل المعالجة أو التبادل سواءً في مرحلة التعامل الداخلي مع المعلومات أو عن طريق تدخل غير مشروع يأتي مبدأ التكامل والسلامة كمكمل لمبدأ السرية، حيث لا يستطيع الأخير الحفاظ على حماية المعلومات بشكل كافٍ بدون أن يساعده هذا المبدأ على إتمام جزء كبير من مهمته، وفيها يتم الحفاظ على المعلومات التي تم حفظها أو تشفيرها أو تخزينها من التخريب المتعمد، بالشكل الذي يجعلها غير صالحة للاستخدام أو تسبب ضررًا لصاحبها. يجب التأكد من ان المعلومات لم تغير أو حذف جزء منها من قبل وسائل غير معروفة أو غير مخولة ومنها(تغيير إحداثيات أمنية أو معلومات استخباراتية عسكرية أو تغيير أسماء المقبولين في قوائم التعيين عن طريق حذف وإدراج أسماء بديلة مما يسبب الارباك للجهة المعنية ، أو تغيير مبلغ تحويل بإضافة أصفار)، أن النظام الأمن يؤمن تكاملية البيانات المخزنة فيه، فالمقصود بالتكاملية حماية البيانات من عمليات

الحذف والتخريب ، ويجري تأمين ذلك من خلال مجموعة من الأساليب توفرها نظم قواعد البيانات فضلا عن علاقات الترابط ما بين البيانات المخزونة فيها[13].

3. استمرارية توفر المعلومات او الخدمة

أي التأكد من استمرار عمل النظام المعلوماتي واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة للمواقع المعلوماتية وأن مستخدم المعلومات لن يتعرض الى منع استخدامه لها أو دخوله اليها، مع الضلع الأخير في ثالوث المبادئ الخاصة بأمن المعلومات، يأتي مبدأ توافر المعلومات كشرط اساسي لتكامل النظام، حيث يهدف هذا المبدأ إلى جعل البيانات والمعلومات في نوع من التوافر والحيازة المرنة، التي تجعل صاحبها قادر على الإطلاع عليها ومراجعاتها واستخدامها في أي وقت بدون أي تعقيدات.

يهدف مبدأ توافر البيانات هذا على مساعدة أصحاب المعلومات على استخدام المميزات التكنولوجية المختلفة من خدمات سحابية وغيرها على تخطي حاجز المكان والزمان فيما يتعلق بالوصول إلى المعلومات، إذا بسهولة ومن خلال خطوات بسيطة يمكن للأشخاص المخول لهم الوصول إلى هذه المعلومات الاطلاع عليها من أي جهاز بدون التعرض لأي خطر أو هجمات أو إلحاق الضرر بأي منها، وذلك باستخدام قنوات اتصال معدة خصيصًا لهذا الغرض.

ومن خلال ما تقدم نرى بأن معظم المنظمات تتعرض الى العدوان على معلوماتها ومحاولة سرقتها والعبث بها، وهذا ما يشكل الجانب السلبي للتطور التكنولوجي لنظام المعلومات، فالجرائم المتحققة عن هذا العدوان تتميز عن الجرائم العادية بسرعتها الفائقة وتأثيرها المدمر، وقدرة مرتكبيها على الإفلات من الملاحقة والعقاب في ظل أفتقاد كثير من الدول نظم قانونية قادرة على التعامل مع هذا العدوان والجرائم الناجمة عنه، وتشير الاحصاءات الدولية الى أن هناك أكثر من ملياري شخص مستخدم لأجهزة الحاسب الآلي، فضلا عن وجود أكثر من (١٣) مليار صفحة على شبكة المعلومات الدولية (الانترنيت) ونحو (٣٠٠) مليون موقع[14].

وهكذا اتسعت البيئة المعلوماتية لتصبح ميدانا فسيحا للعدوان عليها ، وقد بينت دراسة للأمم المتحدة عن مخاطر الحاسب الآلي أن (٧٣) من الجرائم داخلي و (٢٣) منها يرجع الى

مصادر خارجية وقدرت الخسائر الاقتصادية لهذه الجرائم عام (١٩٩٣) بنحو (٢) مليار دولار، ومن أجل الوقوف بوجه هذا العدوان أصدرت منظمة التقييس العالمية للمواصفات العالمية المواصفة القياسية (ISO27001) المختصة بإدارة امن المعلومات.

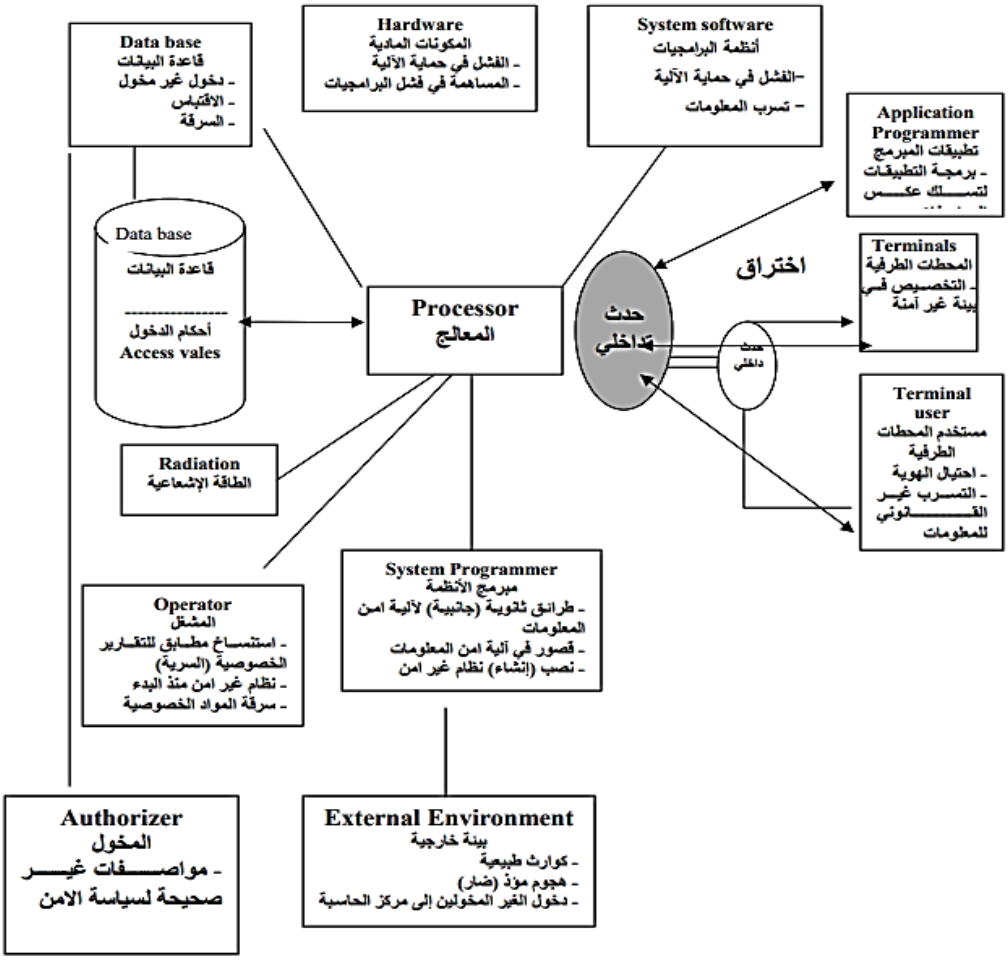
وبذلك قررت منظمة التقييس العالمية (ISO) واللجنة الفرعية المنبثقة عنها لتوحيد مواصفات أمن المعلومات في سلسلة ISO 2700X لعدد من المواصفات التي نشر بعضها ولا يزال بعضها الآخر قيد التطوير والتي تضم عدداً من المكونات الهيكلية الهامة[15]، إذ تركز هذه المكونات على المواصفات المرجعية الموحدة التي تصف متطلبات نظم إدارة أمن المعلومات (ISO27001) ومتطلبات جهات منح الشهادات (ISO 27006) للتوافق مع المواصفة بينما تقدم مواصفات أخرى ارشادات توجيهية في العديد من جوانب تطبيق مواصفات نظم إدارة أمن المعلومات (ISO/IEC 27000:2009) ، وتتضمن عائلة المواصفات القياسية(ISO2700X)المواصفات الآتية[16].

- ISO / IEC 27000: 2009 ، نظم إدارة أمن المعلومات - نظرة عامة والمفردات
- ISO / IEC 27001: 2005 ، نظم إدارة أمن المعلومات - المتطلبات
- ISO / IEC 27002:2005 ، مدونة قواعد الممارسة لإدارة أمن المعلومات
- ISO / IEC 27003: 2010 ، إرشادات تنفيذ نظام إدارة أمن المعلومات
- ISO / IEC 27004: 2009، إدارة أمن المعلومات - مقياس
- ISO / IEC 27005: 2011، إدارة مخاطر أمن المعلومات
- ISO / IEC 27006: 2011 متطلبات هيئات تقديم خدمات التدقيق ومنح الشهادات لنظم إدارة أمن المعلومات
- ISO / IEC 27007: 2011، مبادئ توجيهية لنظم إدارة التدقيق أمن المعلومات
- ISO / IEC 27008: 2011 ، مبادئ توجيهية للمدققين بشأن ضوابط أمن المعلومات
- ISO/IEC27010: 2012 ، إدارة أمن المعلومات للاتصالات بين القطاعات وبين المنظمات

المحور الثالث: مخاطر أمن المعلومات

تتعرض نظم أمن المعلومات التي تعتمد عليها المنظمات للعديد من التهديدات ويمثل التهديد الخطر المحتمل الذي يمكن أن يتعرض له نظام المعلومات وقد يكون شخصاً كالمتجسس أو المجرم المحترف أو الهاكرز المخترق أو شيئًا يهدد الأجهزة أو البرامج أو المعطيات أو حدثًا كالحريق ، وإنقطاع التيار الكهربائي ، والكوارث الطبيعية أن العدد الكبير من التهديدات المحتملة لأنظمة المعلومات أدى الى عدد كبير من الاستراتيجيات الدفاعية والأدوات[17] ، وان الدفاع عن انظمة المعلومات ليس بالمهمة السهلة وغير المكلفة للأسباب التالية:

1. الموارد الحاسوبية ربما تكون متواجدة في عدة مواقع .
2. شبكات المعلومات الحاسوبية يمكن أن تكون خارج المنظمة ومن الصعوبة حمايتها .
3. التغيرات التكنلوجية المتسارعة جعلت بعض الأجهزة الرقابية متقادمة حالما يتم نصبها .
4. العديد من جرائم الكمبيوتر لا يتم أكتشافها لفترات طويلة .
5. الافراد قد ينصرفوا الى انتهاك (اختراق) إجراءات الأمن لكونها غير ملائمة. فالعديد من مجرمي الكمبيوتر والذين تم امساكهم غالبا لم يعاقبوا على جرائمهم لذلك فهناك تأثير قليل لمنعهم أو ردعهم.
6. أن كمية المعرفة الحاسوبية الضرورية لمسك جرائم الحاسوب تكون قليلة.
7. أن تكاليف منع مصادر الخطر يمكن أن تكون غالية لذلك فإن معظم المنظمات ببساطة لا تستطيع وضع الإجراءات الأمنية الضرورية لكل مصادر الخطر المحتملة
8. من الصعوبة تحديد الكلفة - المنفعة (العائد) (cost-benft) للرقابة على المعلومات قبل حدوث الجرم مادام انه من الصعوبة تقديم تكاليف بالمحور الافتراضي.



ومن ابرز صور مخاطر أمن المعلومات ما يلي:

1. الاحتيال الحاسوبي :

تعتبر الأنظمة الحاسوبية أكثر عرضة لجرائم الأحتيال، لوجود ملايين من الأحرف المخزونة في قاعدة البيانات المشتركة . وبإمكان الأشخاص القادرين على الاختراق مثل هذه البيانات, أو تدمير أو تعديل كميات كبيرة من البيانات في وقتٍ قصير نسبيًا، ولكي تتمكن المنظمات من تحقيق أهدافها فأنها بحاجة إلى عددٍ كبيرٍ من الأشخاص القادرين على الدخول الى أنظمتها بمن فيهم الموردين والموظفين والعملاء .

أن أسهل الطرق شيوعًا لارتكاب الاحتيال الحاسوبي هي تعديل مدخلات الحاسوب وهذا يتطلب القليل من المهارات الحاسوبية حيث يحتاج مرتكبو الاحتيال فقط الى فهم معرفة كيفية تشغيل النظام الحاسوبي الأمر الذي يسمح لهم بإخفاء آثارهم.

لقد استخدم بو لسجيم (paulsjiem) تكنولوجيا النشر المكتبي لإنشاء شيكات مكتبية مزيفه أستخدمها في شراء معدات حاسوبية لبيعها وقبض ثمنها وقد قُبض عليه عندما هاجمه جهاز الأمن في شقته ووجد عنده تسع شيكات مزيفة تقدر قيمتها 150 ألف دولار وقد حوكم بسبب ذلك.

ومن الأمثلة الأخرى فتح محتال آخر حسابا في بنك نيويورك وكانت لدية طابعة من أجل تزوير فيش الايداع الفارغة المتشابهة لتلك الموجودة في البنك واستبدل جميع فيش الايداع الموجودة في ردهات البنك بتلك التي قام بتزويرها وقد دققت الايداعات التي تمت بواسطة الوصولات المزورة على حساب المحتال وبعد ثلاثة ايام حضره الى البنك وسحب المبلغ الموجود في حسابة وقد اختفى ولم يعثر عليه كونه استخدم هوية مزورة لم تكشف . وفي احتيالات الانفاق يقوم المحتال بجعل الشركة تدفع كثيرًا مقابل السلع المطلوبة او يجعلها تدفع سلع لم تطلبها أساسًا ومن الأمثلة على ذلك استخدم أحد المحتالين برنامج النشر المكتبي لتجهيز فواتير مزورة للتجهيزات المكتبية لم تطلبها الشركات من شركته ثم أرسل الفواتير للعديد من الشركات في جميع أنحاء البلاد وحافظ على ان تبقى قيم الفواتير اقل من 200 دولار كي لا تدقق الشركات في أمر الشراء ولكي لا تطلب المصادقة على صرف الفاتورة والغريب أن نسبة عالية من الشركات دفعت المبلغ دون أي سؤال. في احتيال المخزون يمكن أن يدخل المحتال الى النظام لكي يحول المخزون المسروق الى خردة وبذلك يتمكن من شطب سرقة المخزون كما لو قام عدد من الموظفين في سكة الحديد ما بإدخال البيانات الى نظام الشركة لإظهار أن أكثر من 200 سيارة من سيارات الشركة هي محطمة وملغاة ثم أزيلت هذه السيارات من خدمة الشركة وتم اعادة بيعها من جديد.

وفي احتيال تسليم النقدية يقوم المحتال بإخفاء السرقة عن طريق تزييف المدخلات للنظام ومن الامثلة على ذلك قام موظف شركة Arizona ببيع بطاقات بكامل السعر للعملاء وادخلها الى النظام بنصف السعر واحتفظ بنصف الآخر لنفسه.

ويمكن الاحتيال الحاسوبي عبر استخدام الأنظمة غير المصرح بها بما في ذلك سرقة خدمات ووقت الحاسوب، ومن هنا لا تسمح العديد من الشركات باستخدام الأنترنيت بصفة شخصية ويعد انتهاك سياسة من هذه السياسات احتيالاً، ولأن العديد من الناس لا ينظرون الى بأنه احتيال.

تمكن محاسبان من الدخول الى نظام سيسكو (نظام مسؤول على ادارة الاسهم) دون ان يكون لديهما الحق في ذلك وعملا على تحويل أكثر من (6.3) مليون دولار من اسهم سيسكو الى حساباتهم الشخصية لدى الوسيط ثم قاموا ببيع الاسهم واستخدموا جزء من الموال في شراء مستلزمات العيش المترف.

جدول (1) تقنيات احتيال واساءة المعاملة باستخدام الحاسوب

التقنية Technique	الوصف Description
البرمجيات الاعلانية Adware	استخدام البرمجيات للتجول على الويب ,وارسال البيانات الى المنظمات الاعلانية. عادة ما يتم ارسال مثل هذه البرمجيات بمعية البرمجيات المجانية والبرمجيات المشتركة التي يتم تحميلها من الانترنت ,وتسبب كذلك ظهور الاشرطة الاعلانية على شاشة الحاسب عند استخدام النت.
غش البيانات Data Didding	تغير البيانات قبل او اثناء او بعد ادخال البيانات الى النظام.
تسرب البيانات Data Leakage	نسخ بيانات الشركة مثل الملفات الحاسوبية بدون رخصة.
هجوم رفض الخدمة Denial _of_ Service Attack	ارسال مئات الرسائل الالكترونية في الثانية الواحدة من عناوين خاطئة بشكل عشوائي الذي يترتب عليه زيادة الحمل على خادم مزود خدمات الانترنت وبالتالي توقفه عن العمل.
هجوم العناوين Dictionary Attack	استخدام برمجيات خاصة من اجل التعرف على عناوين الشركات ومن ثم ارسال رسائل الالكترونية فارغة لها الرسائل غير الراجعة تشير الى عناوين صحيحة يمكن اضافتها الى قائمة العناوين الالكترونية.
التنصت Eavesdropping	الانصات الى صوت خاص او انتقال البيانات من خلال التنصت على خطوط الهاتف.
تزييف البريد الالكتروني E_mail Forgery	ارسال بريد الالكتروني بطريقة يظهر فيها وكانه مرسل من قبل شخص اخر.
تهديدات البريد الالكتروني E_mailthrets	ارسال رسالة تهديد عبر البريد الالكتروني ,وايهام مستلم الرسالة بان احد ما سيقوم بغشهم.
القرصنة Hacking	الدخول الى الانظمة الحاسوبية واستخدامها دون تصريح وعادة ما يتم ذلك بواسطة جهاز حاسب شخصي وشبكة اتصال.

الاختطاف Hijacking	السيطرة على جهاز الحاسوب الخاص بشخص اخر للقيام بأنشطة محظورة كإرسال دعاية دون علم مستخدم الحاسب.
سرقة الهوية Identity Theft	انتحال هوية شخص ما لتحقيق مكسب اقتصادي عادة بشكل غير قانونية من خلال الحصول على معلومات سرية مثل رقم الضمان الاجتماعي.
تضليل الانترنت Internet Misinforamtion	استخدام الانترنت من اجل نشر معلومات خاطئة او مضللة حول الناس او الشركات.
ارهاب الانترنت Internet Terrorism	استخدام الانترنت من اجل عرقلة التجارة الالكترونية او تحطيم اتصالات الافراد او الشركات .
القنبلة المنطقية الموقوتة Logic Bomb Time	تخريب النظام باستخدام برنامج يبقى معطل حتى يحدث امر معين فيوقت معين يجعله يعمل وعندها يتم تدمير البرامج او البيانات او كلاهما.
التنكر او التقليد Masquerading _Impersonation	الدخول الى النظام او التظاهر بامتلاك الصلاحية المقلد يتمتع بنفس امتياز المقلد.
التقاط حزم البيانات Packet Sniffing	استخدام الحاسوب لإيجاد الاسماء وكلمات السر عند انتقالها عبر الانترنت والشبكات الاخرى.
الكشف عن كلمة السر Password Cracking	اختراق دفاعات النظام وسرقة الملفات التي تحزي كلمات السر الصحيحة ومن ثم استخدامها في الدخول الى مصادر النظام مثل البرامج والملفات والبيانات.
انتحال اعتبارية الشركات لخداع الجمهور عبر الرسائل الالكترونية Phishing	ارسال الرسائل الالكترونية وكأنها رسائل صحيحة من الشركات ,والطلب من المستلم ان يذهب الى الموقع الالكتروني ليتحقق من او يملى البيانات المفقودة في سجل الشركة. وعادة ما تظهر الرسائل والمواقع الالكترونية وكأنها تعود للشركات حقيقية, في الغالب تكون شركات مالية.
قرصنة الهواتف Phishing	مهاجمة انظمة الهاتف واستخدام خطوط الهاتف لأرسال الفيروسات والدخول الى الانظمة وتدمير البيانات.
التسلسل والاختباء Piggybacking	الدخول الى خطوط الاتصالات والالتحام مع مستخدم شرعي قبل الدخول الى النظام. وهكذا يقوم المستخدم الشرعي بارتكاب جريمة دون ان يعرف.
التقريب Round _down	تقريب جميع الحسابات الفائدة الى اقرب مرتبتين عشريتين والكسر الباقي يوضع في حساب المحتال.

المصدر: أمن المعلومات، جامعة بابل، شبكة المعلومات الدولية (الانترنت)، على الرابط: https://www.uobabylon.edu.iq/e

2. **الفيروسات**

"تعد الفيروسات من أهم جرائم الحاسوب وأكثرها انتشارا في الوقت الحاضر، وتعريفها بأنها برنامج حاسوب له أهداف تدميرية يهدف إلى إحداث اضرار جسيمه بنظام الحاسوب سواءً بالبرامج أو في الأجهزة ويستطيع أن يعدل تركيب البرامج الأخرى حيث يرتبط بها ويعمل على تخريبها، فضلا عن كونه برنامج مكتوب بإحدى لغات البرمجة من قبل المبرمجين وهو قادر على التوالد والتناسخ ويستطيع الدخول إلى البرامج وله أفضلية أكبر من نظم التشغيل في فحص المكونات المادية مثل الذاكرة الرئيسية أو القرص المرن أو الليزري.

وإن التطورات الحاصلة في مجال إعداد برامج الفيروسات جعلت من الصعوبة إيجاد طريقة مضمونة بدرجة كبيرة للوقاية من الفيروسات ولكن هناك بعض الأساليب الفعالة التي يمكن إتباعها للحماية وهي[18]:

- تركيب برنامج مضاد للفيروسات ملائم لنظام التشغيل المستخدم في جهاز الحاسوب ويفضل أن يكون نسخة أصلية للاستفادة من الدعم الفني للشركات التي يتم شراء البرامج المضادة منها.
- عدم وضع برنامج جديد على جهاز الحاسوب إلا قبل اختباره والتأكد من خلوه من الفيروسات بواسطة برنامج مضاد للفيروسات.
- عدم استقبال أية ملفات من افراد مجهولي الهوية على الإنترنت.
- عمل نسخ احتياطية من الملفات الهامة وحفظها في مكان آمن.
- التأكد من نظافة اقراص الليزر التي يحمل منها نظام التشغيل الخاص بجهاز الحاسوب.

وفي نفس السياق هناك العديد من الأساليب التي يمكن إتباعها ومن شأنها أن تساهم في ضمان حماية أجهزة الحاسوب, ولكن يجب أن نضع نصب أعيننا ولا نتصور أن وجود برنامج مضاد للفيروسات محدث دائمًا في أجهزة الحاسوب يعني أننا في مأمن من الفيروسات، كما أن أي مشكلة في الأجهزة لا تعني دائما أن هناك فيروسًا، لذا يجب تحديد سبب المشكلة ومحاولة إيجاد العلاج لها[19].

3. **قرصنة المعلومات**

هو ما يعرف بـ(الها كرز أو مخترقي الأجهزة) ونتساءل كيف يتم ذلك وهل الأمر بسيط إلى هذا الحد أم يحتاج لدراسة وجهد، في الحقيقة أنه مع انتشار برامج القرصنة ووجودها في الكثير من المواقع أصبح من الممكن اختراق أي جهاز حاسوب وبدون عناء فور انزال إحدى برامج القرصنة. والمقصود بالقرصنة، سرقة المعلومات من برامج وبيانات بصورة غير شرعية وهي مخزونة في ذاكرة الحاسوب أو نسخ برامج معلوماتية بصورة غير قانونية وتتم هذه العملية أما بالحصول على كلمة السر أو بواسطة التقاط موجات كهرومغناطيسية بحاسبة خاصة ويمكن إجراء عملية القرصنة بواسطة رشوة العاملين في المنظمات المنافسة.

أما عن الهدف من عمليات القرصنة فهو سرقة الأسرار أو المعلومات التجارية أو التسويقية أو التعرف على حسابات المنظمات أو أحيانًا بهدف التلاعب بقيود المصارف أو المؤسسات المالية بهدف سرقة الأموال أو يكون الهدف الكشف عن اسرار صناعية (تصاميم منتجات) بهدف إعادة تصنيعها دون إجازة قانونية أو لأهداف سياسية وعسكرية من أجل الحصول على الملفات والخطط السرية العسكرية أو الحكومية.

المحور الرابع: التدابير المعاصرة لأمن المعلومات

وسائل أمن المعلومات هي مجموعة من الآليات والإجراءات والأدوات والمنتجات التي تستخدم للوقاية من أو تقليل المخاطر والتهديدات التي تتعرض لها الكمبيوترات والشبكات وبالعموم نظم المعلومات وقواعدها. وكما أوضحنا، فإن وسائل الأمن متعددة من حيث الطبيعة والغرض ، لكن يمكننا بشكل أساسي تصنيف هذه الوسائل في ضوء غرض الحماية الى الطوائف التالية[20] :-

1. **مجموعة وسائل الأمن المتعلقة بالتعريف بشخص المستخدم وموثوقية الاستخدام ومشروعيته:** وهي الوسائل التي تهدف الى ضمان استخدام النظام أو الشبكة من قبل الشخص المخول بهذا الاستخدام، وتضم هذه الطائفة كلمات السر بأنواعها، والبطاقات الذكية المستخدمة للتعريف ، ووسائل التعريف البيولوجية التي تعتمد على سمات معينة في شخص المستخدم متصلة ببنائه البيولوجي، ومختلف أنواع المنتجات التي تزود كلمات سر آنية أو وقتية متغيرة الكترونيًا، والمفاتيح المشفرة، بل تضم هذه الطائفة ما يعرف بالأقفال الإلكترونية التي تحدد مناطق النفاذ.

2. **مجموعة الوسائل المتعلقة بالتحكم بالدخول والنفاذ الى الشبكة Access control** وهي التي تساعد في التأكد من أن الشبكة ومصادرها قد استخدمت بطريقة مشروعة ، وتشمل من بين ما تشمل الوسائل التي تعتمد على تحديد حقوق المستخدمين ، او قوائم اشخاص المستخدمين أنفسهم ، أو تحديد المزايا الاستخدامية أو غير ذلك من الإجراءات والادوات والوسائل التي تتيح التحكم بمشروعية استخدام الشبكة ابتداءً.
3. **مجموعة الوسائل التي تهدف الى منع افشاء المعلومات لغير المخولين بذلك وتهدف الى تحقيق سرية المعلومات** Data and message confidentiality ، وتشمل هذه الوسائل من بين ما تشمل تقنيات تشفير المعطيات والملفات message encryption وإجراءات حماية نسخ الحفظ protection for backup copies on file and والحماية المادة للأجهزة technology, physical protection of الاحتياطية ومكونات الشبكات physical LAN medium and ,tapes diskettes, etc واستخدام الفلترات والموجهات devices.
4. **مجموعة الوسائل الهادفة لحماية التكاملية (سلامة المحتوى)** وهي الوسائل المناط بها ضمان عدم تعديل محتوى المعطيات من قبل جهة غير مخولة بذلك ، وتشمل من بين ما تشمل تقنيات الترميز والتواقيع الإلكترونية وبرمجيات تحري الفايروسات وغيرها .
5. **مجموعة الوسائل المتعلقة بمنع الإنكار (إنكار التصرفات الصادرة عن الشخص) - Non repudiation**، وتهدف هذه الوسائل الى ضمان عدم قدرة شخص المستخدم من إنكار أنه هو الذي قام بالتصرف، وهي وسائل ذات أهمية بالغة في بيئة الاعمال الإلكترونية والتعاقدات على الخط، وترتكز هذه الوسائل في الوقت الحاضر على تقنيات التوقيع الإلكتروني وشهادات التوثيق الصادرة عن طرف ثالث.
6. **وسائل مراقبة الاستخدام وتتبع سجلات النفاذ أو الأداء (الاستخدام) Logging and Monitoring** ، وهي التقنيات التي تستخدم لمراقبة العاملين على النظام لتحديد الشخص الذي قام بالعمل المعين في وقت معين ، وتشمل كافة أنواع البرمجيات والسجلات الإلكترونية التي تحدد الاستخدام.
7. **برمجيات كشف ومقاومة الفايروسات:** بالرغم من أن تقنيات مضادات الفيروسات تعد الأكثر انتشارًا وتعد من بين وسائل الأمن المعروفة للعموم ، الا أن حجم تطبيق

هذه التقنيات واستراتيجيات وخطة التعامل معها تكشف عن ثغرات كبيرة وعن أخطاء في فهم دور هذه المضادات ، وبالعموم ثمة خمسة آليات أساسية لكيفية تحري هذه المضادات للفيروسات التي تصيب النظام ، كما ثمة قواعد أساسية تحقق فعالية هذه الوسائل والتي تعتمد في حقيقتها على الموازنة ما بين ضرورات هذه التقنيات لحماية النظام وما قد يؤثره الاستخدام الخاطئ لها على الأداء وفعالية النظام.

8. **توثيق صحة البيانات ومصدرها (التوقيع الإلكتروني والشهادات الإلكترونية): إن** التبادل الالكتروني الأمن على الانترنت يتطلب وجود طريقة نتأكد منها من شخصية الطرف الذي نتصل به ومن أن الرسائل التي تستقبلها منه قادمة بالفعل منه وأنها ليست رسائل مزورة، والتقنية المستخدمة لتحقيق ذلك تسمى التوقيع الإلكتروني (Digital Signing)، ففي التوقيع الالكتروني، يقوم المزود الذي سيقوم بإرسال رسالة ما للزبون بغض النظر عن حالة الرسالة من حيث كونها مشفرة أو لا بتشفير هذه الرسالة النهائية مرة أخيرة باستخدام المفتاح الخاص به، وعندما تصل الرسالة إلى الزبون فإنه يقوم بفك تشفيرها باستخدام المفتاح العلني للمزود، فإذا نتج عن فك تشفير هذه الرسالة النتيجة التي يتوقعها الزبون فإنه يعلم بأن المزود هو بالفعل مصدر هذه الرسالة، فنلاحظ هنا بأننا نقوم بعملية عكسية، فبدلا من أن تشفر الرسالة بالمفتاح العلني وترسلها للمزود، بحيث لا يتمكن أحد من فكها إلا المزود، فإن المزود يقوم هو بتشفيرها بمفتاحه الخاص، ويرسلها إلى الزبون، بحيث يتمكن أي شخص من فك تشفير الرسالة باستخدام المفتاح العلني للمزود، لكن المزود وحده فقط يكون قادرا على تشفيرها باستخدام المفتاح الخاص لأنه وحده الذي يملك المفتاح الخاص، وبالتالي نكون متأكدين من أن الرسائل التي تقبل فك التشفير باستخدام المفتاح العلني للمزود هي رسائل مرسلة من المزود نفسه، ونلاحظ أيضًا بأن الرسائل في هذه الحالة تكون عادة مشفرة مرتين، في المرة الأولى تشعر الرسالة الأصلية المحتوية على المعلومات الحساسة بالمفتاح العلني للزبون حتى لا يتمكن أحد من فك تشفيرها سوى الزبون، وتشعر بعد ذلك هذه الرسالة المشفرة نفسها مرة أخرى باستخدام المفتاح الخاص للمزود ليثبت للزبون بأنه هو الذي قام بارسال الرسالة وذلك بأنها تقبل فك

التشفير بالمفتاح العلني للمزود. خوارزمية ال ار اس انه RSA في علم التشفير RSA ليونارد أديمان وادي شامير ورون ريفيست هي قاعدة للتشفير بواسطة مفتاح عام.

كانت القاعدة الأولى المعروفة بكونها مناسبة للتوقيع بالإضافة إلى تشفير، وكانت أحد التقدمات العظيمة الأولى في التشفير بواسطة مفتاح عام أر إس إيه مستخدم في بروتوكولات التجارة الإلكترونية على نطاق واسع، ويعتقد أن تكون مضمونة على اعتبار انه يوجد مفاتيح طويلة بشكل كافي واستعمال أحدث التطبيقات.

ملاحظات ختامية وتوصيات

من خلال البحث في أمن المعلومات الرقمية وتتبع المخاطر التي يتعرض لها، خرجت الدراسة بعدة نتائج هامة يمكن إيجازها في النقاط التالية:

1. إن أمن المعلومات كمصطلح يرتبط بمفهوم الأمن المعلوماتي الذي يعني ضرورة إحساس أفراد المجتمع بعدم وجود إي شكل من أشكال التهديدات لبنى المؤسسات المعلوماتية، وضرورة اتخاذ الاحتياطات كافة للتأهب والعمل الفعلي لمواجهة هذه التهديدات، سواء أكان مصدرها داخليا أم خارجيا.
2. التطور السريع للأساليب والتقنيات المستخدمة في الجرائم الإلكترونية مما يصعب من مهمة شركات البرمجيات المضادة للفيروسات، ووضع ضغوط مستمرة على الهيئات التشريعية.
3. أن أمن المعلومات يقتضي حماية جميع أنواع المعلومات ومصادر الأدوات التي تتعامل معها وتعالجها من التجهيزات الحاسوبية وغير الحاسوبية المتصلة بها بإتباع إجراءات وقائية محددة تكفل المحافظة عليها وحمايتها من الأخطار التي قد تتعرض لها، سواء أكان ذلك من حيث الأمن المادي لمراكز المعلومات أم من حيث امن البرمجيات أم من حيث الأفراد العاملين في مراكز المعلومات.
4. أن القوانين المتبعة في حماية أمن المعلومات الرقمية تبطئ من عمل المديرون في أمن المعلومات لعدم مواكبتها للأساليب الحديثة المتبعة في الهجمات الإلكترونية لأنها ليست فعاله بالشكل الكافي، وتفتقر إلى آلية التطبيق نظراً لتنوع هذه الهجمات وتطورها المستمر.
5. يحتل الحفاظ على امن المعلومات بعناصره الرئيسية المذكورة في البحث أهمية كبيرة في الواقع العملي نتيجة لازدياد اعتماد الدول والمؤسسات الرسمية وغير الرسمية والأفراد في تعاملاتهم على المعلومات الإلكترونية.

6. يتعرض أمن المعلومات للعديد من المخاطر والتهديدات التي تتم في بيئة الإنترنت مع عدم مواكبة التدابير التقنية المضادة لسرعة تطور الطرق الحديثة المستخدمة في عمليات الاعتداءات على أمن المعلومات.

خرجت الورقة بعدة توصيات من خلال دراسة أمن المعلومات من الجانب التقني في البيئة الرقمية وما تتعرض له من جرائم بالإضافة إلى دراسة بعض التدابير اللازمة للحد من هذه الجرائم، وهي كالتالي:

1. ضرورة تدريب العاملين داخل نظام أمن المعلومات والقيام بالعديد من الدورات التي تنمي مهاراتهم وقدراتهم المعرفية والتقنية في مجال أمن المعلومات.
2. استحداث أقسام أو وحدات إدارية مستقلة في دوائر الدولة ومؤسساتها المختلفة تتولى مهمة اتخاذ الإجراءات اللازمة لحماية المعلومات الإلكترونية والمحافظة على أمنها، ورفدها بالكوادر المدربة والمتخصصة في هذا المجال وعقد الندوات وورش العمل في دوائر الدولة ومؤسساتها المختلفة لتعريف الموظفين والعاملين فيها بضرورة المحافظة على امن المعلومات وسلامة الحواسيب
3. ضرورة توحيد الجهود على المستوى الدولي لعمل تشريع موحد يظهر فيه بشكل واضح العقوبات المناسبة لمرتكبي جرائم المعلومات.

المصادر والمراجع:

[1]- المعلومات العالمية. علاء، الكيلاني، عثمان، البياتي، هلال، المعلومات الإدارية "، دار المناهج للنشر والتوزيع، الاردن "، (٢٠١٢)، اساسيات نظم.

[2]- الطائي ، محمد عبد حسين ، نظم المعلومات الادارية ، الطبعة الثانية ، وزارة التعليم العالي والبحث العلمي ، دار الكتب والطباعة والنشر ، موصل ، 2000 .

[3] - الطائي، يوسف حجيم ، العجيلي محمد عاصي والحكيم، ليث علي (2009) . نظم ادارة الجودة في المنظمات الانتاجية والخدمية دار اليازوري العلمية للنشر والتوزيع، عمان الاردن .

[4] - Gelbstein, Eduardo and Kamal, Ahmed, Information security, Asurvival Guide to the uncharted Territories of cyber, New York , UN ICT, 2005.

[5] - السالمي ، علاء عبد الرزاق ، تكنولوجيا المعلومات ، الطبعة الثالثة ، دار المناهج للتوزيع والنشر، الاردن، ص2000

[6] -O'Brien James A, management Information system Amanagemerial End user Perspective, IRWIN, 1990.

[7] - Arnason, Sigurjon Thor & Willett, Keith D. (2008)," How to Achieve 27001 Certification: An Example of Applied Compliance Management", USA:Taylor & Francis Group, LLC

[8] - العامري ، اسامة (2010) اتجاهات ادارة المعلومات الأردن ، عمان ، دار اسامة للنشر والتوزيع.

[9] - القحطاني، منصور بن سعيد (٢٠٠٨)، تهديدات الامن المعلوماتي وسبل مواجهتها دراسة مسحية لمنسوبي مركز الحاسوب الآلي بالقوات البحرية الملكية السعودية بالرياض، جامعة نايف للعلوم الأمنية السعودية، الرياض .

[10] John M. Broky, Thomas H. Bradley. Protecting Information with Cybersecurity, Berlin: Springer International Publishing AG, 2019, Pp. 350- 351, Available At: http://08102q3xn.1104.y.https.link.springer.com.mplbci.ekb.eg/content/pdf, Access Date: (15/4/2024).

[11] -Singh, A., Vaish, A., Keserwani, P. (2014). Information Security: Components and Techniques. In International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, No.1, pp: 1072-1077

[12] - Arnason, Sigurjon Thor & Willett, Keith D. (2008)," How to Achieve 27001 Certification: An Example of Applied Compliance Management", USA:Taylor & Francis Group, LLC

[13] -ISO/IEC 27002:2013" Information technology Security techniques Code of practice for information security controls"

[14] -MacLennan A. Information Governance and Assurance, International Journal of Information Management, Vol. 35, London: Elsevier Fact Publisher, 2015, P. 174, Available At: https://081010y2c-1105-y-https-ac-els--cdn- com.mplbci.ekb.eg, Access Date: (19/4/2024).

[15] - الطائي، يوسف حجيم ، العجيلي ، محمد عاصي والحكيم، ليث علي (2009) . نظم ادارة الجودة في المنظمات الانتاجية والخدمية دار اليازوري العلمية للنشر والتوزيع، عمان الأردن.

[16]- أحمد عبادة العربي معيار المنظمة الدولية للتوحيد القياسي أيزو 27002 لسياسات أمن المعلومات دراسة وصفية تحليلية لمواقع الجامعات المصرية، مجلة جامعة طيبة للآداب والعلوم الإنسانية، مج 4 ، ع 7 ، ص 663، متاح على: http://search.mandumah.com/Record/773513 تاريخ الاطلاع 2024/4/20

[17] - Turban, Efraim and Mcler, Ephraim, and wetherbe James, Information Technology for management, making connection for strateglc Advatage, 2nded, John Wiley & sons. INC. 1999.

[18] - فادية عبد الرحمن خالد سياسة أمن المعلومات في المكتبات ومراكز المعلومات المجلة الأردنية للمكتبات والمعلومات، مج 52، ع 4 ، 2017، ص 74، متاح على: http://content.ebscohost.com/ContentServer.asp: تاريخ الاطلاع 17/4/2024.

[19] - صحوه صلاح عبد الرازق التخطيط الاستراتيجي لأمن المعلومات، أطروحة ماجستير) جامعة أم درمان معهد البحوث والدراسات الاستراتيجية 2017، ص 35، متاح على: http://search.mandumah.com/Record/858537 تاريخ الاطلاع : 2024/4/20.

[20] - جبوري ، ندى اسماعيل (2011). حماية امن انظمة المعلومات : دراسة حالة في مصرف الرافدين فرع شارع فلسطين . مجلة تكريت للعلوم الادارية والاقتصادية (7 (21) 72-91 ، جامعة تكريت للعلوم الإدارية والاقتصادية، تكريت ، العراق.

عروض
الكتب والدراسات

- دور الأسرة العراقية في تعزيز الأمن المجتمعي في ظل التحديات المعاصرة (الواقع والمأمول).

تأليف: الفريق الدكتور ثامر محمد الحسيني عرض بقلم: الحقوقي: محمود محمد محمد

- حرب الفضاء الالكتروني التهديد التالي للأمن القومي وكيفية التعامل معه.

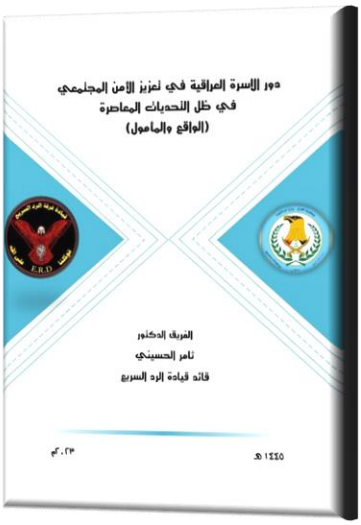
تأليف: ريتشارد كلارك وروبرت نيل عرض بقلم: م.م. اوس رحيم عبد القهار

- التطرف من "إدارة التوحش" الى "فقه الدماء" في التمرد الفكري والجغرافي للقاعدة وداعش.

تأليف: د. علي احمد عبد مرزوك عرض بقلم: م.م. حسين محمد البياتي

دور الأسرة العراقية في تعزيز الأمن المجتمعي
في ظل التحديات المعاصرة (الواقع والمأمول)

تأليف: الفريق الدكتور ثامر محمد الحسيني
عرض بقلم
الحقوقي/ محمود محمد محمد
قيادة فرقة الرد السريع



إنَّ عَرض هَذه اَلدِّرَاسَة يَنصَبُّ عَلَى تَجرِيدِهَا من اَلأَفكَارِ اَلفَرعِيَّة، وَالغَورُ فِي مَكنُونَاتِهَا اَلأَسَاسِيَّة، لِتَقدِيم مُختَصَر غَير مُبتَسَر عَن اَلأَفكَار اَلرَّئِيسَة اَلوَارِدَة بَينَ أَروِقَة صَفَحَاتِهَا، بُغيَةَ مُسَاعَدَة اَلقَارِئ عَلَى فَهمِ جَوهَر اَلدِّرَاسَة وَمَغزَاهَا، وَالإِلمَامُ بِأَجزَائِهَا اَلرَّئِيسَة، اَلَّتِي يَرغَبُ من خِلَالِهَا اَلمُؤَلِّفُ بِإِيصَالِ اَلفِكرَة اَلأَسَاسِيَّة لِلمُطَالِع اَلنَّهم وَمِن دُونِ تَشوِيهٍ لِلفِكرَةِ اَلأَسَاسِيَّة اَلَّتِي تبنَّاها الكاتب.

إنَّ متن هذا الكتاب يتمحور حول تكوين المجتمع ونشأته وتأطير الدّعائم اللّازمة لإسعاف سُلوكيّاته، مُؤيدًا فكرة أنَّ الإنسان ليس ابن بيئته بل ابن تعبئته فالبيئة المتمثلة بالأسرة ابتداءً، هي المُعبأ الأوّل لسواقي الفرد، فإن سُقي صلاحًا، صلح ضِلعٌ في المجتمع الذي هُو عُنصرٌ من عناصِره، وركيزة يُعوّل عليها في بناء مُجتمع يسودهُ الأمن أو العكس، وأنَّ مُلئ سُمًّا كان وُجودهُ داءً وعبئًا على من يقطُن وإيّاه على ذات الرقعة الجغرافية.

تعرِض أسطر هذا المؤلف دور الأُسرة وتحدّياتها المعاصرة الهادفة لتحقيق الأمن والاستقرار في المجتمع، متناولًا في نُصوصه تعريفات مُختلفة عن الأُسرة والعائلة من الجوانب العرفيّة ولاسيّما التّاريخيّة والمعاصرة منها، ويوضّح أنّ الأُسرة أساس المجتمع وأنّ تحقيق الأمن المجتمعيّ يتطلّب دعم دورها ووضع سياسات تُحفزها على القيام بوظائفها بشكلٍ فعّال. وقد

الاستلام 2024/01/04
الارجاع 2024/04/07
القبول 2024/05/15

استخدِم النّص مُصطلحاتٌ عِدّة مزودة بتبيان أوجه الفرق فيما بينها، شارحًا التّحدّيات التِي تُواجِه الأُسرة فِي القرن الحالِيّ.

تبجيل وتعظيم وتكرِيم المرأة فِي الإسلام، إذ يُبيّن الكيفيّة التِي رفع الإسلام بِها مكانة المرأة وأكرمها بِما لم يُكرمها أحد من دعاة الحرية وعباد الدرهم والدينار، حيث إن الغرب الديمقراطي ينقم على المرأة المسلمة في ظل ما أعطاها الإسلام من منـزلة رفيعة، ويريد أن يفسدها حتى يفسد حياة المسلمين ويوهنها، وذلِك بِإعطائها حقّ الرّضاعة والرِّعاية.. فكرمها زوجةً، إذ أوصى بها الأزواج خيرًا، وأمر بالإحسان في عشرتها وأخبر أن لها من الحق مثلما للزوج إلا أنه يزيد عليها درجة، لمسئوليته في الإنفاق والقيام على شئون الأسرة، وبين أن خير المسلمين أفضلُهم تعاملًا مع زوجته، وحرم أخذ مالها بغير رضاها، فضلا عن حمايتها مِن أيدِي السُّوء والأذى.. إلخ من المكارم التي خُصت بها، ويسلِّط الكاتب الضّوء أيضًا على ضرورة تكرِيم الأبناء فِي الإسلام مُبينًا إيجابيّات ذلِك السُّلوك، إذ يتحدّث عن حُقوقِهم فِي التّسمية الحسنة والحنان والرِّعاية والتّعليم والاهتمام بِمستقبلهم وغير ذلك.

ويشرح كذلِك حقّ الرّضاعة الذِي منحه الإسلام لِلرُّضّع بِأن يرضعوا مِن اِمرأة أُخرى غير أُمّهم، مِمّا يُؤكّد على قِيمة الحماية والرِّعاية التِي يمنحها الإسلام لِإحدى أهمّ الركائز القائم عليها المجتمع، كما يتحدّث الكتّاب عن التّحدّيات التِي تُواجِه الأُسرة فِي المجتمع العراقِيّ، فمن نافلة القول، أن الأُسرة تُواجِه العدِيد مِن التّحدّيات الاجتماعيّة، بِما فِي ذلِك تحدّي الدّور والعلاقات الأسريّة والتّوافق والنّمط الثّقافِيّ، ويُبيّن النّص أنّ هذِه التّحدّيات قد تُؤثّر على العلاقات الأسريّة وتسبّب الضّغط والتّوتُّر، وأنّ التّحدّيات المجتمعيّة تزداد تعقيدًا وتفاوتًا مِن مُجتمعٍ لِآخر، ويركّز بِشكل خاصّ على تحدّيات العلاقات الأسريّة واختلاف التّوقُّعات بين الأفراد وتأثِير المتغيّرات الثّقافيّة والاجتماعيّة على العلاقات الأسريّة، وقد تناول الكتّاب تأثِير العوامل الاجتماعيّة والسِّياسيّة والاقتصاديّة على العائلة الرِّيفيّة فِي المجتمع العراقِيّ، منبهًا للالتفات للحُروب وأهميّة تأثيرها على المجتمع والعائلة فِي الرِّيف. ويشير النّص إلى أنّ التّغيرات الاجتماعيّة والاقتصاديّة قد تسببت فِي نُزُوح سُكّان الرِّيف وهجرتهم إلى المدينة، الأمر الذي أثّر على التّواصل الاجتماعِيّ والعلاقات الأسريّة والأعراف والعادات فِي الرِّيف.

وأورد الكتّاب بِشكلٍ عامّ أهمّ مسببات التأثير على العائلة الرِّيفيّة، مؤكدًا على أنّ تلك المسببات تُشكّل تحدّياتٍ جدِيدة تُواجِه العائلة فِي المجتمع العراقِيّ، كما تناول المؤلف موضوع

يعد رأسًا لِهرم ما كتب وأوجد، ألا وهو أهميّة التّعليم فِي المجتمع العراقيّ وتأثيره الاجتماعيّ والثّقافيّ والاقتصاديّ والنّفسيّ، مُشيرًا إلى أنّ التّعليم يُمثّل تحدّيًا كبيرًا فِي الرّيف بِسبب تفاوُت الفُرص التّعليميّة لِأفراده ولاسيّما الفتيات مِنه، عِلاوة على التّحدّيات التّقليديّة التِي تُواجِه المرأة فِي المجتمع الرّيفيّ، مؤكدًا على أنّ دعم منظُومة التّعليم تُساعِد على تحقِيق وتعزِيز وعي الأفراد والمجتمع فضلا عن تحسِين جودة الحياة العائليّة بِصورة عامّة والرّيفيّة بِصورة خاصّة، كما أشاره إلى أنّ التّغيُّرات الاجتماعيّة والاقتصاديّة فِي المجتمع العراقيّ جرّاء ظاهِرة العولمة قد تسببت بِتحدّيات جدِيدة تُؤثّر على العائلة الرّيفيّة فِي التّواصل بِشتى المجالات. وأكّد أيضًا على أهميّة الخدمات الصّحّيّة فِي المجتمعات الرّيفيّة وضرورة توفيرها لِحلّ المشكلات الصّحّيّة التِي تُواجهها تِلك المجتمعات البائسة. وأشاد بأمرٍ ذِي أهميّة جوهرِية، ألّا وهُو شبكة النّقل الرّيفيّة لِتسهِيل الاتّصال بِالمدن والمراكز وتيسِير نقل الخدمات الزّراعيّة إلى إليها، فضلًا عن ذِكره لِأهمّيّة وسائِل الإعلام والاتّصال فِي تغيِير سُلوكيّات المجتمع الرّيفيّ اِبتِغاء تحريرها مِن القيم العشائريّة القديمة البالية المؤدّية إلى الرُّكون والرُّكود فِي قاع التّخلُّف المدقع.

تناوُل الكاتب أيضًا جانبًا فِي غاية الأهمّيّة، ألّا وهُو التّفكُّك الأُسري الواقع نتِيجة تهالُك الرّوابط العائليّة النّاجمة عن التّأثُّر بِالعلاقات الزّوجيّة المفضية بِدورِها إلى قطع صِلة الرحِم الأسريّة مُحولةً سُلوكيّاتها الحميدة إلى طِباع عدائِية، وقد ذكر مُؤلفنا جُملة مِن العوامل تقُود إلى حُدُوث ذلِك التّفكُّك ولعل مِن أبرزِها: عدم وُضُوح الأدوار، وسُوء التّوافق بين الأزواج، مُضافا إليها داء الخلافات بين أفراد الأُسرة والذِي يقُود بِدوره لِلتّأثير سلبًا على الصّحّة النّفسيّة لِكلّ فرد مِن أفرادها، فضلا عن آثاره المؤدّية إلى عدم اِستقرار الأُسرة ككُل، كما أفاد النّص إلى أنّ التّفكُّك الأُسري يُمكِن أن ينتج عنه الانحراف والجرِيمة زِيادةً على إضعاف العلاقة بين الأبناء النّاجمة عن الخلافات، لِذلك يجِب على الأزواج توضِيح الأدوار وتحدِيد الأهداف المشتركة وتحسِين العلاقة بينهما مِن أجل الحفاظ على اِستقرار الأُسرة وعدم اِنهيارها.

تحكِي النصوص عن أثر سُقُوط النّظام المنحل فِي العراق عام (2003) على المؤسّسات الدُّستوريّة والسِّياسيّة والإداريّة، مُشيرًا إلى إن اِنهِيار السُّلطة نتج عنه انجمادًا كُلِّيًّا لِمؤسّسات الضّبط والرّقابة، وهذا يعنِي أنّه لا يُوجد أيُّ سُلطة قادِرة على بِناء المجتمع وتحسِين الظُّروف المعيشيّة لِلأفراد، وبالتّالي تولدت اِضطرابات اِجتماعيّة وتدهور فِي العلاقات بين الأفراد

وزيادة الجريمة بشكلٍ ملحوظ، وحتّى إن تمّ إنشاء مُؤسسات بدِيلة لِإدارة الدّولة، فإنّه سيكُون هُناك صُعُوبة فِي إعادة بِناء الثقة والاستقرار الاجتماعيّ.

يُعانِي العراق مِن مشاكِل اِقتصاديّة نتِيجة لِعدّة عوامِل عدِيدة ومِن جُملتِها سُوء توزِيع وهزل الإدارة للموارد الاقتصاديّة، ومهاترات ومناعرات النِّظام المُنحل التِي مُنِيّ العراق على إثرها بفرض عقوبات دّوليّة عليه، والتي لا زلنا ندفع ثمن آثارها إلى الآن، حيث بعد سُقُوط النِّظام المُنحل، تفاقمت المشاكل الاقتصاديّة فِي العراق جرّاء عدم الاستقرار السِّياسيّ والفساد وغياب سُلطة الضّبط الرِّقابيّ، الأمر الذِي أدّى إلى زِيادة المديونيّة والفقر المدقع والتّضخُّم وتدهور الخدمات العامّة.

إنّ مُشكلة النّازحين فِي العراق تُشكّل ظاهِرة مُتجددة ترجع إلى عوامِل عِدّة، مِن بينها الفساد الإداريّ والماليُّ، ويتجسّد هذا الفساد فِي عِدّة مظاهِر، كالاستغلال السِّياسيّ لِلموارد الوطنيّة، والتّلاعب فِي العُقود الحكوميّة، وتحوِيل أموال الدّولة وغيرِها، ويؤكّد الكتّاب على إن النِّزاعات السِّياسيّة والمنافرات الطّائفيّة والعرقيّة والثّقافيّة المتزايدة بِشكل مطرد، أدّت إلى اِنفِصال النّاس عن الهوِية الوطنيّة وتعلُّقهم بِالهويّات الفرعيّة، وقد اِستغلّت جِهات داخلِية وخارجيّة هذا الانفصال لِتحقِيق أهداف سِياسِيّة وأمنِية تصب لصالحها، ولتحقيق الوحدة الوطنيّة، يجِب على الدّولة العراقيّة بذل مزيد مِن الجُهود فِي تحدِيث القيم الوطنيّة وتوفِير بِيئة تُشجّع على الالتزام بِالمواطنة والهويّة الوطنيّة، مع اِحترام التّنوُّع الثّقافيّ والدِّينيّ والعرقيّ.

خِتامًا، أشاد كاتِب هذِه الدِّراسة بِأهمِّيّة دور المُثقف فِي المجتمع وضرورة اِندِماج وظيفته المعرفيّة مع وظيفته الاجتماعيّة، وكيف أنّ ضعف الطّبقة المثقّفة أدّى إلى ضعف دور النُّخب الثّقافيّة وتحوُّلها إلى مُوظّفِين بِسبب تدهور الأوضاع الاقتصاديّة، داعيًا إلى ضرُورة تشكِيل تكتُّل نخبوِي يُشكّل جماعات ضغط ذات قِيم وأهداف مُشتركة لِلمساهمة فِي تغيِير الواقع المرير.

حرب الفضاء الالكتروني
التهديد التالي للأمن القومي وكيفية التعامل معه

تأليف: ريتشارد كلارك وروبرت نيل
عرض بقلم
م.م. أوس رحيم عبد القهار
قيادة فرقة الرد السريع

إن ما يدور في العالم اليوم وما تجري من صراعات متواترة وعلى كافة الأصعدة السياسية والعسكرية والاقتصادي وايضا على الصعيد الاجتماعي، وعلى مختلف مسميات الحروب التي تنتهجها الدول المتقدمة من أجل فرض الهيمنة والقوة وتحقيق الأهداف بأفضل الأساليب المبتكرة والحديثة.

إذ يتمحور كتاب حرب الفضاء الالكترونية تكملة لما قام به الكاتب البروفيسور ويليام كاوفان في مجال حرب الفضاء الالكتروني الذي توفي عن عمر ناهز التسعين عاما.

أن أول من قام باستخدام حرب الفضاء الالكتروني الولايات المتحدة الامريكية في العقد الأول من القرن الحادي والعشرين حيث قامت بتطوير نوع جديد من الأسلحة، وبدأت في استخدامه بصورة منهجية اعتماداً على تقنيات جديدة من دون أن تركن إلى استراتيجية رصينة؛ فأنشأ قيادة عسكرية جديدة للخوض في نوع جديد من الحروب باستخدام أحدث التقنيات، لكن بلا حوار عام ومن دون مناقشات إعلامية أو رقابة جادة من جانب الكونجرس ولا تحليلات أكاديمية ولا حوار دولي. ولعلنا اليوم في زمن يشبه! إلى حد مدهش الخمسينيات من القرن العشرين؛ ولذلك قد تكون بحاجة إلى إجراء المناقشات

الاستلام 2024/02/07
الارجاع 2024/04/10
القبول 2024/05/01

المدروسة والتحليلات الدقيقة لهذا النوع الجديد من الأسلحة، وهذا النوع الجديد من الحروب.

تضمن الفصل الأول من الكتاب هجمات حرب الفضاء الالكترونية وهي كالتالي:

اولاً: تفجير موقع على ضفاف الفرات في سوريا وفجأة ودون سابق إنذار ظهر فوق الموقع شيء يشبه النجيمات، فأضاء المنطقة بضوء أبيض ضارب للزرقة أقوى من ضوء النهار، وفي أقل من دقيقة واحدة، بدت دهراً لنفرٍ من السوريين والكوريين كانوا لايزالون بالموقع، برق وميض ساطع يعمي الأبصار، تبعته موجة ارتجاجية صوتية عنيفة، ثم انهمر فوق رؤوسهم حطام متناثر، ولو لم تكن الانفجارات قد شلت أسماعهم شللاً مؤقتاً لكان كل من على الأرض على مقربة من المكان قد سمع ضجيجاً طويلاً صادراً من محركات الطائرات العسكرية النفاثة التي غطت سماء المنطقة. ولو استطاع أحد من السوريين أو الكوريين أن يرى ما وراء ألسنة اللهب التي اندلعت في موقع البناء أو ما فوق مقذوفات الإثارة التي تهبط بمظلات صغيرة لشاهدوا طائرات "إيجل إف 15" و "فالكون إف 16" تنحرف لتستدير شمالاً عائدة نحو تركيا، وربما لمح بعضهم علامة نجمة داوود السداسية مرسومة باللونين الأزرق والأبيض الخفيف على أجنحة ذلك التشكيل الهجومي التابع لسلاح الجو الإسرائيلي وهو يتجه عائداً إلى إسرائيل من دون أن يصيب طائراته خدش واحد، وقد خلف وراءه دماراً شاملاً في موقع المشروعات السرية التي استغرق إنشائها اعواماً قرب ذاك الوادي.

ثانيا: ضربت الهجمات الإلكترونية مواقع الحكومة الجورجية على الإنترنت. ففي المراحل الأولية، وجه المهاجمون ضربات أساسية لتعطيل خدمة المواقع الحكومية الجورجية، واخترقوا الجهاز الخادم الخاص بموقع الرئيس التشويه يوضع صور تقارن بين الزعيم الجورجي ميخائيل ساكاشفيلي وأدولف هتلر. وفي بادئ الأمر بدا هذا الهجوم تافهاً بل وصبيانياً. لكن مع اندلاع القتال البري اشتدت الهجمات الإلكترونية في حدتها ودرجة تعقيدها.

وعندما بلغت هجمات تعطيل الخدمة أوجها صارت تأتي من ست شبكات مسيرة مختلفة تستخدم أجهزة حاسوب مستلبة يملكها مستخدمو إنترنت عاديون لا يشكون في شيء، وتستخدم أيضاً متطوعين يقومون بتنزيل برامج القرصنة من العديد من مواقع

الإنترنت المناهضة لجورجيا. وبعد تثبيت هذه البرامج ينضم المتطوع إلى حرب الفضاء الإلكتروني بالضغط على زر مكتوب عليه "ابدأ الطوفان".

ثالثاً: قبل عطلة الرابع من تموز / يوليو مباشرة، أرسل أحد عملاء كوريا الشمالية رسالة. مشفرة إلى نحو 400 ألف حاسوب حول العالم وهي محملة بفيروس للسطو على الشبكات، حيث تضمنت الرسالة مجموعة بسيطة من التعليمات التي تجعل الحاسوب يبدأ في إرسال نبضات المطالبة بالاتصال بقائمة من مواقع الإنترنت الخاصة بالولايات المتحدة وحكومة كوريا الجنوبية وعدد من الشركات الدولية، وعندما يتم تشغيل الأجهزة المصابة بالفيروس فإنها تنضم في هدوء إلى الهجوم. فلو كان حاسوبك أحد هذه الأجهزة المسطو عليها، فربما تلاحظ أنه أصبح أبطأ من المعتاد، وأنك تستغرق وقتاً أطول من المعتاد للوصول إلى صفحات الإنترنت التي تطلب الدخول عليها، ولكن دون أن يكون هناك شيء غريب بدرجة كبيرة نعم، لقد كانت هذه هجمة أخرى من هجمات تعطيل الخدمة باستخدام أجهزة حاسوب تم السطو عليها وتكوين شبكة مسيرة منها، وفي أثناء عطلة نهاية الأسبوع لاحظت الحكومة الأمريكية أن النطاقين dhs.gov و state.gov غير متوافرين مؤقتاً، ولو فكر أحد وقتها في استطلاع مستويات التهديد الإرهابي من واقع بيانات وزارة الأمن الداخلي قبل أن يقرر الذهاب لمشاهدة الألعاب النارية في "ناشيونال مول" لما تمكن من الحصول على تلك المعلومات من موقع الوزارة.

رابعا: في التاسع من تموز / يوليو تم توجيه ما يتراوح بين 30 ألفا و 60 ألف حاسوب مصاب بنوع آخر من الفيروس لاستهداف نحو عشرة أو أكثر من مواقع حكومة كوريا الجنوبية والمصارف الكورية وشركة كورية جنوبية تعمل في مجال أمن الإنترنت. ويبدو أن القراصنة اقتنعوا بأن الهجوم على المواقع الأمريكية لم يعد فعالاً بعد أن بدأت الحكومة والمؤسسات الكبرى في التعاون مع مقدمي خدمة الإنترنت الفرز الهجمات وصدها، وفي السادسة صباحاً بتوقيت كوريا في العاشر من تموز / يوليو، بدأ العدوان الأخير، حيث شرع ما يقدر بمئة وستة وستين حاسوباً في أربع وسبعين دولة في إغراق مواقع المصارف الكورية والهيئات الحكومية الكورية ولكن في نهاية المطاف تم احتواء الأضرار، فلم تحاول الهجمة السيطرة على أي نظام

من النظم الحكومية أو تعطيل أي خدمة من الخدمات الضرورية. ويبدو أن المقصود من هذا الهجوم كان الإنذار فحسب. كل ما نعرفه أن الهجوم كان وراءه أجندة وحافز، لأنه لم يكن مجرد عدوى دودية" انطلقت في غياهب الإنترنت وسمح لها بالانتشار، فقد كان هناك من يتحكم في الهجوم ويوجهه ويعدل قائمة الأهداف للتركيز على المواقع الكورية الأضعف من غيرها.

تضمن الكتّاب محاولات سرية لوضع الاستراتيجية تسيطر على الفكر الأمريكي بشأن موضوع حرب الفضاء الإلكتروني النظرية القائلة بأن القضاء الإلكتروني "نطاق" أو ساحة تدور فيها رحى الحرب، ويجب أن "تهيمن" عليها الولايات المتحدة. وتكشف الاستراتيجية العسكرية القومية السرية (التي أفرج عن جانب منها بناء على ما نص عليه قانون حرية المعلومات عن موقف العسكريين من حرب الفضاء الإلكتروني لأسباب عدة، منها أن هذه الوثيقة تمت كتابتها على اعتبار أننا نحن المدنيين لا ينبغي أن نطلع عليها أبداً، أي إنها توضح كيف يدور الحديث عن حرب الفضاء الإلكتروني خلف أبواب البنتاجون المغلقة والمدهش في الوثيقة ليس فقط الاعتراف بأن حرب القضاء الإلكتروني حقيقة واقعة، ولكن الطريقة التي تناقش بها والتي تقترب من درجة الإجلال، على أساس أن حرب الفضاء الإلكتروني هي حجر الأساس في صرح القدرات القتالية الحديثة. وفي ضوء قلة الفرص المتاحة للاستماع إلى ما بقوله العسكريون الأمريكيون عن استراتيجية حرب الفضاء الإلكتروني، يجدر بنا أن نقرأ هذه الوثيقة قراءة فاحصة لكونها محاولة على مستويات سرية لوضع استراتيجية ما لحرب الفضاء الإلكتروني.

يتصدر الوثيقة خطاب موقع من وزير الدفاع، وتعلن الوثيقة أن هدفها هو اضمان التفوق الاستراتيجي للجيش الأمريكي في نطاق الفضاء الإلكتروني». هذا التفوق مطلوب لضمان "حرية التحرك" للجيش الأمريكي وحرمان أعدائنا من هذه الحرية".

كما يسميه الكاتب (الشرق الأحمق) من واقع ما نعرفه عن قدرات الصين في مجال حرب الفضاء الإلكتروني، وحملات التجسس التي شنها الصينيون يمكن القول بأن هذا النهج الثنائي هو النهج الذي سيؤثر الصينيون اتباعه، فمنذ أواخر التسعينيات عمدت الصين إلى اتخاذ كل ما يمكن لبلد أن يفعله بطريقة منهجية عندما يفكر في بناء قدرات هجومية في مجال حرب

الفضاء الإلكتروني، ويفكر في أنه قد يكون هو نفسه هدفاً لهذا النوع من الحرب، فقامت بما يلي:

1. تكوين جماعات من قراصنة الإنترنت من المواطنين الصينيين.
2. القيام بعمليات تجسس إلكتروني واسعة، منها ما طال معدات الحاسوب الأمريكية وبرامجها.
3. اتخاذ خطوات عديدة لحماية فضائها الإلكتروني، أي شبكاتها.
4. إنشاء وحدات عسكرية لحرب الفضاء الإلكتروني.
5. زرع القنابل المنطقية في ثنايا البنية التحتية الأمريكية.

وبينما تعمل الصين على تطوير استراتيجيتها النووية، فإنها تستخدم أيضاً قراصنة من الأفراد المرتبطين بمصالح الدولة ارتباطاً وثيقاً، إذ تقدر لجنة المراجعة الاقتصادية والأمنية الأمريكية - الصينية أن هناك ما يصل إلى 250 جماعة من قراصنة الإنترنت في الصين ممن يتمتعون بالمهارات المتقدمة بما يشكل خطراً على المصالح الأمريكية على شبكة الإنترنت. وقد رأينا في مطلع التسعينيات بعض الشواهد على قدراتهم، عندما تزعمت الولايات المتحدة حملة لإيقاف المذابح التي كانت القوات العربية ترتكبها في كوسوفا، وكانت الولايات المتحدة قد برعت في صنع الأسلحة الذكية التي استخدمتها للقضاء على الآلة العسكرية الصربية التي تعود إلى الحقبة السوفيتية من دون أن تفقد حياة أمريكي واحد ولم تسقط إلا طائرة حربية أمريكية واحدة بسبب عطل ميكانيكي)، ولكن لسوء الحظ لا يمكن أن تعوض الأسلحة الذكية رداءة المعلومات، فقد أسقطت إحدى الطائرات الأمريكية ست قنابل أصابت بدقة هدفها وفقاً للإحداثيات التي حددها مخططو المهمة بناءً على معطيات وكالة الاستخبارات المركزية الأمريكية، وكان من المفترض أن يكون هذا الهدف هو المديرية الفيدرالية اليوغوسلافية للإمداد والتموين، وهي هيئة تخطيطية تابعة للجيش العربي، إلا أن الإحداثيات كانت تبعد نحو 900 قدم عن المديرية وتنطبق تماماً على السفارة الصينية.

في الفصول الأخيرة تناول الكتاب الأسباب القوية التي تدعونا إلى الاعتقاد بأن معظم الحروب الفعلية التقليدية في المستقبل ستصاحبها حروب فضاء إلكتروني، وأنه ستكون هناك حروب فضاء إلكترونية أخرى قائمة بذاتها، من دون أي انفجارات أو قوات مشاة أو قوات جوية أو بحرية، ولكننا لم نشهد حتى الآن حرب فضاء إلكترونية شاملة تتبارى فيها

الدول الكبرى في هذا النوع من القتال في استخدام أشد أدواتها تطوراً ضد غيرها. ولذلك لا ندري حقاً من عساه يفوز ولا ندري ما هي النتائج التي ستتمخض عنها مثل هذه الحرب. وفي هذه الفصول اتضح لنا كيف أن عدم إمكانية التنبؤ المرتبطة بحرب الفضاء الإلكتروني الشاملة تعني أن ثمة احتمالاً قوياً أن صراعاً كهذا يمكن أن يغير ميزان القوى العسكرية العالمية ومن ثم يؤدي إلى تغيير جوهري في العلاقات السياسية والاقتصادية. كما يطرح الكتّاب بعض السبل الممكنة للحد من انعدام هذه القدرة على التنبؤ بما سيأتي به المستقبل على هذا الصعيد.

وبحلول عام 2003، كانت الصين قد أعلنت عن إنشاء وحدات حرب الفضاء الإلكتروني، حيث تضم القاعدة البحرية الكائنة بجزيرة هاينان Hainan الإدارة التقنية الثالثة بجيش التحرير الشعبي الصيني وجهاز لينجشوي Lingshui لاستخبارات الإشارة، وهاتان الوحدتان حسبما يقول البنتاجون مسؤولتان عن الهجوم والدفاع على شبكة الإنترنت، وقد صممنا لهذا الغرض أجهزة خاصة بالشبكة لم يسبق لها مثيل، ولا توجد أي دفاعات تستطيع التصدي لها. وفي إحدى المطبوعات يعطي الصينيون الأمثلة العشرة التالية لهذه الأسلحة والتقنيات:

1. زرع الالغام المعلوماتية
2. إجراء عمليات الاستطلاع المعلوماتي
3. تغيير بيانات الشبكات
4. إطلاق القنابل المعلوماتية
5. دفن النفايات المعلوماتية
6. نشر الدعاية
7. الخداع المعلوماتي
8. تنظيم الدفاعات المعلوماتية
9. إطلاق معلومات مستنسخة (كذا في الأصل)
10. إنشاء محطات تجسس على الشبكات

وقد أنشأت الصين "محطتين للتجسس على الشبكات" في دولة لا تبعد كثيراً عن الولايات المتحدة، وهي كوبا بإذن من حكومة كاسترو، حيث أقام الجيش الصيني منشأة الرصد التحركات الأمريكية على الإنترنت، ومحطة أخرى لمراقبة اتصالات وزارة الدفاع

الأمريكية. وفي الوقت الذي أعلنت فيه الصين عن إنشاء وحدات حرب الفضاء الإلكتروني، تعرضت الولايات المتحدة الواحدة من أسوأ حلقات التجسس الإلكتروني حتى وقتنا هذا. ويطلق على هذه الواقعة الاسم الرمزي Titan Rain (أي مطر العمالقة) الألغام المعلوماتية وفيها تم سحب ما يتراوح بين 10 و20 تيرابايت من المعلومات من شبكة البنتاغون غير السرية. كما استهدف القراصنة أيضاً إحدى شركات المقاولات الدفاعية وهي شركة لوكهيد مارتن" Lockheed Martin وغيرها من المواقع العسكرية، ولأسباب يتعذر فهمها حتى اليوم البنك الدولي أيضاً. واعتمدت الهجمة على تحديد مواطن الضعف بطريقة منهجية في شبكة البنتاجون والشبكات الأخرى المستهدفة ثم استغلالها لانتزاع المعلومات من خلال أجهزة خادمة تقع في كوريا الجنوبية وهونج كونج. كما تمكن المحققون من تتبع حركة التدفق من هذه الأجهزة الخادمة الوسيطة إلى الجهاز الخادم النهائي ومقره جواندونج في الصين. فألقى ويليام لورد William Lord اللواء بسلاح الجو الأمريكي باللائمة مباشرة وعلناً على الحكومة الصينية نفسها، وليس على النشطاء من قراصنة الإنترنت.

ركز الكتاب فيما سبق على الصين لأن تطورها في مجال حرب الفضاء الإلكتروني يعتبر واضحاً جلياً إلى حدٍ ما، وهو أمر غريب، إلا أن مسؤولي الاستخبارات الأمريكيين لا يعتبرون أن الصين هي التهديد الأكبر للولايات المتحدة في مجال الفضاء الإلكتروني، حيث قال أحدهم: إن الروس بالقطع أفضل منهم، حتى أنهم يكادون يضارعوننا في قدراتهم. ويبدو أن الآراء تتفق على أن الصين تحظى باهتمام أكبر لأنها - بقصد أو بدون قصد - دائماً ما تترك أثراً يمكن اقتفاؤه، وهو ما ينتهي دائماً إلى الميدان السماوي في بكين.

أما القراصنة الروس غير التابعين للحكومة، ومنهم عصابات إجرامية كبيرة في عالم الإنترنت، فيمثلون قوة لا يستهان بها في الفضاء الإلكتروني، كما رأينا في الفصل الأول في الهجمات التي تعرضت لها إستونيا وجورجيا، إذ يعتقد بصفة عامة أن قراصنة الإنترنت ومجرميها يعملون تحت مظلة ما كان يعرف باسم المديرية 16، وهي جزء من جهاز الاستخبارات السوفيتي الرهيب المعروف باسم "كي جيه بي " KGB، والتي سميت فيما بعد باسم FAPSI، ذلك المختصر الذي لا يذكر دلالته إلا القليلون من ضباط الاستخبارات الأمريكية (فهو مختصر العبارة باللغة الروسية تعني اللجنة الفيدرالية للاتصالات والمعلومات

الحكومية). ويكتفي رجال الاستخبارات الأمريكيون بإطلاق اسم " وكالة الأمن القومي بموسكو" على هذه اللجنة.

وتناول الكتاب في فصوله الأخيرة ايضًا جوانب الضعف في الانترنت وعمليات التحكم في الأجهزة الالكترونية عبر الفضاء واجهزة الحاسوب المربوطة على آلات الحروب والصواريخ وتحديد الأماكن عن بعد وايضًا تحليل شفرات الحاسبات عند الاختراق وكيفية توظيف هذه الاجهزة وأدارتها في عمليات الاختراق.

وتناول الكتاب ايضا فشل الدفاعات في صد الهجمات البدائية لتعطيل الانترنت ولماذا لم يفعل أحد أي شيء لمعالجة أوجه الضعف تلك ؟ ولماذا التأكيد على قدرتنا على مهاجمة الآخرين، بدلاً من إعطاء أولوية للدفاع عن أنفسنا ضد مثل هذا الهجوم ؟ الإجابة أننا حاولنا ابتكار دفاعات خاصة بحرب الفضاء الإلكتروني ولكن من الواضح أنها فشلت.

ففي عام 1994 ركزت اللجنة المعروفة بلجنة الأمن المشترك التي أنشأتها وزارة الدفاع بالتعاون مع وكالات الاستخبارات الأمريكية على المشكلة الجديدة الناتجة عن انتشار تقنيات المعلومات، فجاء تقرير اللجنة النهائي مصيباً بشأن ثلاثة مفاهيم مهمة:

- تقنية نظم المعلومات تتطور بمعدل أسرع من تقنية أمن نظم المعلومات.
- أمن نظم المعلومات والشبكات هو التحدي الأمني الأساسي في هذا العقد، وربما في القرن القادم... ولا يوجد وعي كافي بالمخاطر الجسيمة التي نواجها في هذا المضمار.
- تزايد الاعتماد في القطاع الخاص على نظم المعلومات؛ مما يجعل الوطن بأكمله وليس البنتاجون فقط عرضة للأخطار.

هذه النقاط الثلاث سليمة تماماً، بل وتنطبق بدرجة أكبر على ما نعيشه اليوم. وجدير بالذكر أن مجلة تايم نشرت في عام 1995 مقالاً سابقاً لعصره في ذلك الوقت أوضح أن حرب الفضاء الإلكتروني وجوانب الضعف الداخلية لدى الولايات المتحدة موضوعات تم تنبيه واشنطن عليها منذ خمسة عشر عاماً.

وتوضيحا لما احتواه الكتاب من التفاعل بين هذه العوامل الثلاث (الهجوم والدفاع والاعتماد)، أعددت الجدول البياني التالي، الذي يبين تقييم عدد من الدول بالدرجات لكل عامل من هذه العوامل. وقد يعترض البعض على بساطة المنهج المستخدم، على أساس أنني أعطيت نفس الوزن للعوامل الثلاثة، وجمعت درجاتها معاً لحساب الدرجة النهائية للدولة،

وأود أن أنوه هنا بأن الدرجات التي أعطيتها لكل دولة تستند إلى تقييمي الشخصي لقوتها الهجومية وقدراتها الدفاعية ومدى اعتمادها على نظم الشبكات الإلكترونية، وثمة جانب واحد في القياس ربما لا يبدو بديهياً، وهو أن الدولة كلما قل اعتمادها على الشبكات الإلكترونية زادت درجتها على مقياس الاعتماد وتفسير ذلك أن انتشار الشبكات الإلكترونية في البلاد أمر طيب، ولكنه ليس كذلك عندما تنظر لهذا الانتشار على أنه مقياس لقدرتها على الصمود أمام حرب الفضاء الإلكتروني.

محصلة القوة في مجال حرب الفضاء الإلكتروني

الدولة	هجوم الكتروني	اعتماد الالكتروني	دفاع الكتروني	الاجمالي
الولايات المتحدة	8	2	1	11
روسيا	7	5	4	16
الصين	5	4	6	15
ايران	4	5	3	12
كوريا الشمالية	2	9	7	18

وتطرق الكتّاب في الفصل الأخير الى أنه على رؤساء الدول وفي إطار المراجعة السنوية ينبغي أن يقوموا بمراجعة سجل قيادة حرب الفضاء الإلكتروني ليروا ما الشبكات التي تم اختراقها، وما الخيارات المتاحة أمامهم في أوقات الأزمات، وهل هناك تعديلات مطلوبة في توجيهاتهم السابقة. هذه المراجعة تشبه التقرير السنوي للعمليات السرية والمحاولات الدورية لإزالة الغبار عن خطة الحرب النووية بمشاركة الرئيس، فعندما يعرف الجميع أن هناك مراجعة سنوية فإنهم يلتزمون الصدق مع النفس، وبينما يقوم الرئيس بمراجعة تنفيذ استراتيجية حرب الفضاء الإلكتروني، يمكنه الاطلاع على تقرير سنوي من إدارة الدفاع الإلكتروني التي اقترحتها حول ما أحرزته من تقدم في تأمين الهيئات الحكومية وشركات المستوى الأول التي تقدم خدمات الإنترنت وشبكة الربط الكهربائي.

وكون الكتّاب يتمحور في دور الولايات المتحدة في حروب الفضاء الالكتروني يقع على عاتق الرئيس أن يضع تقليص التجسس الإلكتروني من جانب الصين على رأس الأولويات الدبلوماسية، كون الصين اصبحت المنافس الاقوى للولايات المتحدة الامريكية وأن يوضح أن هذا المسلك يرقى إلى درجة الحرب الاقتصادية.

الاستنتاجات

1. أن حرب الفضاء الإلكتروني تحدث بسرعة الضوء، فعندما تتدفق فوتونات الحزم المهاجمة عبر كابل الألياف الضوئية فإن الوقت المستغرق بين شن الهجمة وتأثيرها يكاد يتعذر قياسه، مما يخلق المخاطر أمام صناع القرار في أثناء الأزمات.
2. أن حرب الفضاء الإلكتروني حرب عالمية الطابع، وفي نطاق أي صراع يستشري العدوان الإلكتروني على مستوى العالم سريعاً، لأن أجهزة الحاسوب والأجهزة الخادمة المخترقة خفية أو التي تم السيطرة عليها في شتى أنحاء العالم سرعان ما تنضم إلى الهجمة، فتنجر بلاد كثيرة إلى الصراع سريعاً.
3. أن حرب الفضاء الإلكتروني لا تحتاج إلى ساحات المعارك التقليدية، فالأنظمة المختلفة التي يعتمد عليها الناس - من المصارف إلى رادارات الدفاع الجوي - يمكن الوصول إليها عبر الفضاء الإلكتروني والسيطرة عليها سريعاً أو تعطيلها دون الحاجة إلى دحر الدفاعات التقليدية للدول.

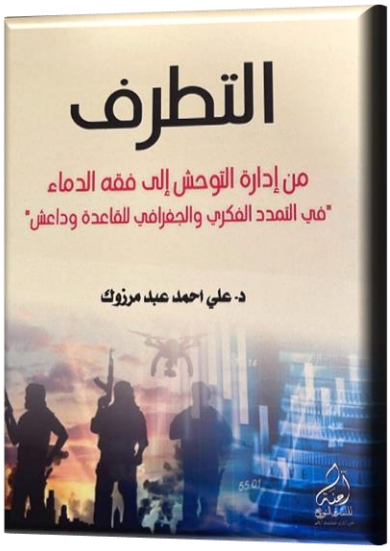
التوصيات

1. اجراء مزيد من التدريبات المشتركة والسيناريوهات أو الممارسات للتصدي للهجمات الإلكترونية. الاهتمام بكون الفضاء السيبراني عنصر من عناصر الدولة الاربعة .
2. فهم وإدراك طبيعة الفضاء الإلكتروني واعتباره عنصر رئيسي في الأمن القومي، إذ أن لها علاقة وطيدة بقضايا التنمية السياسية والاقتصادية والاجتماعية وضرورة إدماجه في العقيدة الأمنية للدولة ووضع استراتيجية قادرة على التعامل مع التهديدات والهجمات التي يكون مصدرها الفضاء الإلكتروني.
3. ضرورة تحديث الجيوش وتدريبها على هذه الحروب والاعتماد على تكنولوجيا المعلومات.
4. ضرورة تفعيل التشريعات والقوانين التي تُنظم الفضاء الإلكتروني، خاصةً قوانين الحروب الإلكترونية.
5. ضرورة نشر التوعية بخطورة هذه الحروب والأهداف منها، حتى يكون هناك فهم وإدراك لدور الأفراد في بناء الأمن.

التطرف

" من "إدارة التوحش" إلى "فقه الدماء في التمدد الفكري والجغرافي للقاعدة وداعش

نشر هذا الكتاب في دار آمنة للنشر والتوزيع/ المملكة الأردنية الهاشمية



تأليف: د. علي احمد عبد مرزوك
عرض بقلم
م.م. حسين محمد البياتي
قيادة فرقة الرد السريع

خلَال السَّنوات الأخيرة كَثرَت الرُّؤى الفكْريَّة والْمطارحات الفلْسفيَّة حَوْل التَّطَرُّف ومظاهره وارْتباطاته المفْهوميَّة وتنوُّع مَصادره وأشْكاله وَتنوعَت خَلفية تلْك الرُّؤى والْمطارحات فهناك الأعْمال الفكْريَّة الَتي تَظهَر في شَكْل تَحليل فَلسَفي، وهناك الأعْمال الَتي تَنطَلق من المعْرفة المتراكمة في مَجَال علْم النَّفْس وَخصُوصًا فيمَا يَتعلَّق ببناء وتطوُّر الشَّخْصيَّة، ومظاهر الأمْراض النَّفْسيَّة، ثُمَّ هُنَاك رُؤَى وأفْكَار في حَفْل الَعلُوم السِّياسيَّة تَرصُد وتبْحث أَسبَاب مَظاهر التَّطَرُّف وانْتقالات المفْهوم وَمدَى تأْثيره في المجَال الْعام السِّياسيّ ورصدتْ الَعديد من تلْك الَجهُود والتَّغيُّرات الَتي تَحدُث على ظَاهرة التَّطَرُّف والتَّوْضيح للمتغيِّرات المترابطة بهَدف تَحديد الأسْباب والنَّتائج بُغيَة إيجَاد البدائل في السِّياسات الَتي تتَّخذهَا الحكومات المناهضة الظَّاهرة وقطْع جُذورهَا.

والتَّطرُّف ظَاهرة لَهَا بُعْدها التَّاريخيّ وَتطورَت مع تَطوُّر المجْتمع البشَريّ، وَهي قَضيَّة مُعَقدَة وَمَركبَة قديمًا وحديثًا، وبواعثهَا أيْضًا كَثيرَة ومتنوِّعة ومتداخلة، بَعضُها قريب وَبَعضهَا بعيد، بَعضُها مُبَاشر، وَبَعضهَا غَيْر مُبَاشر، وَبَعضهَا وَاضح لِلعيْن، وَبَعضهَا فَائز في الأعْماق،

الاستلام 2024/02/04
الارجاع 2024/04/01
القبول 2024/05/13

ووصفتْ ظَاهِرة التَّطَرُّف المنْتجة لِلْإِرْهاب بِالتَّزمُّتِ اَلفكْرِي، والتَّشدُّد الدِّيني، ثُمَّ اِتَّخذ أنْصارهَا مَواقِف دِينيَّة وسياسيَّة واجْتماعيَّة، أَسفَرت عن عَدائِها لِلْمجْتمع ومؤَسَّساته مِمَّا أَدَّى إِلى تَهدِيد مَنظُومة التَّعايش اَلسلْمِي لِلْمجْتمعات فضْلا عن تَهدِيد مَنظُومة الأَمْن وَتخرِيب مُؤَسَّساته.

وأَنَّ الإِرْهاب المولود مِن رَحِم الفكْر المتطرِّف يعْد أَخطَر الظَّواهر الإِجْراميَّة اَلتِي عَرَفتهَا المجْتمعات الحديثة لِمَا يُمثله مِن تَهدِيد لِلْفكْر والْعقيدة والْكِيان السِّياسِيّ والْحضارِيّ لِلشُّعوب، وباتِّساع مَفهُومه أَضحَى مِن أَبرَز التَّحدِّيات والْمهدَّدات الأَمْنيَّة والاجْتماعيَّة فِي العالم لِمَا لَه مِن تأْثيرات بَعِيدَة المدى على الإِنْسانيَّات كَافَّة، كَونُه يَتخِذ صُورا وأَشْكالا وصيغًا مُتَعددَة تَهدف إِلى تَروِيع فَرْد أو جَماعَة أو دَولَة بُغيَة تَحقِيق أَهدَاف لَا تُجيزهَا القوانين المحلِّيَّة أو الدَّوْليَّة أو الأَعْراف الاجْتماعيَّة والدِّينيَّة السَّائدة . واسْتأْثر التَّطَرُّف بِالْعديد مِن النِّقاشات والْجدالات والْمواقف المتضاربة والْمتعارضة وَكَان لَافتًا فِي هذَا السِّيَاق مُخرجَات التَّطَرُّف - الإِرْهاب - على نَحْو سَيِّئ، مِن خِلَال إِلصَاق مَفهُوم الإِرْهاب بِالدِّين الإِسْلامِيّ، وبمطْلب بِنَاء الدَّوْلة الإِسْلاميَّة المتخيَّلة فِي أَذهَان اَلعدِيد مِن التَّنْظيمات الإِرْهابيَّة كالْقاعدة وَداعِش، وارْتباط مَفهُوم الجهَاد بِالْحَرْب على المخالفين، خُصوصًا اَلَّذين كَانُوا يعْتدون على الدِّين الإِسْلامِيّ والْمسْلمين فِي مَرْحَلة الدَّعْوة المحمَّديَّة اَلأُولى أو بعْدهَا، وسيق بِشَأن هذَا الْموْضوع اَلعدِيد مِن الأساطير، إِلى دَرجَة أَنَّ هُنَاك من يرى أَنَّ الإِسْلام مُرَادِف لِمفْهوم الجهَاد اَلذِي تتبنَّاه تِلْك الجماعات المتطرِّفة، زِيادة على ذَلك أَخْذ مَفهُوم التَّطَرُّف بِالتَّشتُّتِ بَيْن مَفاهِيم ومصْطلحات كَثِيرَة، آلتْ إِلى تَركِيز جُهُود عِلْميَّة نَحْو فكّ اللَّبْس عن تِلْك المفاهيم وتمْيِيزهَا عن التَّطَرُّف، فِي الوقْتِ اَلذِي نَحْتاج إِلى قَطْع دَابِر هذَا الفكْر وتحوُّلاته الإِرْهابيَّة .

وَإِن تبيَّين الأَسْباب الجذْريَّة لِلتَّطَرُّف اَلمُؤدي إِلى الإِرْهاب، عَمَليَّة مُعَقدَة تَتطلَّب تقْديرًا لِلفوارق الاجْتماعيَّة والثَّقافيَّة والسِّياسيَّة المرْتبطة بِمشْهد العوْلمة اَلسرِيع التَّطَوُّر، فالتَّطَرُّف مُتَعدد اَلْأَوجه - وفْقًا لِتعدُّد أَسْبابه ومَا تُفْرزه مِن أَنمَاط وأَشْكَال لِلتَّطَرُّف - وَتوجَّه فضاءَات اِفْتراضيَّة عَدِيدَة ومترابطة، وَهُو يَقتَرن بِظروف تاريخيَّة وسياسيَّة وجيوسياسيَّة واقْتصاديَّة واجْتماعيَّة مُحَددَة يُمكِن أن يَظهَر فِيهَا التَّقْنين العقائديُّ والْأَيْديولوجيَّات المتطرِّفة، وَيمكِن أن تَشمَل الأَسْباب الجذْريَّة لِلتَّطَرُّف أَيْضًا قَبُول وَتطبِيع التَّفاوتات الاجْتماعيَّة، وَرفَض التَّسامح، ومشاكل الصِّحَّة النَّفْسيَّة، والْجاليات والْمجْموعات المنْفصلة وَلكِن مِن اَلمهِم إِدرَاك أَنَّ دَوافع

التَّطَرُّف تَتَجَاوَز المفاهيم السَّطْحيَّة المتمثّلة فِي الأفْراد المحْرومين من حُقوقِهم والْمنْفصلين عن مُحيطِهم، ولاسيَّمَا فِي سِيَاق الشَّبَاب، فإن التَّطَرُّف مُسْتوْحًى من مَجْمُوعة مُتَنوعَة من الأيْديولوجيَّات أَكثَر مِمَّا كان يُفتَرَض فِي الماضي، مِمَّا يُؤدّي إلى تَفاقُم التَّحدّيات الَتِي تُوَاجِه المؤسَّسات الحكوميَّة وبرامج الوقاية المحلِّيَّة، مَا يستوْجِب اِسْتيعاب آليَّة التَّحَوُّل نَحْو التَّطَرُّف الَمُؤدي إلى الإرْهاب .

وَمِن هذَا المنْطلق اِعتمَد الباحثون فِي تَحليل ظَاهِرة غَرْس التَّطَرُّف وصناعة الإرْهاب على عدد من التَّفْسيرات تَختَلف فِي دَرجَة عُمْقِها ومنْظوراتهَا، فَبَعضهَا يسير فِي اِتِّجاه إعطَاء الأوْلويَّة لِلْبنْيات والْبيئة السِّياسيَّة المساعد على تَنامِي الأفْكار المتطرِّفة، والدَّوْر الَذي تؤَديه البيئة النَّفْسيَّة والْإحْساس بِالْمظالم فِي جَعْل الفرْد قابلا لِلتَّحَوُّل نَحْو التَّطَرُّف الَعنيف، وهناك تفْسيرات أُخرَى تُركّز على مَراحِل ومسارات التَّطَرُّف، بِحسْبانهَا سِلْسلة أو حَلَقات مُترابطة، وَفِي هَذِه الدِّراسة ستركّز على آليَّة الانْتقال من الفكْر (التَّطَرُّف) إلى الفعْل (الإرْهاب)، عَبْر اِسْتراتيجيَّة اِفْتراضيَّة لِعَمل التَّنْظيمات الإرْهابيَّة . ونظرًا لِحَجم المخاطر الَتِي يُنْتجهَا التَّطَرُّف على المنْظومة الأمْنيَّة الحاضنة لِلتَّعايش الَسلْمِي فِي الدَّوْلة، تَأتِي هَذِه الدِّراسة لِتفْكيك إِشْكاليَّة التَّطَرُّف فِي العرَاق بَعْد الْعام 2005 وُصولًا إلى الْعام 2022 وإبْرَاز تأْثيراتهَا على الأوْضاع الثَّقافيَّة العراقيَّة وَبِنيَة الأمْن، إذ تَركَت التَّنْظيمات المتطرِّفة حَالَة من التَّفَسُّخ والانْحلال فِي المجْتمع العراقِيّ، فضْلا عن تركات تَمثلَت بِالصِّراعات الحالية خَرجَت عن حُدُود الطَّبيعِيّ والْمأْلوف، وباتتْ تُهدّد لَيْس فقط حَالَة الاسْتقْرار الثَّقافِيّ، بَيْن أَفكَار وَقيَم مُتباينة بَيْن المجْموعات الاجْتماعيَّة المتنوّعة وحوامل أنْساقهَا الثَّقافيَّة بِمخْتَلف مشاربهَا الدِّينيَّة واللُّغويَّة، والْعرْقيَّة.. إلخ، وَإنمَا أيْضًا على حَالَة الاسْتقْرار الَأمْنِي الحاضنة لِلتَّعايش، وَإن التَّراكمات الَتِي سبَّبهَا التَّطَرُّف وجدالات الانْقسام الَتِي تَمتَد وتترَشَّح وتتمَثَّل بِحروب عَقلِية دَاخلِية تُطيح بِكلِّ سِياسَات التَّعايش والتَّكامل الوطَنِيّ القائمة على الوسطيَّة والاعْتدال وقواعد المنافسة الثَّقافيَّة والْحوار والتَّسامح الَفكْرِي والتَّوافق على مُشْتركات ثَقافِية وَطَنيَّة، وأَنَّ تفْكيكً وَتحليل ظَاهِرة التَّطَرُّف المنْتجة لِلْإرْهاب فِي العرَاق وتراكماتهَا على حَالَة الأمْن والتَّعايش ومَا سبَّبْته من آثار جَعلَت المجْتمع والدَّوْلة فِي مَوضع الهشاشة تَدعُونا إلى طَرْح سِياسَات أَمنية مُجْتمعيَّة مُلَائمَة لِمعالجة هَذِه الظَّاهرة.

اقرأ في هذا العدد ايضاً

البحوث والدراسات

- السياسات الاستراتيجية العراقية في مواجهة تداعيات التغيرات المناخية على الامن الوطني العراقي.
- الأساس القانوني لدور مجلس الأمن والمحكمة الجنائية الدولية في مكافحة الجرائم الدولية.
- الحرب الروسية – الأوكرانية وتداعياتها على أمن الطاقة للاتحاد الأوروبي.
- أمن المعلومات بين الضرورات الآنية والتدابير المستقبلية

عروض الكتب والدراسات

- دور الاسرة العراقي في تعزيز الأمن المجتمعي في ظل التحديات المعاصرة (الواقع والمأمول).
- حرب الفضاء الالكتروني التهديد التالي للأمن القومي وكيفية التعامل معه.
- التطرف من "إدارة التوحش" الى "فقه الدماء" في التمدد الفكري والجغرافي للقاعدة وداعش.

رقم الإيداع في دار الكتب والوثائق العراقية ببغداد (2698) لسنة 2023

00964 772 877 8806
erdaliraq@gmail.com
بغداد ، مطار بغداد الدولي، 87367ch