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

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

وزارة التعليم العالي والبحث العلمي
جامعة النهرين
كلية العلوم السياسية

قضايا سياسية
Political Issues

مجلة فصلية محكمة

العدد ٨٢
Issue 82

تموز - آب - ايلول / ٢٠٢٥
Jul. - Aug. - Sep. / 2025

جامعة النهرين
كلية العلوم السياسية

E-ISSN 2790-2404
P- ISSN 2070-9250
DOI prefix: 10.58298

قضايا سياسية
Political Issues

مجلة فصلية محكمة تعنى بنشر الأبحاث والدراسات السياسية العراقية والعربية والدولية
http://pissue.iq

مجلة قضايا سياسية

pissue.iq

قواعد النشر

- لغة المجلة هي اللغة العربية والانكليزية على أن يراعى الوضوح وسلامة النص.
- ترحب المجلة بنشر البحوث والدراسات السياسية النظرية والتطبيقية ولا سيما التي تجعل من قضايا المنطقة والعالم محط اهتمامها، ماضياً وحاضراً ومستقبلاً، وعلى وفق الآتي:

1. أن لا يزيد عدد صفحات البحث أو الدراسة عن (15) صفحة مطبوعة بحجم خط (14) والتباعد (1,15) ونوع الخط Simplified Arabic تقدم عبر المنصة الاليكترونية للمجلة على الرابط : https://pissue.iq/index.php/pissue/about/submissions
2. أن تتصف البحوث والدراسات بالموضوعية والدقة العلمية.
3. أن تعتمد الترقيم العشري للعناوين الأساسية والفرعية او التنصيف المعياري العام.
4. يرفق مع كل بحث او دراسة ملخصين (احدهما باللغة العربية والآخر باللغة الانكليزية/ يتضمن اهداف البحث ، المنهج والمعالجة ، ابرز النتائج واهم الاستنتاجات والمقترحات) مع ضرورة مراعاة ان الملخص مختلف اختلافا جذريا عن المقدمة وليس تكرارا لها .
5. تخضع جميع البحوث المقبولة للنشر الى نظام الاستلال الالكتروني في كلية العلوم السياسية –جامعة النهرين.
6. يرفق مع كل بحث ودراسة سيرة ذاتية مختصرة للباحث وتعهد .

- تقوم المجلة بإخطار الباحثين بإجازة بحوثهم أو دراساتهم من عدمها بعد عرضها على محكمين تختارهم على نحو سري من بين أصحاب الاختصاص.

مجلة قضايا سياسية

pissue.iq

- يجوز للمجلة أن تطلب إجراء تعديلات شكلية أو شاملة على البحث أو الدراسة قبل إجازتها للنشر بما يتماشى مع أهدافها.
- البحوث المنشورة تعبر عن آراء أصحابها ، ولاتعبر عن راي المجلة .
- ترحب المجلة بالمناقشات الموضوعية لما ينشر فيها أو في غيرها من الدوريات وبأية ردود فكرية أو تصويب، وكذلك ترحب بنشر التقارير عن المؤتمرات والندوات ذات العلاقة ومراجعات الكتب وملخصات الرسائل الجامعية التي تتم إجازتها على أن تكون من إعداد أصحابها.

توجه جميع المراسلات إلى هيأة التحرير على العنوان الآتي
مجلة قضايا سياسية، كلية العلوم السياسية، جامعة النهرين-بغداد – الجادرية.
E.mail: pirj@nahrainuniv.edu.iq

الموقع الاليكتروني
https://pissue.iq/index.php/pissue

E-ISSN 2790-2404
P- ISSN 2070-9250
DOI prefix: 10.58298

جدول المحتويات

الامن السيبراني وأثرة على الاستقرار السياسي في العراق بعد عام 2003 (دراسة تحليلية)[▽]

Cybersecurity and Its Impact on Political Stability in Iraq After 2003: (An Analytical Study)

م.م فاضل عباس صباح[*] Fadhil Abass Sabah

الملخص

تهدف هذه الدراسة إلى استكشاف العلاقة بين الأمن السيبراني والاستقرار السياسي، من خلال تحليل كيفية تأثير التهديدات السيبرانية على المؤسسات السياسية، والأنظمة الانتخابية، والثقة المجتمعية بالحكومات. تستند الدراسة إلى منهج تحليلي يعتمد على تتبع الأحداث السيبرانية الكبرى، مثل الهجمات على البنى التحتية، والتدخلات الرقمية في العمليات الانتخابية، وحملات التضليل المعلوماتي. قد أظهرت النتائج أن ضعف الأمن السيبراني يفاقم من هشاشة النظم السياسية، ويؤدي إلى زعزعة الاستقرار السياسي من خلال إضعاف ثقة المواطنين بالمؤسسات، وتأجيج الانقسامات الداخلية، وتعزيز التدخلات الخارجية. أن تعزيز الأمن السيبراني لم يعد خيارًا تقنيًا فحسب، بل ضرورة سياسية لضمان سيادة الدولة واستقرارها في البيئة الدولية المعاصرة لكونه يعد الركيزه الأساسية للأمن القومي، كما يتطلب تعزيز البنية القانونية، والتعاون الدولي، وتأهيل الكوادر البشرية، إضافة إلى رفع الوعي المجتمعي لضمان حماية الفضاء الرقمي، ودعم الاستقرار السياسي.

الكلمات المفتاحية: الاستقرار السياسي، الامن السيبراني، العراق

Abstract

This study aims to explore the relationship between cybersecurity and political stability by analyzing how cyber threats impact political institutions, electoral systems, and public trust in governments. The study adopts an analytical approach based on tracking major cyber events, such as attacks on critical infrastructure, digital interference in electoral processes, and disinformation campaigns. The findings reveal that weak cybersecurity exacerbates the fragility of political systems and leads to political instability by undermining citizens' trust in

[▽] تاريخ التقديم : 2025/8/15 تاريخ القبول: 2025/9/19 تاريخ النشر: 2025 /9/30

[*] جامعة كربلاء – كلية علوم الحاسوب وتكنولوجيا المعلومات fadhil.a@uokerbala.edu.iq

institutions, fueling internal divisions, and facilitating foreign interference. Strengthening cybersecurity is no longer merely a technical option, but a political necessity to ensure state sovereignty and stability in the contemporary international environment, as it constitutes a fundamental pillar of national security. This requires the enhancement of legal frameworks, international cooperation, capacity building, and raising public awareness to safeguard the digital space and support political stability .

Keywords: **Cybersecurity, Political Stability, Iraq**

المقدمة:

في ظل التطور المتسارع للتكنولوجيا الرقمية، برز الأمن السيبراني كمجال معرفي حديث وركيزة أساسية في تشكيل القوة الوطنية والدولية. فقد أدت الابتكارات في تكنولوجيا المعلومات إلى تغييرات جوهرية في مصادر النفوذ، حيث لم تعد القوة مقتصرة على الأدوات التقليدية، بل أصبحت القدرة على حماية الفضاء الرقمي من أبرز مؤشرات السيادة. ويُعد الأمن السيبراني من أبرز الاكتشافات المعاصرة لما له من دور محوري في حماية البنى التحتية الرقمية وضمان أمن تدفق المعلومات عبر الشبكات العالمية. وقد أسهم الاعتماد المتزايد على الفضاء السيبراني في توسيع فرص التنمية والتواصل، لكنه في المقابل فتح المجال أمام تهديدات أمنية متصاعدة، تجاوزت الأفراد لتطال مؤسسات الدولة وقطاعاتها الحيوية، من خلال هجمات تستهدف تسريب معلومات استراتيجية تمس الأمن الوطني والاقتصادي. وفي هذا السياق، تُعد الهجمات السيبرانية وأعمال التجسس الإلكتروني من أبرز التهديدات التي تواجه الأمن القومي للدول، بما في ذلك العراق. فقد أصبح الفضاء السيبراني بيئة خصبة لصراعات غير تقليدية تؤثر بشكل مباشر على الاستقرار السياسي. وفي الحالة العراقية، يمكن ملاحظة أن ضعف منظومات الحماية السيبرانية أسهم في زيادة فرص التدخل الخارجي، وتسريب البيانات الحكومية، واختراق أنظمة مؤسسات الدولة، ما ينعكس سلبًا على ثقة المواطن بالمؤسسات الرسمية، ويُضعف من قدرة الدولة على إدارة أزماتها الداخلية والخارجية. علاوة على ذلك، فإن الاستخدام غير المنضبط للفضاء الرقمي من قبل بعض الجهات الفاعلة، سواء كانت داخلية أم خارجية، ساهم في بث الشائعات، وتأجيج الانقسامات السياسية والطائفية، والتأثير في الرأي العام بوسائل رقمية يصعب السيطرة عليها، مما يزيد من تعقيد المشهد السياسي العراقي ويهدد أمنه واستقراره. وعليه، فإن تعزيز الأمن السيبراني في العراق لم يعد خيارًا، بل ضرورة استراتيجية ترتبط ارتباطًا مباشرًا

بالحفاظ على سيادة الدولة واستقرارها السياسي والاجتماعي، في ظل عالم يتجه بشكل متسارع نحو الاعتماد الكامل على النظم الرقمية.

أهمية البحث: تكمن أهمية هذا البحث في تسليط الضوء على الأمن السيبراني الذي يُعد من العوامل الحاسمة والهامة في حفظ استقرار السياسي للدولة العراقية، فقد استُخدم الفضاء السيبراني للتأثير على الرأي العام، والتلاعب بالانتخابات، واستهداف البُنى التحتية الحيوية. هذا جعله أداة ضغط سياسية، مما أدى إلى ربط الأمن السيبراني مباشرةً بالاستقرار السياسي والأمن القومي للدول.

هدف البحث: يهدف البحث الى

1- تعريف الامن السيبراني وأهميته في حماية البيئة التحتية الرقمية.

2- إيضاح تأثير الهجمات السيبرانية على الاستقرار السياسي للدولة العراقية.

2- استعراض السياسات الحكومية وتقديم توصيات لتعزيز الأمن السيبراني كوسيلة لدعم الاستقرار السياسي.

اشكالية البحث: تنطلق إشكالية هذا البحث من التساؤل الرئيسي مفاده إلى أي مدى أسهم انفتاح العراق على العالم الإلكتروني والتقني والمعلوماتي في زيادة تعرضه للهجمات السيبرانية، وما مدى انعكاس تلك التهديدات على الاستقرار السياسي للعراق؟ ومن هذا التساؤل المحوري تتفرع مجموعة من التساؤلات الثانوية التي يسعى البحث إلى الإجابة عنها، وهي:

1. ما المقصود بالأمن السيبراني، وما هي أهميته في العصر الرقمي؟
2. ما العلاقة بين الأمن السيبراني والاستقرار السياسي للدولة؟
3. ما هي الاستراتيجيات والسياسات الوطنية المتبعة في العراق لمواجهة التهديدات السيبرانية ؟

فرضية البحث:

تفترض هذه الدراسة أن للأمن السيبراني تأثيراً مباشراً على الاستقرار السياسي في العراق، وقد تجلّى هذا التأثير من خلال الهجمات السيبرانية الإرهابية التي استهدفت مؤسسات الدولة، وانتشار الدعاية الإلكترونية المضللة، فضلاً عن الاختراقات التي طالت البُنى التحتية الحكومية، مما ساهم في زعزعة الاستقرار السياسي والأمني في البلاد.

منهجية البحث: اعتمد الباحث على المنهج الوصفي التحليلي، حيث يسعى إلى دراسة وتحليل تأثير الامن السيبراني على الاستقرار السياسي في العراق.

هيكلية البحث: تم تقسيم الدراسة الى محورين:

أولا: ماهية الامن السيبراني.

ثانياً: التأثيرات السيبرانية على الاستقرار السياسي في العراق واستراتيجيات المواجهة. فضلاً عن المقدمة والخاتمة.

أولاً: ماهية الامن السيبراني

1- مفهوم الامن السيبراني

يعرف الامن السيبراني مجموعه من الاجراءات المتخذة في مجال الدفاع ضد الهجمات برانيه ونتائجها التي تشمل تنفيذ التدابير المضادة المطلوبة لذلك ويعرف "بانة عباره عن مجموعه من الاجراءات التي تتخذها في الدفاع ضد هجمات قراصنة الكمبيوتر ويتضمن تنفيذه المضادة المطلوبة" (عمارات، 2022، صفحة 15) وفي جوهره، يشير الأمن السيبراني إلى الممارسات والعمليات والتقنيات المستخدمة لحماية أنظمة الحاسوب والشبكات والبيانات من الوصول غير المصرح به أو التلف أو السرقة. ويتضمن ذلك حماية المعلومات والأنظمة من التهديدات السيبرانية مثل البرمجيات الخبيثة، والتصيد الاحتيالي، والقرصنة، وغيرها من الأنشطة الضارة التي تُنفذ عبر الإنترنت أو الشبكات الأخرى. وهناك ابعاد عدة الامن السيبراني منها:

1- امن المعلومات: حماية سرية البيانات وسلامتها وتوافرها. تضمن السرية أن البيانات متاحة فقط للأشخاص المصرح لهم بالاطلاع عليها. تتضمن النزاهة الحفاظ على دقة البيانات واتساقها وضمانها، ويضمن التوافر إمكانية الوصول إلى المعلومات عند الحاجة.

2- أمن الشبكات: يركز أمن الشبكات على حماية سلامة الشبكة والبيانات وسهولة استخدامها وموثوقيتها وسلامتها أثناء النقل. ويشمل ذلك تدابير للحماية من التطفل غير المصرح به على الشبكة. ويشمل ذلك استخدام جدران الحماية والشبكات الافتراضية الخاصة. (VPN) وأنظمة كشف التطفل.

3- أمن التطبيقات: يتضمن هذا البعد تأمين التطبيقات من التهديدات التي قد تنشأ أثناء دورة حياة التطبيق. يشمل أمان التطبيقات التدابير المتخذة أثناء مرحلة التطوير، مثل ممارسات التحقق من صحة المدخلات والترميز، والتدابير المستخدمة عند نشر التطبيقات، مثل التحديثات والتصحيحات المنتظمة

4- أمن نقطة النهاية: يهتم أمان نقطة النهاية بحماية شبكة الشركة عند الوصول إليها عبر أجهزة بعيدة مثل أجهزة الكمبيوتر المحمولة والهواتف الذكية والأجهزة اللاسلكية الأخرى. ويشمل ذلك ضمان التزام هذه الأجهزة بمستوى محدد من الامتثال لسياسة الأمان.

5- إدارة الهوية وأمن البيانات: يشمل ذلك العمليات والتقنيات اللازمة لضمان وصول الأفراد المناسبين إلى الموارد المناسبة في السياقات المناسبة. ويشمل ذلك مصادقة المستخدم وتفويضه والإدارة العامة لهويات المستخدمين.

6- الأمن المادي: يشير الأمن المادي إلى حماية الأجهزة والمرافق والأصول الملموسة الأخرى من التهديدات المادية مثل السرقة أو التلف. ويشمل ذلك استخدام الأقفال وكاميرات المراقبة وغيرها من أدوات التحكم المادية. (Cybellium, 2023, p. 15)

3- مفاهيم مرتبطة بالأمن السيبراني

أ- الفضاء السيبراني

ان فلاسفة الاغريق استخدم مفهوم السيبرنطقيا واشتقت هذه الكلمة من الفعل اليوناني كيبرنو الذي يعني يقود وبعدها اصبح السيبرانيه اسم علم الاتصالات والمعلومات والتحكم خلال الفضاء من البيانات الإلكترونية ووضع هذا المفهوم الكاتب الامريكي نوربرت فينر قدمه كعلم قائم له قواعد وقد عرفه "مجموع مجال نظريه التحكم والتوصيل سواء في الاله او الحيوان" ويعرفه فريدريك مايور السيبراني "بانه بيئة انسانيه والتكنولوجية جديده" (الصادق، 2016، الصفحات 29-30) و الفضاء السيبراني هو مجال افتراضي من صنع الانسان على انظمه الكمبيوتر والشبكات الانترنت والكم الهائل من البيانات والمعلومات والأجهزة وهناك الكثير من عرفه هو بانه الذراع الرابع للجيوش الحديثة" واخرون من يرى انه البعد الخامس للحرب والاكثر اعتمادا هو تعريف الاتحاد الدولي للاتصالات والذي عرف الفضاء السيبراني المجال المادي وغير المادي الذي يتكون وينتج عن عناصر هي: اجهزة الكمبيوتر، الشبكات، البرمجيات حوسبة المعلومات المحتوى، معطيات النقل والتحكم، ومستخدمو كل هذه العناصر" (ابوضيافة، 2019، صفحة 1016) لقد اصبح الفضاء السيبراني احد العناصر الرئيسية و المؤثرة على النظام الدولي لما يوفر من ادوات التقنية التكنولوجية لعمليات التعبئة في العالم اضافه الى تأثيره على القيم السياسية والاقتصادية والعسكرية والاجتماعية وان سهوله استخدامه ورخص التكلفة ازاد من قدرته في الاستخدام هذه المجالات و اكثر قدره على تحقيق اهدافه والتأثير على سلوك الجهات الفاعلة التي تستخدم هذه البيئة (خريسان، 2020، صفحة 10) وان المكون الاول في الفضاء الالكتروني الطبقي او المادي والذي يتمثل والمحولات والبنيه التحتية المعلوماتية الكابلات والمكونات والثاني يشمل في المحتوى الذي يعكس شكل الفضاء الالكتروني والمكون الثالث يشتمل في عمليه التوصيل

بين المعلومات واكثر ويرتبط بين الناس وثقافاتهم ولا يتكون الفضاء الالكتروني من شبكات الاتصال فقط من يتكون من معلومات لها قيمه في جميع المجالات. (الصادق، 2016، صفحة 35)

ب- الردع السيبراني

يعرف بانه منع الاعمال الضارة ضد الأصول الوطنية في الفضاء والأصول التي تدعم ويرتكز على ثلاثة ركائز هي عمادية الاستراتيجية، الدفاع السبراني، مصداقية الدفاع والقدرة على الانتقام والرغبة في الانتقام.

ت- الهجمات السيبرانية

تعرف بانها فعل يقوض من قدرات وظائف الشبكة المعلوماتية من خلال استغلال أحد نقاط الضعف مما يسمح للمهاجم القدرة على التلاعب بالنظام ويعرفه جونيدو مارشال"عملية استغلال متعمد لأنظمة الكمبيوتر والشبكات المعتمدة على التكنولوجيا من خلال البرمجيات الضارة وتتعدد ما بين الأساليب الممكنة والعشوائية التي تستخدم من طرف الرسمين او أساليب الضغط من فبل محترفين لتحقيق نفع ذاتي او مصالح شخصية منظمة من طرف الجماعات المارقة" (الحماصصة، 2024، صفحة 21)

ث- التجسس السيبراني

يشير التجسس الى جمع المعلومات السرية او الحساسة بشكل غير قانوني وغير مسموح بيه الهدف منه الحصول على معلومات استخباراتية او تجارية او عسكرية. ويكون هذا التجسس عن طريق استخدام مجموعة من الأساليب منها الاختراقات شبكات الهندسية والاجتماعية وبرامج التجسس، وعادة ما يكون التجسس من دولة ذات مصلحة للحصول على المعلومات الاستخبارية ليسبب التجسس اضرار كبيرة على الصعيد السياسي والاقتصادي وفقدان الثقة بين الدول وتعريض المعلومات الحساسة الى الخطر، لذا يتطلب مكافحة التجسس تعاون دولي، وتعزيز الإجراءات الأمنية على مستوى الشبكات والأنظمة الحساسة (البلقاسي، 2024، الصفحات 55-60)

ج- القوة السيبرانية: هي قدرة الدولة على فرض السيطرة والنفوذ داخل الفضاء السيبراني ومن خلالة تدعم العناصر الأخرى المكونة لقوة الدولة وبالاقتران معها ويعتمد تحقيق القوة السيبرانة على قدرة الدولة على تطوير الموارد اللازمة للعمل في الفضاء السيبراني (university, 2016, p. 198)

3- نظريات العلاقة بين الامن السيبراني والاستقرار السياسي

في العصر الرقمي المتسارع، أصبحت الفضاءات السيبرانية ساحة جديدة للصراع والتأثير، مما أفرز تحديات معقدة أمام الدول والحكومات في سعيها نحو تحقيق الأمن والاستقرار. وتُعنى نظريات العلاقة بين الأمن

السيبراني والاستقرار السياسي بدراسة كيف تؤثر التهديدات السيبرانية، مثل الهجمات الإلكترونية وحملات التضليل الرقمي، على النظم السياسية ومؤسسات الحكم واستقرار المجتمعات ومن هذه النظريات منها:

أ- نظرية النظام الدولي (Regime Theory)

تقوم هذه النظرية على أن المؤسسات والاتفاقيات السيبرانية الدولية — مثل اتفاقية بودابست لمكافحة الجريمة الإلكترونية تُسهم في تنظيم سلوك الدول وتطوير التعاون عبر الحدود، مما يعزز الاستقرار السياسي العالمي بتقليل التوترات السيبرانية بين الدول.

ب- نظرية الردع السيبراني (Cyber Deterrence)

تناقش كيف يمكن للدول استخدام قدرات سيبرانية لردع هجمات السيبرانية، أو العكس، وكيف يغيّر الفضاء السيبراني طبيعة المفهوم التقليدي للردع. أحد التحديات الرئيسية هو صعوبة نسب الهجمات، ما يضعف سياسات الردع التقليدية (https://en.wikipedia.org/wiki/Regime_theory، 2010)

ت- نظرية مفاهيم الأمن (Critical Security Studies)

من منظور النقد البنيوي، تُستخدم مفاهيم الأمن السيبراني كأدوات تغطية سياسية تُبرر توسّع الدولة أو تقييد الحريات باسم الحماية، وهو ما قد يؤدي إلى زعزعة الثقة المجتمعية والسياسية نموذج ALERT لتحليل الهجمات السيبرانية السياسية النموذج العلمي "ALERT (Actors–Levers–Effects–Response) يُصنف كيف تُوظَّف أنظمة المعلومات كأدوات للاضطراب السياسي، ويظهر ديناميكية العلاقة بين الجهات الفاعلة، الوسائل المستخدمة، النتائج المحتملة والاستجابة الحكومية، مما يوفر إطاراً شاملاً لقياس التأثير السياسي للهجمات السيبرانية.(Desouza, 2020, p. 101606)

ث- نظرية تأثير النظام السياسي (Polity Flux Effect)

وجدت دراسة حديثة علاقة غير خطية بين طبيعة النظام السياسي وقوة الأمن السيبراني: الديمقراطيات المستقرة تمتلك أداءً سيبراني أفضل بسبب مؤسسات شفافة وتعامل شامل. الأنظمة الهجينة (Anocracies)، مثل الانتقالية، تواجه تحديات كبيرة في الاستقرار السيبراني وقد تشكل خطراً أكبر داخلياً وخارجياً. الأنظمة السلطوية يمكنها فرض إجراءات سيبرانية بسرعة، لكنها غالباً ما تستخدمها في قمع المعارضة والتلاعب بالمعلومات. (kiliner, 2022, p. 1196) وهنالك امثلة واقعية وبارزة توضح علاقة الامن السيبراني بالاستقرار السياسي منها الهجمات الإلكترونية الروسية على أوكرانيا (2015–2022): يُعتقد أن روسيا، بقصد زعزعة استقرار أوكرانيا في ظل التوترات الجيوسياسية المستمرة، هي مصدر هذه

الهجمات. منذ عام 2015، استهدفت سلسلة من الهجمات الإلكترونية مؤسسات حكومية أوكرانية، وبنية تحتية حيوية، والقطاع المصرفي. ومن أبرز الحوادث هجمات عامي 2015 و2016 على شبكة الكهرباء الأوكرانية، والتي تسببت في انقطاعات واسعة النطاق للتيار الكهربائي. لم تتسبب هذه الهجمات في انقطاعات فورية فحسب، بل ساهمت أيضًا في استمرار عدم الاستقرار في أوكرانيا، مما قوّض ثقة الجمهور في المؤسسات الحكومية. وقد أظهرت هذه الهجمات قدرة العمليات الإلكترونية على تكملة الاستراتيجيات العسكرية التقليدية.(Block, 2023) وكذلك التدخل في الانتخابات الامريكية 2016 باستخدام تسريبات واختراق للمؤتمرات الحزبية، لإثارة الانقسام السياسي واستخدام المعلومات كسلاح سياسي. (Desouza، 2020، صفحة 101606)

ثانياً: التأثيرات السيبرانية على الاستقرار السياسي في العراق واستراتيجيات المواجهة

تعد التأثيرات السيبرانية على الاستقرار السياسي العراقي من القضايا المهمة الحيوية والمعقدة في ظل تزايد الاعتماد على التكنولوجيا والمجال السيبراني في جميع القطاعات وخصوصا الأمنية والسياسية والاقتصادية. وفيما ما يلي أبرز التأثيرات السيبرانية التي تؤثر على الاستقرار السياسي في العراق منها:

1- التأثيرات السيبرانية

أ- الهجمات الإرهابية السيبرانية :

بدأ استخدام مصطلح "الإرهاب الإلكتروني" في أوائل ثمانينيات القرن العشرين على يد الباحث باري كولين، الذي أشار إلى التحديات الكبيرة في وضع تعريف جامع ومحدد لهذا المفهوم الناشئ. وفي سياق محاولاته لتأطير المصطلح، قدم كولين تعريفاً للإرهاب الإلكتروني باعتباره "هجوماً إلكترونياً يهدف إلى تهديد الحكومات أو الاعتداء عليها، وذلك من أجل تحقيق أهداف ذات طابع سياسي أو ديني أو أيديولوجي". ويشترط في هذا النوع من الهجمات أن تُحدث أثراً تدميرياً وتخريبياً يعادل من حيث الشدة والنتائج الأفعال المادية المرتبطة بالإرهاب التقليدي. (كمال، 2022، الصفحات 122-123) وعرفه جميس لويس james lewiss " بأنه استخدام أدوات شبكات الحاسوب في تدمير أو تعطيل البنى التحتية الوطنية المهمة مثل: الطاقة والنقل والعمليات الحكومية، أو بهدف ترهيب حكومة ما أو مدنيين" (كمال، 2022، صفحة 123) يُعدّ الإرهاب السيبراني أحد أبرز التهديدات المستجدة التي تستهدف الأمن القومي للدول، حيث يسعى من خلال أدواته الرقمية إلى نشر الفوضى وإحداث الدمار، فضلاً عن التسبب بخسائر مادية

واقتصادية جسيمة، والإضرار بالمصالح الأمنية والعسكرية والمدنية للمؤسسات والدول على حد سواء. وتتعدد أشكال الإرهاب السيبراني وفقاً لأساليبه وتقنياته، ومن أبرزها: (نصار، 2017، صفحة 84)

- **القصف الإلكتروني** :ويقصد به استهداف وتدمير المواقع الإلكترونية، وقواعد البيانات، والبنى التحتية للمعلومات.
- **إدارة العمليات الإرهابية** :من خلال استخدام الشبكة المعلوماتية لتنسيق وتنفيذ الهجمات، وتبادل المعلومات بين الجهات المنفذة.
- **الحرب النفسية والإعلامية** :عبر بث الشائعات ونشر المعلومات المضللة بهدف إثارة الخوف والقلق بين السكان.
- **الحرب الإعلامية الرقمية** :والتي تُمارَس من خلال التأثير في الرأي العام المحلي والدولي عبر المنصات الإلكترونية.

ويُعد الابتزاز والتشهير الإلكتروني من أبرز مظاهر الإرهاب السيبراني في العراق، حيث يُستغل ضعف الوعي الرقمي وانتشار الحسابات المزيفة على مواقع التواصل الاجتماعي في تنفيذ هذه الأفعال، مما يعرّض الأفراد والمؤسسات لمشكلات أمنية واجتماعية واقتصادية معقدة يصعب التعامل معها بوسائل تقليدية. ان تنظيم الجماعات الإرهابية استخدم مجال عالم الرقميات في الهجمات الإرهابية بواسطة التكنولوجيا وتجنيد العناصر الإرهابية ونشر الدعاية داخل العراق وخارجة عن طريق الانترنيت. (كمال، 2022، صفحة 24) يمكن القول إن العراق، منذ عام 2003، واجه موجة متصاعدة من الهجمات الإرهابية التي شكلت إحدى السمات البارزة لحالة عدم الاستقرار الأمني والسياسي وقد تنوعت هذه الهجمات من حيث الوسائل والأساليب، لكنها ظلت في معظمها تعتمد على العنف المادي المباشر كوسيلة لإضعاف مؤسسات الدولة وتقويض سيادتها.

ب- الدعاية الرقمية السيبرانية:

تُستخدم وسائل الإعلام في كثير من الأحيان لنشر معلومات مشوهة أو مضللة بهدف تشكيل قناعات الأفراد والتأثير في قراراتهم. وقد تُوظف هذه الدعاية في سياقات سياسية أو إعلامية أو تجارية. وتُعدّ أخطر أشكال الدعاية تلك التي تتخفى وراء قناع الموضوعية، فلا يُعرف مصدرها الحقيقي، ولا يُدرك المتلقّون حقيقتها، مما يجعلها تتسلل خفية بين تدفقات المحتوى الإعلامي. ويكمن خطر هذا النوع في قدرته على التأثير العميق في الرأي العام، نظراً لاعتماده على معلومات غير دقيقة أو زائفة تُبنى عليها مواقف وآراء

قد تكون مضلِّلة أو مضرة. (القادر، 2020، الصفحات 31-71) تكتسب الدعاية فاعلية وتأثيرًا أكبر في المجتمعات التي تفتقر إلى المعرفة الكافية بمختلف جوانب الحياة. فعلى سبيل المثال، تُسهم الثقافة السياسية في تمكين الأفراد من التمييز بين الحقائق والادعاءات الزائفة التي قد تروجها بعض الدول المعتدية الساعية إلى استغلال خيرات الشعوب. كما تسهم المعرفة الاقتصادية في الحد من تأثير الدعاية السلبية التي تُصمم خصيصًا للترويج لمنتجات أو مصالح معينة دون مراعاة للحقيقة أو المصلحة العامة. (التميمي، 2015، صفحة 124) ان المعلومات الوهمية موجودة في العديد من الدول، ولكنها بدأت تتفاقم في العراق بشكل واضح ومكشوف وخصوصاً في الفترة التي تسبق الانتخابات بوجود سماسرة يقومون برفع اي "هاشتاك" لترند تويتر، بأسعار تبدأ من 200 دولار صعودا مع وجود خيارات بعدد التغريدات التي ترافق كل "هاشتاك" والتي تعتبر عاملا في زيادة الاسعار. أن شبكات التواصل الاجتماعي بأشكالها المختلفة، لعبت دورا كبيرا في ايجاد حركة مرور واضحة لهذه الاخبار بصورة او اخرى، على الرغم من أن هذه المنصات تعتبر نفسها منافذ محايدة للمعلومات والاخبار. (https://ina.iq/ar/local/138134--.html?utm، 2021) يمكن القول ان الدعاية تعزز الاستقطاب الطائفي والسياسي مما يؤدي الى اضعاف اللحمة الوطنية العراقية.

ت- التأثير على الانتخابيات والعمليات الديمقراطية:

الأمن السيبراني أصبح أحد العوامل الحاسمة في حماية نزاهة الانتخابات السياسية في العصر الرقمي. فمع تطور التكنولوجيا، أصبحت العمليات الانتخابية عرضة لهجمات سيبرانية تهدف إلى التأثير على النتائج أو زعزعة ثقة المواطنين في النظام الديمقراطي. ومع تزايد الاعتماد على الأنظمة الإلكترونية وإدخال مفاهيم الحوكمة الرقمية في إدارة الانتخابات، أصبحت العملية الانتخابية في العراق أكثر عرضة للتهديدات السيبرانية، مما يشكّل تحديًا حقيقيًا أمام ضمان النزاهة والشفافية، لا سيما في ظل ضعف البنية التحتية للأمن الرقمي. تُعد آلية نقل نتائج التصويت عبر منظومة الاتصال الفضائي (VSAT) إحدى نقاط الضعف، ورغم اعتمادها كبديل احترازي عن شبكة الإنترنت للحد من مخاطر الاختراق، إلا أنها لا تضمن الحماية الكاملة، خصوصًا في مواجهة جهات تمتلك قدرات متقدمة للتلاعب بالبيانات الانتخابية. يُحتّم هذا الواقع على المفوضية العليا وجهاز الأمن الوطني تعزيز إجراءات الحماية السيبرانية، عبر توفير تقنيات متطورة، وتدريب كوادر بشرية مؤهلة، وتبني نهج استباقي في رصد التهديدات والتعامل معها. ونظرًا لحداثة تجربة العراق في هذا المجال، تبرز الحاجة إلى الانفتاح على التعاون الدولي، وتبني استراتيجية وطنية

متكاملة تشمل تأسيس مراكز بحثية متخصصة في أمن المعلومات والانتخابات، تنظيم برامج تدريبية مستمرة، وتخصيص موازنات كافية لتحديث الأنظمة والبرمجيات الأمنية. إن تحقيق الأمن السيبراني بات عنصرًا جوهريًا في صون العملية الانتخابية وضمان مصداقيتها، بما يعزز ثقة المواطنين بالمؤسسات الديمقراطية ويحمي الإرادة الشعبية من التلاعب الإلكتروني. (خضوري، 2021) وأول رد فعل لحماية الانتخابات العراقية من الاختراق السيبراني تم تشكيل لجنة سيبرانية خاصة ضمن "اللجنة العليا لتأمين انتخابات مجالس المحافظات" لعام 2023 تضم مجموعة من الخبراء بمهام فنية، بهدف حماية الأجهزة المستخدمة في العملية الانتخابية وضمان سلامة السجلات والعدّ والفرز كما تم فحص جميع أجهزة المفوضية والتأكد من جاهزيتها التقنيّة وأمنها الإلكتروني بإشراف وحدات أمنية خاصة. (jasssim, 2023)صفوة القول إن الأمن السيبراني في العراق ليس مجرد مسألة فنية، بل هو عنصر رئيسي في الحفاظ على نزاهة العملية الديمقراطية وشرعيتها. من تسريبات البيانات إلى تدخل المحتمل من جهات داخلية وخارجية، ثم التعدد للحلول الوقائية مثل تشكيل لجان فنية وإجراءات أمنية متقدمة كل ذلك يوضّح كيف يشكل الأمان السيبراني عمودًا أساسيًا في تعزيز الثقة في الانتخابات وبخلافة سيكون هناك تأثير كبير على العملية السياسية واستقرارها.

ج- استهداف الشركات والمؤسسات الحكومية

تُعد المؤسسات الحكومية والشركات الكبرى أهدافًا رئيسية للهجمات السيبرانية، حيث يلجأ المهاجمون إلى أساليب متعددة مثل البرمجيات الخبيثة، والتصيّد الاحتيالي، وأحيانًا استغلال الفساد الداخلي لاختراق الأنظمة والوصول إلى معلومات حساسة. وقد تؤدي هذه الهجمات إلى تسريب بيانات تؤثر بشكل مباشر على السياسات الاقتصادية والإدارة المالية، مما يشكل تهديدًا حقيقيًا للأمن القومي. وغالبًا ما تُوجَّه هذه الهجمات نحو الوزارات والهيئات الاقتصادية الكبرى باستخدام تقنيات اختراق متطورة، ما يُسفر عن زعزعة استقرار الدولة وإضعاف قدرتها على إدارة شؤونها المالية والاقتصادية بفعالية. (حمد، 2014، صفحة 10) وفي شهر أيلول 2019 تعرض نحو (30) موقعاً الكترونياً تابعاً للحكومة العراقية للاختراق مستهدفاً جهاز الامن الوطني ووزارتي الداخلية والصحة وثم تبنى عملية اختراق من جانب المخترقون اطلقوا على انفسهم "ماكس برو" تحدثوا عن عمليات ابتزاز وتسريب معلومات وبيعها تتعلق بالأمن الوطني من جانب اخر. (العلي، 2025، الصفحات 190-191)

2- الاستراتيجية العراقية للأمن السيبراني

أعلنت مستشاريَّة الأمن الوطني عن (إستراتيجية الأمن السيبراني العراقي) منذ 2017، لتوفير التدابير المتماسكة والإجراءات الإستراتيجية لضمان أمن وحماية الوجود العراقي في الفضاء السيبراني، وحماية البنية التحتيَّة الحيويَّة للمعلومات، وبناء ورعاية مجتمع انترنت موثوق فيه، وحدد التهديدات السيبرانيَّة الرئيسة في الجريمة الإلكترونية، والإرهاب الإلكتروني، والصراع السيبراني، والتجسس السيبراني، الى جانب إساءة معاملة الاطفال واستغلالهم الكترونياً، وشددت الاستراتيجية على ضرورة تقييم مواطن الضعف الوطنية في المجال السيبراني وقياس الاثار والفرص، بهدف الاسهام في احداث تشريعات شاملة لمكافحة الجريمة السيبرانية والتدابير المضادة للتهديد السيبراني، وتطوير امكانات الامن السيبراني على جميع مستويات الدولة في العراق. وقد وضعت الاستراتيجية خريطة طريق تفصيليَّة من ثمانية محاور، متمثلة بالحكومة الفعالة، والإطار التشريعي والتنظيمي، وأطار تكنولوجيا الأمن السيبراني، وثقافة الامن السيبراني وبناء القدرات، والبحث والتطوير نحو الاعتماد على الذات، والامتثال والتنفيذ، والجاهزية لحوادث الأمن السيبراني، الى جانب التعاون الدولي. وجرى الإعلان عن فريق وطني مشترك مختص للاستجابة للحوادث السيبرانية وحماية البنية التحتية للأنترنت ونشر الوعي في مجال حماية الخصوصية والحماية الذاتية للأفراد والمؤسسات على الانترنت يعمل تحت إشراف مستشارية الأمن الوطني العراقي. 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، وتحقيق الرصانة والموثوقية للأنظمة الالكترونية، وتعزيز ثقة المواطن بالمؤسسات والارتقاء بمستوى العراق دولياً في مجال الامن السيبراني لتشجيع تطوير الخدمات الالكترونية ودعم مشروع أتمته الخدمات والحكومة الالكترونية. 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. كما 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. (صفد، 2021) فأن استراتيجية الأمن السيبراني في العراق تهدف إلى حماية الفضاء السيبراني الوطني من التهديدات والهجمات الإلكترونية، وتوفير بيئة رقمية آمنة تدعم الامن الوطني، والتنمية الاقتصادية، والاستقرار السياسي في العراق. هذه الاستراتيجية تُعد جزءاً أساسياً من التوجهات الوطنية نحو التحول الرقمي وبناء القدرات التكنولوجية. وهناك عدة تحديات تواجة الاستراتيجية منها ضعف البنية التحتية التكنولوجية، ضعف تشريعات الامن السيبراني، غياب الامن الإلكتروني جعل العراق يعاني من انكشاف استراتيجي حيال أغلب بلدان العالم ومهد الطريق لهم لاختراقه والتجسس على البيانات والمعلومات بمنظومته الأمنية. (صليبي، 2024، صفحة 516)

الخاتمة والاستنتاج:

بعد الدراسة والبحث في تأثير الامن السيبراني على الاستقرار السياسي في العراق توصلنا الى ما يلي

أولا: الاستنتاجات

1- ضعف التشريعات الخاصة بالأمن السيبراني.
2- أصبح الفضاء السيبراني يشكّل ساحة متجددة ومعقدة للتهديدات الأمنية التي تؤثر بشكل مباشر على الاستقرار السياسي في العراق.
3- ظهور مخاطر متعددة استهدفت البنى التحتية الحيوية، والقطاعات الاقتصادية، والقطاعات الدفاعية.
4- بات الأمن السيبراني عنصراً محورياً من مكونات الأمن القومي العراقي، وركيزة أساسية في الحفاظ على سيادة الدولة واستقرارها.
5- على الرغم من محدودية القدرات التقنية، والتحديات اللوجستية والتنظيمية التي واجهتها الدولة العراقية خلال العقود الماضية، إلا أن الحكومة اتخذت سلسلة من السياسات والاستراتيجيات الرامية إلى تعزيز أمن الفضاء السيبراني، وتقليص أثر الهجمات الإلكترونية المحتملة.

ثانياً: التوصيات:

1- تطوير البنية القانونية والتنظيمية للأمن السيبراني في العراق.

2- – تفعيل التعاون الدولي مع الشركاء الإقليميين والدوليين في مجالات تبادل المعلومات، والاستجابة للحوادث السيبرانية، ومكافحة الجريمة الإلكترونية.

3- تدريب وتأهيل الكوادر البشرية المتخصصة في الامن السيبراني، ورفع مستوى الوعي المجتمعي والإعلامي بمخاطر الفضاء السيبراني.

4- دعم الجامعات ومراكز البحوث لإنشاء برامج دراسات عليا متخصصة في الأمن السيبراني والسياسة الرقمية.

References:

https://www.academicblock.com/world-affairs/modern- (2023) Academic Block. Academic Block. .*diplomacy/cybersecurity-and-foreign-policy*

Weaponizing information systems january, 2020). 5) Atif Ahhmad, humza naseer Desouza. for political disruption: The Actor, Lever, Effects, and Response Taxonomy (ALERT). .*security & computers*

proceeding of the 11th internantion conferrence and security. .(2016) Boston university. USA: Boston university .

Cybellium Ltd. *cybersecurity training for employees.* .(2023) Cybellium.

Iraq forms a special cybersecurity committee to ensure NOV, 2023). 10) Hoda jasssim. Aletihad: https://en.aletihad.ae/news/mena- *elections' safety, integrity.* world/4441900/iraq-forms-a-special-cybersecurity-committee-to-ensure-elect?utm

.(2010) .*https://en.wikipedia.org/wiki/Regime_theory*

How political regimes affect national cybersecurity: the polity flux effect. .(2022) Jan kiliner. .*Democratazation*

اسماعيل ابوضيافة. (2029). الفضاء السيبراني والتحول في مفاهيم القوة والصراع. *مجلة العلوم السياسية*، صفحة 1016.

باسم علي خريسان. (2020). الفضاء السيبراني: حتمية الاتصال وتحدي التواصل مع الاخر. *مركز الدراسات الاستراتيجية والدولية*.

بد الرزاق التميمي. (2015). *الدعاية والشائعات والرأي العام رؤية معاصرة*. عمان: دار اليازودي.

جهاد صحراوي. (2021). الفضاء السيبراني واشكالية الحرب النفسية للمعلومات عبر وسائل التواصل الاجتماعي. *مجلة الف*.

حسين عبد القادر. (2020). *الرأي العام والدعاية وحرية الصحافة*. مصر: وكالة الصحافة العربية.

سامر خضوري. (17 سبتمبر, 2021). *الامن السيبراني وتحدياته على انتخابات 2021 في العراق*. تم الاسترداد من كتابات: https://kitabat.com/%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A-%D9%88%D8%AA%D8%AD%D8%AF%D9%8A%D8%A7%D8%AA%D9%87-%D8%B9%D9%84%D9%89-%D8%A3%D9%86%D8%AA%D8%AE%D8%A7%D8%A8%D8%A7/

شرين فهمي. (2023). الجهود الدولية لمواجهة مخاطر الإرهاب السيبراني. *مجلة شؤون عربية*.

عادل عبد الصادق. (2016). *العلاقات الدولية والفضاء الالكتروني*. مصر: المركز العربي.

علي صفد. (2021). ماواقع الامن السيبراني في العراق. *صحيفة الصباح*.

غادة نصار. (2017). *الارهاب والجريمة الإلكترونية*. مصر: دار العربي للنشر.

فارس محمد العمارات، ابراهيم الحماصصة. (2024). *الامن السيبراني المفهوم وتحديات العصر*. الاردن: دار الخليج.

فراس محمد عمارات. (2022). *الامن السيبراني*. الاردن: دار الخليج.

محمد كمال. (2022). *الارهاب السيبراني عندما يستخدم الارهابي الكيبورد بدلاً من القنبلة*. القاهرة: دار كليم للنشر.

منال البلقاسي. (2024). *تامين التهديدات السيبرانية تحت المجهر الرقمي*. العيبكان للنشر.

نسرين رياض شنشول ، انور حامد حمد. (2014). *الأمن السيبراني وحماية الاقتصاد العراقي*. العراتق: مركز البيان للدراسات والتخطيط.