

المؤتمر الدولي الرابع

## استراتيجية الأمن الوطني العراقي في تعزيز التنمية المستدامة



المؤتمر الدولي الرابع

## استراتيجية الأمن الوطني العراقي في تعزيز التنمية المستدامة

## استراتيجية الأمن الوطني العراقي في تعزيز التنمية المستدامة

تحت شعار "استراتيجية وطنية فاعلة لتنمية مستدامة"، افتتح المؤتمر عميد الكلية الأستاذ المساعد الدكتور عادل عبد الجمزة جليل المحترم بكلمة أشار فيها إلى أن الدول التي تعاني من الفقر والبطالة وعدم الاستقرار، تعاني أيضاً من تهديدات أمنية كبيرة، وفي المقابل فإن الاستثمار في التعليم والصحة والبيئة التحتية يسهم بشكل مباشر في بناء مجتمع آمن ومستدام. مؤكداً أن الأمن ليس حصن من الفولاذ، إنما هو منظومة متكاملة من القيم والمؤسسات والاستراتيجيات والسياسات التي تهمي الوطن وتضمن مقدراته، موضحاً أن التنمية ليست مجرد أرقام ومؤشرات اقتصادية، بل هي عملية شاملة تستهدف الإنسان، وتؤمن بقدراته، مبيناً أن الأمن الوطني لا يقتصر على حماية حدودنا، ومواجهة المخاطر الإرهابية، أو التهديدات الخارجية فقط، بل يجب أن ندرك أن الأمن ينطلق من داخل مجتمعاتنا، إذ أن الأمن الوطني لا يتحقق عبر القوة العسكرية أو الامتيازات السياسية فحسب، بل يكون له زخم حقيقي، عندما يتداخل مع مفهوم التنمية المستدامة، فالأمن الوطني لا يتفصل عن التنمية فهما وجهان لعملة واحدة.

إن الاستفادة من الخيرات والموارد اللازمة لتحقيق التنمية المستدامة في العراق، فضلاً عن تنويع مصادر الدخل والاعتماد عن الاعتماد الكلي على النفط، عن طريق الاستثمار في القطاعات الأخرى، لتحقيق تنمية مستدامة في العراق، فضلاً عن الحفاظ على البيئة وحماية الموارد الطبيعية، والحد من تلوث الماء والهواء، والذي وصل مستويات كبيرة في العراق، لاسيما في العاصمة بغداد، مع التأكيد على تعزيز مشاركة المرأة والشباب في جميع أبعاد البيئة المستدامة السياسية، والاقتصادية، والاجتماعية في العراق، والعمل في البرلمان العراقي لإصدار التشريعات المناسبة للمشاركة المستدامة، فضلاً عن إيجاد البيئة السياسية، والاقتصادية، والاجتماعية المناسبة للتنمية المستدامة في العراق، عن طريق مكافحة الفساد، وتقليل البيروقراطية في الإدارة والمؤسسات.



كلية العلوم السياسية-جامعة بغداد  
بالتعاون مع مستشارية الأمن القومي



استراتيجية الأمن الوطني العراقي

في تعزيز التنمية المستدامة



❖ أعمال المؤتمر الدولي الرابع:

استراتيجية الأمن الوطني العراقي في تعزيز التنمية المستدامة

في كلية العلوم السياسية - جامعة بغداد

بالتعاون مع مستشارية الأمن القومي

الإعداد والتحرير:

أ.م.د. أحمد عدنان الميالي

الإخراج الفني:

م.م. سهاد حميد ذياب

التدقيق اللغوي:

م.م. حسين فاضل ملوح

٢٠٢٤ م



## فهرس المحتويات

- ١١ كلمة السيد رئيس اللجنة التحضيرية - عميد كلية العلوم السياسية – جامعة بغداد  
أ.م.د. عادل عبد الحمزة ثجيل المحترم
- ١٣ المقدمة: بقلم معاون عميد كلية العلوم السياسية – جامعة بغداد.....  
أ.م.د. أحمد عدنان الميالي
- ١٥ التأطير الاستراتيجي للأمن والتنمية: لتحقيق استقرار مستدام في العراق.....  
أ.د. خميس دهام حميد، د. إسراء عبد علي كاظم
- ٣٨ معوقات تحقيق الأمن المستدام في العراق وسبل تعزيزه.....  
أ.د. طارق عبد الحافظ الزبيدي
- ٦٠ جدلية العلاقة بين الأمن الوطني والتنمية المستدامة: التحديات والفرص.....  
أ.د. عمار حميد ياسين، أ.د. عبيدسهم مهدي
- ٩٣ الضرورات الفكرية لبناء ثقافة استراتيجية حاكمة لاستراتيجية الأمن الوطني  
العراقي: التنمية المستدامة أنموذجًا.....  
أ.د. دينا محمد جبر
- ١١١ خطاب التنمية وما بعدها.. مفارقة النماذج الوافدة والبيئات المتباينة.....  
أ.د. عبد القادر دندن
- ١٣٨ تحديات استراتيجيات الأمن الوطني في تعزيز التنمية المستدامة.....  
م.م. فاطمة محمد علي طالب، أ.د. أزهار عبد الله حسن

## فهرس المحتويات

- ١٥٩ ..... أمن الطاقة واستراتيجية الأمن الوطني العراقي
- أ.د. رياض مهدي الزبيدي
- ٢٠٠ ..... سياسة الأمن السيبراني الدولية في العراق بعد عام ٢٠٠٥ في ظل التحديات الراهنة
- أ.م.د. إبراهيم حربي إبراهيم
- ٢٣١ ..... تداعيات الأمن السيبراني على الأمن الوطني العراقي
- أ.م.د. بدرية صالح عبد الله
- ٢٦٢ ..... جدلية العلاقة الترابطية بين الأمن والتنمية من منظور تعاوني: العراق أنموذجًا
- أ.م.د. سداد مولود سبع، م.د. ماجد حميد خضير
- ٢٨٠ ..... آليات إدارة تهديدات الأمن الوطني العراقي: الهجمات السيبرانية أنموذجًا
- د. علاء عبيس راضي الجبوري، م.م. عذراء محمد عبد الرضا
- ٢٠٥ ..... تمكين المرأة العراقية - رؤية جديدة لإستراتيجية التنمية المستدامة
- أ.م.د. أورداد محمد مالك كمونه
- ٣١٩ ..... دور استراتيجية الأمن الوطني العراقي في تحقيق أهداف التنمية المستدامة: التحديات والفرص
- م.د. أثير هاني حرز
- ٣٥٦ ..... التنمية المستدامة ودورها في تعزيز الأمن وبناء المجتمعات السلمية: دراسة حالة العراق
- م.د. دعاء نوري فليح
- ٣٩١ ..... القدرات السيبرانية وإدارة التهديدات الأمنية في العراق "دراسة تحليلية"
- م.د. زمن ماجد عودة، م.د. هبة نصير عبد الرزاق

## فهرس المحتويات

- ٤٠٨ .....جدلية الأمن والتنمية (علاقة التأثير والتأثر)..... م.د. إياد مالك عبد المجيد
- ٤٢٣ .....الرهانات الاستراتيجية العراقية للتنمية المستدامة وانعكاساتها على الأمن الوطني م.د. فراس عباس هاشم مجيد
- ٤٥٦ .....دور سياسة حماية المنتجات الوطنية في دعم الاقتصاد العراقي بعد عام ٢٠١٠..... م.د. سامرناض خضير، م.د. علياء محمد طارش
- ٤٨٨ .....التكنولوجيا السبيرانية كأداة لتعزيز التنمية المستدامة وحماية الموارد الرقمية..... م. فاطمة رضا عطية، د. إسراء عبد علي كاظم
- ٥٠٥ .....اسناد جهود الأمن الوطني في تعزيز سبل التنمية المستدامة..... م.م. عبد الخالق جواد عبد الحسين
- ٥١٧ .....تمكين الشباب في استراتيجية الأمن الوطني العراقي ودورها في تحقيق التنمية المستدامة..... م.م. مقدم جابر أحمد، م.م. خولة نصير عبدالرزاق
- ٥٣٤ .....التنمية السياسية ودورها في تعزيز التعايش السلمي..... م.م. أماني محمد صبري، م.م. حسناء محمد مهدي
- ٥٥٣ .....الأمن والتنمية: علاقة تكاملية واستراتيجية مستدامة في سياق البناء الوطني العراقي أ.د. عمر جمعة، م.م. سيف ضياء دغير
- ٥٨٤ .....التنمية المستدامة والمواطنة في العراق بعد عام ٢٠٠٣ دراسة في التأثير والتأثر..... م.م. صبا حميد صالح التميمي



## فهرس المحتويات

٦٢٣	استراتيجيات الأمن والتنمية المستدامة.....	م.م. نور عبد السلام حسن
٦٣٩	دور السياسة العامة في تحقيق التنمية المستدامة: العراق أنموذجاً.....	م.م. بلسم علاء الدين حسن قاسم، م.م. زهراء حيدر جاسم
٦٦٠	التحديات الأمنية في العراق وتأثيرها على جهود التنمية المستدامة.....	م.م. بنين سعد صافي م.د. ايمان جواد عبد الكاظم
٦٧٦	استراتيجية بناء التنمية الاقتصادية في العراق: دراسة مقارنة مع التجربة الماليزية...	م.م. فاطمة محمد رضا
٧١٥	التحديات الاستراتيجية للأمن الوطني العراقي في تعزيز التنمية المستدامة بعد العام ٢٠٠٣.....	م.م. مسرة علي رشك
٧٤٠	التنمية المستدامة والمجتمع المحلي: دراسة في طبيعة التأثير والتأثر.....	م.م. رواء كاظم فرهود
٧٦٠	جدلية الأمن والتنمية: دراسة مفاهيمية.....	م.م. زمن جاسم محمد
٧٧٨	استراتيجية الأمن السبراني ودورها في تحقيق أهداف التنمية المستدامة: العراق أنموذجاً.....	م.م. شيماء محمد ناصر

## فهرس المحتويات

- ٨١٤ ..... التلازم بين الأمن الوطني والتنمية لتحقيق الاستدامة
- م.م. إيمان عباس مهدي
- ٨٣٥ ..... التنمية المستدامة في العراق بعد عام ٢٠١٥: الفرص والتحديات
- م.م. زهراء صالح مهدي
- ٨٦٠ Reinforcements of Cyber security mechanisms to enhance  
Sustainability and Strategic Security
- Mohammed Alaa H. Altemimi, PhD

استراتيجية الأمن السيبراني ودورها في تحقيق أهداف التنمية المستدامة:

العراق انموذجاً

م.م شيماء محمد ناصر

كلية العلوم السياسية - جامعة بغداد

shaima.mohammed@copolicy.uobaghdad.edu.iq

الملخص:

يتعرض العراق بين الحين والآخر إلى هجمات سيبرانية معقدة، تستهدف مؤسساته وبنية الرقمية، من قبل جماعات متطرفة وهاكرز غير معروفين، يُسهم ذلك في خلق تحديات لتحقيق أهداف التنمية المستدامة، إذ أصبحت أهمية الأمن السيبراني ليس مجرد حاجة تقنية، بل ضرورة استراتيجية لدعم جهود تحقيق التنمية المستدامة. على هذا النحو يهدف البحث التطرق إلى كيف يمكن للأمن السيبراني أن يحقق أهداف التنمية المستدامة في العراق؟ عبر تحليل أهداف التنمية المستدامة التي أدرجتها الأمم المتحدة، والتحديات السيبرانية التي تواجه العراق، وينظر البحث في العلاقة الترابطية ما بين الأمن السيبراني وتحقيق التنمية المستدامة. استخدمت الباحثة المنهج التحليلي والاستقرائي في تحليل محاور البحث، وخلص البحث بأثبتات الفرضية التي انطلق منها كأساس منهجي أن تعزيز استراتيجية الأمن السيبراني يُعد خطوة أساس لت تحقيق أهداف التنمية المستدامة، إذ أنه يوفر بيئة آمنة وموثوقة للابتكار والنمو الاقتصادي، ويحمي البنية التحتية ويعزز الثقة في المؤسسات الحكومية والخاصة، وأوصى البحث على ربط استراتيجية الأمن السيبراني بأهداف التنمية المستدامة، وتعزيز الدبلوماسية السيبرانية، وبما يخدم أمن البنى التحتية واستمرارية عمل هذه القطاعات، ويمكن للعراق الاستفادة من تجارب الدول التي قامت بتطبيق هذا النهج. الكلمات المفتاحية: التنمية المستدامة، الأمن السيبراني، البنية التحتية، التهديدات السيبرانية، الدبلوماسية السيبرانية.

**Abstract:**

Iraq often meets sophisticated cyberattacks started by extremist groups and unidentified hackers, targeting its institutions and digital infrastructure. These attacks pose significant obstacles to achieving Sustainable Development Goals (SDGs), underscoring the critical role of cybersecurity as a strategic imperative that extends beyond its technical functions to support development initiatives. This research explores the relationship between cybersecurity and the attainment of SDGs in Iraq. It analyzes the United Nations' SDGs and examines the country's cybersecurity challenges, highlighting the interconnection between advancing cybersecurity measures and fostering an environment conducive to sustainable development. Employing an analytical and inductive approach, the study confirms its central hypothesis: enhancing cybersecurity strategies is a fundamental step toward realizing sustainable development goals. Robust cybersecurity provides a secure and dependable foundation for innovation, economic growth, critical infrastructure protection, and increased trust in public and private institutions. The findings advocate integrating cybersecurity strategies with sustainable development aims and emphasize the importance of advancing cyber diplomacy to protect infrastructure and keep the functionality of critical sectors. Furthermore, Iraq can draw valuable insights from the experiences of countries that have successfully implemented such approaches to strengthen sustainable development and safeguard digital resources.

**Keywords:** Sustainable Development, Cyber security, Infrastructure, Cyber Threats, Cyber Diplomacy.

## المقدمة:

يحتل الأمن السيبراني (Cybersecurity) وما يرتبط به من قضايا التهديدات السيبرانية المرتبة الرابعة ضمن أبرز المخاطر التي تهدد العالم، وخاصة بعد صعود تطبيقات موازية للتكنولوجيات البازغة مثل: تطبيقات الجيل الخامس 5G، وتطبيقات الذكاء الاصطناعي AI، وتطبيقات الحوسبة السحابية cloud computing .

وقد أشارت نتائج أعمال المؤتمر الدولي للاقتصاد الرقمي والتنمية المستدامة بمعهد التخطيط القومي في نيسان ٢٠٢١، وكذلك الأمم المتحدة ووكالاتها المتخصصة إلى أن التهديدات السيبرانية يمكن أن تهدد، أو تهدر جهود تحقيق أهداف التنمية المستدامة العالمية، وأهداف التنمية المستدامة الوطنية على مستوى العالم.

هذه المخاطر والتهديدات دفعت العديد من الدول إلى تبني استراتيجيات وخطط للأمن الوطني السيبراني، مثل الصين، والولايات المتحدة الأمريكية، والإمارات العربية المتحدة، والسعودية هدفها الأساس حماية اقتصاديات وسلاسل القيمة الرقمية الصاعدة من المخاطر السيبراني التي يمكن ان تهدر جهود التنمية المستدامة في هذه الدول.

## أهداف البحث:

من أهداف البحث توضيح مفاهيم الأمن السيبرانية والتنمية المستدامة المتعلقة بالعراق، وتوضيح العلاقة ما بين الأمن السيبراني وتحقيق أهداف التنمية المستدامة من مختلف الجوانب. عبر تشخيصها للواقع ورصد الأبعاد والمؤشرات لتساعد على تكوين رؤية واضحة واتخاذ القرار المناسب.

## أهمية البحث:

تكمن أهمية البحث في أنه يتناول العلاقة الحيوية بين الأمن السيبراني وتحقيق التنمية المستدامة في العراق، في ظل تزايد حجم التهديدات الالكترونية والمخاطر الأمنية في الفضاء الإلكتروني والحاجة الماسة إلى حماية الأنظمة الرقمية والبيانات الحيوية من الهجمات

## استراتيجية الأمن الوطني العراقي في تعزيز التنمية المستدامة.....

السيبرانية التي قد تعيق مسار التنمية. كذلك يسعى البحث إلى تقديم حلول واستراتيجيات لتعزيز الأمن السيبراني بما يضمن استمرارية تحقيق الأهداف المتعلقة بالاستدامة الاقتصادية والاجتماعية والبيئية.

### إشكالية البحث:

في ظل التحول الرقمي السريع وتعرض العراق بشكل متزايد لهجمات سيبرانية تستهدف مؤسساته وبنيتة التحتية الرقمية، باتت التنمية المستدامة تواجه خطراً حقيقياً نتيجة لهذه الهجمات. وعليه تطرح إشكالية رئيسة: ما مدى فاعلية استراتيجيات الأمن السيبراني الحالية في العراق في مواجهة التحديات السيبرانية التي قد تعيق تحقيق أهداف التنمية المستدامة؟ وماهي الاستراتيجيات التي يجب اتباعها لتعزيز هذا الدور بشكل مستدام ومتكامل؟

### فرضية البحث:

يسعى البحث لأثبات فرضية مفادها أن تعزيز استراتيجية الأمن السيبراني يعد خطوة أساسية لتحقيق أهداف التنمية المستدامة، إذ أنه يوفر بيئة آمنة وموثوقة للابتكار والنمو الاقتصادي، ويحمي البنية التحتية، ويعزز الثقة في المؤسسات الحكومية والخاصة.

### منهجية البحث:

تناول البحث المنهج التحليلي والاستقرائي في قراءة البيانات ومناقشتها.

### هيكلية البحث:

تضمن البحث فضلاً عن المقدمة والخاتمة والنتائج والتوصيات ثلاثة محاور:

المحور الأول: الأمن السيبراني (المفهوم والعناصر).

المحور الثاني: التنمية المستدامة (المفهوم والتحديات).

المحور الثالث: دور استراتيجية الأمن السيبراني في تحقيق أهداف التنمية المستدامة في العراق.

## المحور الأول: الأمن السيبراني (المفهوم والعناصر)

### أولاً: مفهوم الأمن السيبراني:

شاع استخدام مصطلح (الأمن السيبراني) في السنوات الأخيرة على نطاق واسع، وأخذ يحظى بشعبية متزايدة بعد أن استخدمه الرئيس الأمريكي السابق (بارك أوباما) في العام ٢٠٠٩ في خطابه الذي دعا فيه الشعب الأمريكي إلى الاهتمام بالأمن السيبراني لتعزيز الأمن الوطني الأمريكي<sup>[١]</sup>.

وقد عد التهديد القادم من الفضاء السيبراني من أهم التحديات الأمنية والاقتصادية التي تواجه الولايات المتحدة الأمريكية، ولهذا جعله في مقدمة اهتماماته، وعين لهذا الغرض مسؤول عن الأمن السيبراني، ويكون عضواً في مجلس الأمن القومي، ويكون على اتصال وتنسيق دائم معه<sup>[٢]</sup>.

وهناك العديد من التعاريف التي تناولت مصطلح الأمن السيبراني، عرفه أستاذ الاتصالات في جامعة كاليفورنيا (Richard A. Kemmerer) على أنه "عبارة عن وسائل دفاعية من شأنها كشف واحباط المحاولات التي يقوم بها القراصنة "[٣]، كذلك يُعرّف على أنه النشاط أو العملية، أو القدرة، أو الحالة التي يتم بموجبها وعبرها حماية الأنظمة والشبكات والبرامج والاتصالات والمعلومات الواردة فيها، والدفاع عنها ضد الضرر أو الاستخدام غير المصرح به، أو التعديل، أو الاستغلال، وحدد موقع (كسبارسكي Kaspersky) ستة مجموعات للأمن السيبراني وكما يلي<sup>[٤]</sup>:

١. أمن الشبكات Network security: في مواجهة أخطار هجمات متعمدة أو عابرة.
٢. أمن التطبيقات Application security: لتحسين البرمجيات والأجهزة سيبرانياً.
٣. أمن المعلومات Information security: ويرتبط بترتيبات ضمان سلامة وخصوصية البيانات في التخزين والتداول.
٤. الأمن العملياتي: operational security: وترتبط بقواعد حفظ وتداول البيانات.

٥. أمن التعافي واستمرارية الأعمال disaster recovery and business continuity :

ويرتبط بتعزيز قدرات الجهات في إدارة التعامل ، والتعافي من الخطر السيبراني .

٦. أمن التعلم وتركييم الخبرات end user education : بما يعزز قدرات الأشخاص

والمنظمات التي تعرضت للهجمات في استباق وتجنب المخاطر السيبرانية.

يشمل تعريف الأمن السيبراني مجموعة واسعة من التدابير الوقائية التي تهدف إلى الدفاع عن الأصول الرقمية من التهديدات المختلفة. في جوهره، هو تطبيق التقنيات والعمليات والضوابط التي تعمل بشكل تآزري لحماية الأنظمة والشبكات والبرامج والأجهزة والبيانات من مجموعة من الهجمات السيبرانية[٥]. تتجلى أهمية الأمن السيبراني في العصر الرقمي عبر دوره في حماية الخصوصية الشخصية ضد الوصول غير المصرح به وضمان سلامة المعلومات الحساسة.

مع تعمقنا في عالم الأمن السيبراني، من الأهمية بمكان فهم الأنواع المختلفة من التهديدات التي تواجهها المنظمات والأفراد. أحد أكثر أشكال التهديدات السيبرانية انتشارًا هو البرامج الضارة، تشمل هذه الفئة الفيروسات، والديدان، وأحصنة طروادة، وبرامج التجسس، وبرامج الفدية، وكلها يمكن أن تلحق ضررًا كبيرًا بالبنية التحتية الرقمية. يمكن للبرامج الضارة إتلاف البيانات، أو سرقة المعلومات الحساسة، أو منع المستخدمين من الوصول إلى أنظمتهم بالكامل، وغالبًا ما تطالب بفدية لاستعادة الوصول. هناك تهديد كبير آخر وهو التصيد الاحتيالي، وهي طريقة تستغل تقنيات الهندسة الاجتماعية لخداع الأفراد لإفشاء معلومات حساسة، مثل كلمات المرور أو أرقام بطاقات الائتمان. غالبًا ما تتنكر هجمات التصيد الاحتيالي في هيئة اتصالات مشروعة، مما يخدع المستخدمين لتعريض أمنهم للخطر. فضلاً عن ذلك، تمثل هجمات رفض الخدمة (DoS) تهديدًا إلكترونيًا خطيرًا آخر، إذ تحاول الجهات الخبيثة إغراق موقع ويب بحركة مرور مفرطة. يؤدي هذا التدفق من حركة المرور إلى تعطيل العمليات العادية، مما يجعل مواقع الويب غير متاحة للمستخدمين



## استراتيجية الأمن الوطني العراقي في تعزيز التنمية المستدامة.....

الشرعيين ويسبب انتكاسات تشغيلية كبيرة للمؤسسات [٦]. يعد فهم هذه التهديدات أمراً بالغ الأهمية لتطوير استراتيجيات فعالة للأمن السيبراني يمكنها التخفيف من المخاطر المحتملة وحماية الأصول القيمة.

باختصار، الأمن السيبراني هو مفهوم متعدد الأوجه يشمل حماية الأصول الرقمية من مختلف التهديدات، بما في ذلك البرامج الضارة والتصيد الاحتيالي وهجمات رفض الخدمة. وهو أمر حيوي لحماية البيانات الشخصية والتنظيمية، والحفاظ على الثقة في التفاعلات الرقمية، وضمان سلامة الأنظمة التكنولوجية. عبر فهم أنواع التهديدات وتنفيذ تدابير الأمن السيبراني الفعالة، مثل الحماية من الفيروسات وجدران الحماية والتشفير، يمكن للأفراد والمنظمات حماية أنفسهم بشكل أفضل في عالم رقمي متزايد. ومع استمرار تطور التكنولوجيا وتطور التهديدات السيبرانية، ستزداد أهمية الأمن السيبراني، مما يجعله مجالاً أساسياً للتركيز لجميع الذين يتعاملون مع المنصات الرقمية.

ثانياً: عناصر الأمن السيبراني:

### ١. القوة السيبرانية (cyber power):

يُعدّ مفهوم القوة السيبرانية من المفاهيم الجديدة التي احتلت مكانة أكاديمية في أدبيات العلوم السياسية، وبات يُستخدم في توصيف القوة (الصلبة)، أو (الناعمة)، أو (الذكية) وشرحها. ويرجع الفضل في التنظير لهذا المفهوم إلى عالم السياسة الأميركي (جوزيف ناي) الذي عرّف (القوة السيبرانية) على أنها القدرة على تحصيل نتائج مرجوة بواسطة الاعتماد على مصادر المعلومات المرتبطة بالفضاء السيبراني، أي إنها القدرة على استخدام الفضاء السيبراني بهدف إيجاد مزايا للدولة، وتحقيق مصالحها، ومنحها قوة للتأثير في محيطها بما يضمن أمنها القومي. وجادل في كتابه (القوة الناعمة)، أنه في عالم اليوم المتسم بالتطور المتسارع، ما عاد في الإمكان حساب قوة الدولة اعتماداً على العناصر المادية، العسكرية والاقتصادية فحسب، إذ إنّ لتقدم العلم والتكنولوجيا أثراً متناقضة في القوة

## استراتيجية الأمن الوطني العراقي في تعزيز التنمية المستدامة.....

المادية، فقد ظهر مثلاً عدد من التهديدات الأمنية، مثل الإرهاب والجرائم الدولية وانتشار الأوبئة والأمراض السارية، التي تتطلب امتلاك موارد القوة الناعمة لمواجهتها والتصدي لها [٧]، [٨].

وقد أصبح الفضاء السيبراني مجال جديد للتفاعلات الدولية، سواء أكانت تصارعيه أم تعاونية، وأثر ذلك على تغير طبيعة القوة وبروز تهديدات الفضاء الإلكتروني، وأثر بدوره على استراتيجيات الأمن القومي، والسعي إلى الاستحواذ على مصادر القوة داخل الفضاء الإلكتروني لمنع تعرض بنية الدولة التحتية والحيوية للخطر.

### ٢. الفضاء السيبراني:

هو عبارة عن بيئة افتراضية تفاعلية حديثة، يتم إنشاؤها عبر الربط بين أنظمة الحوسبة والشبكات الرقمية، مثل الإنترنت والأجهزة المرتبطة بها. ويطلق عليها (الذراع الرابعة للجيش الحديث) ويتكون الفضاء السيبراني من مجموعة من الحواسيب، الخوادم، قواعد البيانات، البرمجيات، والشبكات التي تتيح الاتصال وتبادل المعلومات بشكل سريع وفعال [٩]. يتجاوز الفضاء السيبراني الحدود الجغرافية التقليدية، مما يسمح بالتواصل بين الأفراد، الشركات، والحكومات في جميع أنحاء العالم. يُعد هذا الفضاء مجالاً حيوياً في العصر الحديث، وقد أصبح هدفاً للصراعات والهجمات السيبرانية وتصفية الخلافات بكل أنواعها بين أطراف الصراع كافة، إلى جانب ذلك تُجرى فيه الكثير من الأنشطة الاقتصادية، والاجتماعية، والسياسية.

### ومن أهم خصائصه:

١. العالمية: يمتد عبر جميع أنحاء العالم ولا يرتبط بحدود جغرافية محددة.
٢. التفاعلية: يسمح بالتفاعل المباشر والفوري بين المستخدمين.
٣. الأمنية: يرتبط بتهديدات أمنية متعددة مثل الجرائم السيبرانية والهجمات الإلكترونية.
٤. الافتراضية: البيئة فيه ليست مادية، ولكنها تعتمد على التكنولوجيا الرقمية.

الفضاء السيبراني بات جزءاً لا يتجزأ من حياتنا اليومية في مختلف المجالات، ويشكل تحديات وفرصاً جديدة في مجالات مثل الأمن، الاقتصاد، والسياسة.

### ٣. الردع السيبراني:

تُعد عملية تحقيق الردع بمفهومه التقليدي أمراً غير ممكن في الفضاء السيبراني سواء على مستوى المفهوم، أو آليات التطبيق نظراً لعدم تماثل القوى، وعدم التناسب بين شدة الهجمات السيبرانية. ويعرف الردع على أنه (منع الأعمال الضارة ضد الأصول الوطنية في الفضاء والأصول التي تدعم العمليات الفضائية) ويرتكز على ثلاث ركائز هي أساس استراتيجية الدفاع السيبراني، وتتمثل في (مصادقية الدفاع، القدرة على الانتقام، الرغبة في الانتقام). هذه الصعوبات تتطلب البحث عن طرق جديدة أو تعريف مرّن للردع في الفضاء السيبراني، وذلك عبر زيادة مرونة الدولة في التعامل مع الهجمات السيبرانية، وتبني خطط جديدة وأنظمة بديلة تحل محل الأنظمة التي تتعرض لهجمات سيبرانية أو تخرج عن الخدمة [١٠].

### ٤. الهجوم السيبراني أو الإرهاب الإلكتروني

كان بدايات استخدام مصطلح الإرهاب الإلكتروني ((cyber terrorism) في الثمانينيات من القرن العشرين من قبل (Barry collin) على أنه (استخدام الانترنت والتكنولوجيا لشن هجوم على الحكومات ويكون ذات أثر تدميري مكافئ للهجمات المادية لتحقيق أهداف سياسية، أو اقتصادية، أو عسكرية، أو دينية، أو ايدلوجية) [١١].

وفي هذا السياق تعرض العراق بتاريخ ٢٦ و٢٧/ أيلول/ ٢٠١٩ إلى هجوم سيبراني من قبل قراصنة طالت قرابة (٣٠) موقعاً حكومياً، أبرزها مواقع وزارة الدفاع والداخلية والخارجية والأمن الوطني والصحة، وقد استفاد المهاجمون من بعض نقاط الضعف فعملوا على تطبيق التغيرات على موقع البحث التي من شأنها توجيه المستخدمين إلى صفحة بحث

## استراتيجية الأمن الوطني العراقي في تعزيز التنمية المستدامة.....

مختلفة، وعلى الرغم من نجاح الجهود المبذولة من قبل المؤسسات الحكومية في استعادة المواقع، إلا أن العملية استغرقت وقتاً طويلاً [١٢].

### ٥. الجريمة السيبرانية:

تعد الجرائم الالكترونية واحدة من أكبر التحديات للبيئة التي ترتكب فيها، وتعرف على: انها مجموعة الأفعال والأعمال غير القانونية التي تتم عبر معدات، أو أجهزة الكترونية، أو شبكات الأنترنت، أو تبث عبرها محتوياتها، وهي ذلك النوع من الجرائم التي تتطلب الامام الخاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها، أو التحقيق فيها، ومقاضاة فاعليها. فهي الجريمة المتصلة باستخدام الحاسوب، أي تصرف غير قانوني يرتكب باستخدام تقنيات المعلومات والاتصالات [١٣].

ومع اعتمادنا بشكل متزايد على المنصات الرقمية للأنشطة الشخصية والمهنية، لا يمكن المبالغة في أهمية الأمن السيبراني. فهو لا يحمي الخصوصية الشخصية فحسب، بل يحمي أيضاً الشركات من الخسائر المالية الكبيرة ويحافظ على الثقة بين المستخدمين في النظام البيئي الرقمي. لذلك، فإن فهم تعريف وأنواع التهديدات وأفضل الممارسات في مجال الأمن السيبراني أمر ضروري لأي شخص منخرط في عالم اليوم المترابط.

### المحور الثاني: التنمية المستدامة (المفهوم والتحديات).

#### أولاً: مفهوم التنمية المستدامة:

أصبحت التنمية المستدامة واحدة من المفاهيم الأساسية في الساحة الدولية، إذ تزايد الوعي بالحاجة إلى إيجاد توازن بين الأبعاد الاقتصادية والاجتماعية والبيئية للتنمية. ومع تصاعد التحديات العالمية مثل التغير المناخي، وفقدان التنوع البيولوجي، والفقر، يبرز هذا المفهوم كإطار توجيهي لتحقيق رفاهية مستدامة للأجيال الحالية والمستقبلية، وعرفتتها الأمم المتحدة في تقرير (لجنة برونتلاند) عام ١٩٨٧ على أنها "التنمية التي تلبّي احتياجات الحاضر

## استراتيجية الأمن الوطني العراقي في تعزيز التنمية المستدامة.....

دون أن تؤثر على قدرة الأجيال على تلبية احتياجاتها" [١٤]، مما يوضح التوجه الشامل الذي يتبناه هذا المفهوم لتحقيق نمو اقتصادي مستدام، وتقديم اجتماعي، وحماية بيئية. وعرفها قاموس ويبستر (webster) على أنها: استخدام الموارد الطبيعية دون أن تسمح باستنزافها، أو تدميرها [١٥]، كذلك عرفتها منظمة التعاون والتنمية الاقتصادية (OECD) بأنها " التنمية التي تسعى إلى تحقيق نمو اقتصادي عبر توازن بين الأبعاد الاجتماعية والاقتصادية والبيئية بطريقة تحقق المنفعة للجميع".

هذه التعريفات تعكس التنوع في رؤى التنمية المستدامة، إذ تتناول تحقيق التوازن بين الأبعاد الاقتصادية والبيئية والاجتماعية لضمان مستقبل مستدام. ثانياً: تحديات الأمن السيبراني من منظور التنمية المستدامة.

في العصر الرقمي، أضحت مسألة الأمن السيبراني من القضايا الحرجة التي تؤثر على الأفراد والمؤسسات والحكومات على حد سواء، وتتطلب معالجة دقيقة ومستدامة. ومع تزايد الاعتماد على التكنولوجيا الرقمية، برزت تحديات جديدة تُهدد الأمن السيبراني في العراق، مما يستدعي تطوير استراتيجيات تساهم في حماية الأنظمة والمعلومات وتدعم الاستدامة. من منظور التنمية المستدامة، لا تقتصر أهمية الأمن السيبراني على حماية البيانات فحسب، بل تتعداها لتشمل المساهمة في بناء بيئة رقمية آمنة تعزز الثقة، وتدعم النمو الاقتصادي، وتضمن العدالة الاجتماعية عبر وصول أمن ومتكافئ للتقنيات.

في الجدول رقم (١) نوضح التحديات الرئيسة للأمن السيبراني في العراق، ويحللها ضمن إطار التنمية المستدامة، إذ يتناول الأبعاد البيئية، والاقتصادية، والاجتماعية والسياسية التي ترتبط بهذه التحديات. عبر هذا التحليل، يمكن تسليط الضوء على كيفية تأثير السياسات والتدابير الأمنية على تحقيق أهداف التنمية المستدامة، مما يعكس أهمية وضع استراتيجية شاملة تساهم في حماية البنية التحتية الرقمية ودعم مستقبل مستدام وآمن.

الجدول (١):

تحديات الأمن السيبراني من منظور التنمية المستدامة

الهدف	التحدي الرئيسي	تهديدات الأمن السيبراني
القضاء على الفقر	ارتفاع معدلات الفقر في العراق يحتل المرتبة (٣٣) على وفق مؤشر البوس العالمي لعام ٢٠٢٣ [١٦].	يعتمد إنهاء الفقر على قدرة الأفراد على الوصول إلى المعلومات على الأنترنت، ومن ثم يمكن تعطيله بسبب الضعف في الوصول إلى الخدمات والفجوة الرقمية بين سكان المناطق الحضرية والريفية [١٧]، إن أغلب الأفراد لديهم نقص الوعي في الأمن السيبراني، لكون هذه المناطق تعاني من ضعف البنية التحتية الرقمية، كذلك أن الهجمات السيبرانية تؤدي إلى عرقلة وصول المساعدات المالية وبرامج الشمول المالي، إذ أن أغلب برامج التخفيف من حدة الفقر التي تستخدمها وكالات المعونة والحكومات تعتمد على رقمته أنظمة تحديد الهوية [١٨].
القضاء على الجوع	نقاط ضعف سلاسل التوريد الغذائية	أصبحت سلاسل الامدادات الغذائية رقمية ومتصلة مما يجعلها عرضة للهجمات الإلكترونية التي قد تعطل نقل الغذاء بين المزارع والمستهلك، والتسبب في اتلاف المخزون الغذائي، ومن الممكن ان تتعرض مراكز البحث والتطوير الزراعي إلى هجمات قد تؤدي إلى سرقة الابتكارات والتكنولوجية المتعلقة بزيادة الإنتاج الغذائي وتعطيل الأبحاث التي تهدف إلى تطوير طرق استدامة للإنتاج الزراعي ، ومع انتشار منصات الدفع الرقمية والبرامج الغذائية المدعومة حكومياً مثل برامج التحويل النقدي ، يؤدي الضعف السيبراني إلى سرقة أموال الدعم والمساعدات الغذائية والوصول غير المصرح به إلى بيانات المستفيدين مما يؤدي إلى نقص الغذاء وزيادة انعدام الأمن الغذائي [١٩].

<p>البيانات الصحية الشخصية تعد من أكثر البيانات حساسية وقيمة، إذ تحتوي السجلات الطبية على معلومات قد تكون ذات صلة بحياة المريض، وإن حماية هذه البيانات على المدى الطويل تحدي كبير والحاجة إلى مخططات حماية يمكنها ضمان سلامة وسرية المعلومات مثل السجلات الطبية [٢٠]. ومن أمثلة هذه الهجمات، الهجوم على مجموع سنغافورة للخدمات الصحية مما أدى إلى سرقة البيانات الشخصية لـ (1.5) مليون مريض، بما في ذلك الوصفات الطبية لرئيس الوزراء (لي هسين لونج) [٢١].</p>	<p>حماية البيانات الصحية الشخصية</p>	
<p>تزايد الهجمات الإلكترونية على المستشفيات والمنظمات الصحية مثل هجمات الفدية (Ransomware) هذه الهجمات تعطل الأنظمة الصحية ومن ثم الوصول إلى الخدمات، مما يضرب بصحة المرضى حتى يتم دفع الفدية، وتؤثر هذه الهجمات على سير عمل قسم الطوارئ، ورعاية الأمراض المزمنة، والرعاية الشخصية لمقدمي الرعاية الصحية [٢٢].</p>	<p>الهجمات على أنظمة الرعاية الصحية</p>	<p>الصحة الجيدة</p>
<p>الأجهزة الطبية المتصلة بالإنترنت تمثل نقاط ضعف محتملة لهجمات سببرانية، إذ يمكن اختراقها والسيطرة عليها، وإن هذا الاختراق يمكن أن يؤدي إلى تغيير إعدادات العلاج أو تعطل الأجهزة، مما يؤدي إلى أخطار جسيمة على حياة المرضى.</p>	<p>الاتصال بين الأجهزة الطبية و إنترنت الأجهزة الصحية IOMT</p>	
<p>مع انتشار التطبيق عن بعد بشكل متزايد، إذ تم استهداف هذه الأنظمة بالهجمات السببرانية سيؤثر على قدرة المرضى على الوصول إلى الرعاية الصحية عن بُعد، مما يتعارض مع هدف تحسين الصحة للجميع [٢٣].</p>	<p>التكنولوجيا السحابية والرعاية الصحية عن بعد</p>	

## استراتيجية الأمن الوطني العراقي في تعزيز التنمية المستدامة.....

<p>الكثير من العاملين في مجال الرعاية الصحية ليس لديهم الوعي بأهمية الأمن السيبراني أو كيفية مواجهة التهديدات، مما يؤدي إلى الوقوع ضحية لهجمات التصيد الاحتيالي، أو تسريب بيانات المرضى، أو انتهاكات أمنية أخرى [٢٤].</p>	<p>نقص الوعي الأمني لدى العاملين في المجال الصحي</p>	
<p>تفتقر المؤسسات الصحية العراقية إلى التمويل الكافي لتطبيق حلول متقدمة للأمن السيبراني، مما يزيد من صعوبة تعزيز أنظمة الحماية ويجعل المؤسسات عرضة للهجمات السيبرانية [٢٥].</p>	<p>تمويل الأمن السيبراني في الرعاية الصحية</p>	
<p>التطبيقات الصحية التي يستخدمها الأفراد لمراقبة صحتهم (مثل تطبيقات اللياقة البدنية) قد لا تلتزم بمعايير الأمان العالمية، فأنها تصبح هدفاً للهجمات، مما قد يعرض بيانات المستخدمين الشخصية للخطر.</p>	<p>خصوصية البيانات في التطبيقات الصحية</p>	
<p>تعد البنية الصحية جزءاً من البنية التحتية الحيوية للدولة، واستهدافها يمكن أن يسبب انهياراً كبيراً في النظام الصحي.</p>	<p>الهجمات السيبرانية على البنية الصحية الوطنية</p>	
<p>الاستخدام المتزايد للذكاء الاصطناعي في التشخيص والعلاج يجعل هذه الأنظمة هدفاً جديداً للهجمات. إذا تم اختراق أنظمة الذكاء الاصطناعي، فقد يؤدي ذلك إلى أخطاء طبية مما يؤثر على دقة التشخيص والعلاج مما يتسبب في تقديم رعاية صحية غير مناسبة، مما يعرض حياة المرضى للخطر [٢٦].</p>	<p>أمن الذكاء الاصطناعي في الصحة</p>	
<p>يؤدي دمج التقنيات الرقمية في التعليم، إلى أن تصبح هدفاً للهكرز لما تحتويه من بيانات ومحتوى دراسي من الكتب المدرسية والموارد الخاصة.</p>	<p>منصات التعليم الرقمية</p>	<p>التعليم الجيد</p>



## استراتيجية الأمن الوطني العراقي في تعزيز التنمية المستدامة.....

<p>ازداد الاعتماد على التعلم عن بعد خاصة بعد جائحة كورونا، مما يزيد من تعرض الأنظمة التعليمية للهجمات الالكترونية مثل التصيد الاحتيالي (phishing) أو البرمجيات الخبيثة.</p>	<p>التعلم عن بعد</p>	
<p>يعد إجراء الاختبارات والتقييمات الأمانة عبر الأنترنت أمراً صعباً بسبب احتمالية الغش والحاجة إلى مع الوصول غير المصرع به إلى محتوى الاختبار [٢٧].</p>	<p>تقييمات أمانة عبر الأنترنت</p>	
<p>النساء والفتيات يواجهن اشكالا متزايدة من العنف السيبراني مثل الابتزاز والتنمر، والهجمات على الخصوصية عبر محاولات اختراق حساباتهن واستغلال معلوماتهن الشخصية، هذه التهديدات قد تكون أكثر انتشاراً عند النساء الاتي يعملن في المجال العام أو الناشطات في قضايا المساواة، هذا العنف الرقمي يؤدي إلى إسكات النساء وخفض مشاركتهن في الحياة الاجتماعية والسياسية، ومن ثم يعرقل التقدم نحو المساواة بين الجنسين [٢٨].</p>	<p>التنمر والابتزاز الالكتروني</p>	<p>المساواة بين الجنسين</p>
<p>يمكن لشبكات الاتجار بالبشر استخدام التكنولوجيا في استغلال النساء والفتيات، سواء عبر استدراجهن عبر الأنترنت، أو استخدام تقنيات الذكاء الاصطناعي لاستغلال صورهن بشكل غير قانوني، فضلا عن ذلك أدى اقتصاد المنصات المدعوم من الأنترنت إلى زيادة فرص العمل المؤقت عبر الأنترنت، مما يخلق مخاوف بشأن حقوق الإنسان والاستدامة، وخاصة بالنسبة للعاملين المؤقتين الذين يفتقرون إلى الأمن الوظيفي ومزايا العمل.</p>	<p>التوظيف عبر الأنترنت والاتجار بالبشر</p>	

<p>تعتمد البنية التحتية للمياه بشكل متزايد على الأنظمة الرقمية والمتكندلكت الصناعية (SCADA) لإدارة وتنظيم توزيع المياه. هذه الهجمات تؤدي إلى تعطيل امدادات المياه، مما يعرض الصحة العامة والصرف الصحي للخطر، إن التلوث المتعمد لمصادر المياه كجزء من هجوم إرهابي يمكن ان يكون له عواقب طبية وصحية واقتصادية خطيرة.</p>	<p>الهجمات السيبرانية على أنظمة إدارة المياه</p>	<p>المياه النظيفة والنظافة الصحية</p>
<p>تشمل أنظمة إدارة المياه بيانات حساسة مثل جودة المياه، توجيهات التوزيع، ومعلومات المستخدمين، إذ أن تزايد استخدام أجهزة (IOT) في مراقبة توزيع المياه الذي يمثل تحدياً أمنياً. إن ضمان دقة وموثوقية البيانات من أجهزة الاستشعار التي تراقب جودة المياه أمر بالغ الأهمية لاتخاذ القرارات مهمة بشأن معالجة المياه وتوزيعها [٢٩].</p>	<p>حماية البيانات</p>	
<p>العديد من أنظمة المياه في العراق تعتمد على بنية تحتية قديمة لم يتم تصميمها للتعامل مع تهديدات الأمن السيبراني الحديثة.</p>	<p>البنية التحتية القديمة</p>	
<p>إدارة المياه المشتركة بين العراق ودول الجوار، تتطلب تعاوناً دقيقاً لضمان التوزيع العادل للمياه وضمان الجودة والاستدامة، أي هجوم سيبراني يؤدي إلى التلاعب في البيانات حول مستويات المياه، والتدفقات، وجودة المياه قد يسبب عدم الثقة ويؤدي إلى نزاعات حول حقوق المياه، في حالات أكثر خطورة قد تتمكن الهجمات السيبرانية من السيطرة على أنظمة التحكم في السدود أو محطات الضخ المشتركة، أو تعطيل أنظمة المراقبة والاتصالات المدمجة التي تعتمد عليها الدول في</p>	<p>إدارة المياه عبر الحدود</p>	

## استراتيجية الأمن الوطني العراقي في تعزيز التنمية المستدامة.....

إدارة المياه يمكن أن يؤدي إلى عرقلة تدفق المياه ، أو إغراق مناطق معينة مما يؤدي إلى كوارث بيئية وإنسانية [٣٠] .		
أنظمة الطاقة الحديثة تعتمد على شبكات اتصالات معقدة تربط بين محطات الطاقة والمستهلكين. الهجمات السيبرانية على هذه البنية قد تؤدي إلى انقطاع الكهرباء، مما يؤثر على إمدادات الطاقة الحيوية، ومن ثم على توفر الطاقة بأسعار معقولة، وقد استخدمت هذه الهجمات أثناء الحرب الروسية – الأوكرانية [٣١].	هجمات البنية التحتية للطاقة	طاقة نظيفة وأسعار معقولة
أنظمة الطاقة الشمسية والرياح تعتمد على تقنيات متصلة بالشبكة، مثل المزارع الشمسية وطواحين الهواء، والتي يمكن استهدافها من قبل المهاجمين.	أمن منشأة الطاقة المتجددة	
الشبكات الذكية تهدف إلى تحسين كفاءة استهلاك الطاقة وتوزيعها، لكنها تعتمد على أنترنت الأشياء والمستشعرات المتصلة. أي ضعف في هذه الشبكات قد يسمح للمتسللين بالتحكم في توزيع الطاقة أو سرقة البيانات الشخصية.	الثغرات في الشبكات الذكية	
الكثير من عمليات توليد الطاقة من مصادر متجددة تتم عبر أنظمة يتم التحكم فيها عن بعد، إذا تم اختراق هذه الأنظمة، قد يتعرض الاستقرار الكهربائي للخلل أو يتم التعديل على أداء محطات الكهرباء [٣٢].	التحكم عن بعد في الانظمة	
قد يؤدي صعود الأتمتة والتقنيات التي تعتمد على الذكاء الاصطناعي من ارتفاع معدلات البطالة، وانخفاض مهارات العمال، مما يؤثر على عملية النمو الاقتصادي [٣٣].	الأتمتة وتعطيل الوظائف	العمل اللائق ونمو الاقتصاد

## استراتيجية الأمن الوطني العراقي في تعزيز التنمية المستدامة.....

الهجمات التي تستهدف البنوك والمؤسسات المالية وشبكات الدفع الالكترونية قد تعطل الاقتصاد والاستقرار، دمج التكنولوجيا الرقمية في التحول الاقتصادي يطرح أخطاراً وتهديدات جديدة.	الهجمات السيبرانية على القطاعات الاقتصادية الحيوية	
التحول الرقمي المتزايد في إدارة سلاسل التوريد، تصبح الأنظمة الإلكترونية أكثر عرضة للهجمات، مما يؤدي إلى توقف العمليات ويؤخر الإنتاج والشحن، كذلك ان الهجمات تؤدي إلى سرقة البيانات والمعلومات، إذ ان سلاسل التوريد تعتمد على مشاركة البيانات بين الشركات والموردين، مثل خطط الإنتاج، تفاصيل الموردين، أو بيانات العملاء، فضلاً عن الاضرار بسمعة الشركة مما يعرض الشركات للخسائر التنافسية والقانونية [٣٢].	اعتماد سلاسل التوريد الرقمية	
يفتقر العراق إلى التشريعات والأنظمة التي تحمي الاقتصاد من الجرائم الإلكترونية، مما يؤدي إلى انتشار الهجمات السيبرانية التي تؤثر على الشركات الصغيرة والمتوسطة بشكل خاص.	التشريعات والسياسات غير الكافية	
يؤدي دمج التقنيات الرقمية في البنية التحتية الحيوية مثل شبكات الطاقة والمياه والمواصلات تعتمد بشكل متزايد على الأنظمة الرقمية، عدم تأمين هذه البنية بشكل جيد يؤدي إلى تعطل الخدمات الأساسية، ويؤثر على الاقتصادات المحلية ويهدد الأمن العام.	ضعف أمن البنية التحتية	الصناعة والابتكار والهياكل الأساسية
هجمات الاختراق وسرقة البيانات التقنية من قبل القراصنة الذين يستهدفون الشركات والمؤسسات للولوج إلى براءات الاختراع أو تصاميم المنتجات أو خطط التصنيع، هذه المعلومات المسروقة قد تُستغل من قبل	سرقة الملكية الفكرية	

## استراتيجية الأمن الوطني العراقي في تعزيز التنمية المستدامة.....

جهات منافسة في الأسواق العالمية، مما يؤدي إلى تقويض الابتكار ويؤثر على قدرة الشركات على الاستمرار والتطور[٣٤].		
إن الهجمات الإلكترونية التي تستهدف مجموعات المجتمع المدني قد تؤدي إلى تعطيل أنشطتها وسرقة المعلومات الخاصة، الأمر الذي يعوق قدرتها على تقديم الخدمات الاجتماعية، فضلاً عن ذلك أدى ظهور المنصات الإلكترونية إلى زيادة التهديدات الاجتماعية الإلكترونية، بما في ذلك خطاب الكراهية والمعلومات المضللة، والتي قد تؤدي إلى ترسيخ عدم المساواة وتهميش مجتمعات معينة.	التهديدات السيبرانية للشبكات الاجتماعية	الحد من أوجه عدم المساواة
في ظل تزايد الرقمنة، يتم جمع كميات كبيرة من البيانات الشخصية التي قد تستخدم في اتخاذ قرارات تؤدي إلى التمييز، مثل التوظيف أو الحصول على القروض.	استغلال البيانات الشخصية في التمييز	
الفئات الضعيفة، مثل اللاجئين والأقليات، غالباً ما تفتقر للحماية الرقمية الكافية. هذه الفئات تكون أكثر عرضة للتهديدات مثل سرقة الهوية، مما يؤدي إلى استغلالهم وزيادة عزلتهم الاجتماعية[٣٥].	التهديدات الموجهة للفئات الضعيفة	
في المدن الذكية، يعتمد الكثير من البنية التحتية على أجهزة إنترنت الأشياء، مثل أجهزة الاستشعار، وكاميرات المراقبة، ونظم الإضاءة الذكية. قد تحتوي هذه الأجهزة على ثغرات أمنية، مما يجعلها عرضة للاختراق ويتيح للمهاجمين الوصول إلى بيانات حساسة أو تعطيل الخدمات.	نقاط ضعف المدن الذكية	مدن ومجتمعات محلية مستدامة

## استراتيجية الأمن الوطني العراقي في تعزيز التنمية المستدامة.....

تتعتمد المدن الذكية على شبكات اتصال متقدمة لنقل البيانات وتشغيل الأنظمة. أي هجوم سيبراني على هذه الشبكات قد يؤدي إلى تعطيل الخدمات وحدوث الفوضى في المدن الكبرى.	البنية التحتية للاتصالات	
افتقار المناطق الريفية للتمويل والتقنيات، هذا التفاوت يعزز أوجه عدم المساواة ويعوق تحقيق هدف جعل المدن والمجتمعات شاملة وأمنة [٣٦].	التفاوت في القدرات الأمنية بين المناطق الحضرية والريفية	
تعطيل الكفاءة وزيادة استهلاك الموارد.	اختراق أنظمة إدارة الطاقة الذكية	الإنتاج والاستهلاك المستدام
انقطاعات متكررة وزيادة الانبعاثات الكربونية.	الهجمات على شبكات الكهرباء الذكية	
كشف بيانات حساسة تعطل تخطيط وتحسين الاستدامة [٣٧].	سرقة بيانات الأنظمة الموفرة للطاقة	
تقديم بيانات مضللة عن الانبعاثات أو الظواهر المناخية، مما يؤثر على القرارات المناخية.	اختراق أنظمة التغير المناخي	العمل المناخي
تعطيل إنتاج الطاقة النظيفة وزيادة الاعتماد على الوقود الاحفوري.	الهجمات على البنية التحتية للطاقة المتجددة	
تقليل فعالية إجراءات الحد من انبعاثات الكربون أو التسبب في زيادة غير مبررة.	اختراق الأنظمة الذكية للتحكم في الانبعاثات	
إعاقة الاستجابة للأزمات المناخية، مما يزيد من الأضرار البشرية والبيئية.	تعطيل أنظمة الاستجابة للكوارث الطبيعية	
تأخير مبادرات العمل المناخي بسبب تعطيل الأنظمة الرقمية أو المطالبة بفدية مالية.	هجمات الفدية على مشاريع المناخ	
تسهيل الاتجار غير المشروع بالموارد الطبيعية وزيادة الممارسات التي تضر بالمناخ [٣٨].	الجرائم البيئية الإلكترونية	

## استراتيجية الأمن الوطني العراقي في تعزيز التنمية المستدامة.....

اختراق أنظمة مراقبة المحيطات والبحار	تضليل البيانات حول صحة النظم البحرية وتلوث المياه، مما يعوق اتخاذ القرارات المبنية على أسس علمية.	الحياة تحت الماء
الهجمات على الأنظمة الرقمية لإدارة مصائد الأسماك	تعطيل جهود الحفاظ على الثروة السمكية وزيادة الصيد غير المشروع.	
اختراق أنظمة الإنذار المبكر للتلوث البحري	تأخير الاستجابة لتسربات النفط أو الكوارث البيئية البحرية، مما يؤدي إلى تفاقم الأضرار.	
الهجمات على شبكات السفن الذكية	إعاقة عمليات الملاحة أو التسبب في حوادث بحرية، مما يؤدي إلى ارتفاع معدلات التلوث البحري والمخاطر البيئية.	
القرصنة البيئية الإلكترونية	تسهيل التجارة غير المشروعة للكانات البحرية المهددة بالانقراض أو الموارد البحرية المحمية [٣٩].	
اختراق أنظمة مراقبة التنوع البيولوجي	تعطيل جمع البيانات الحيوية عن الأنواع المهددة بالانقراض أو تدهور الأنظمة البيئية البرية	الحياة في البر
الهجمات على الأنظمة الرقمية لإدارة الغابات	تقليل فعالية مراقبة وإدارة الغابات، مما يسهم في زيادة التصحر وفقدان التنوع البيولوجي.	
اختراق أنظمة الإنذار المبكر للكوارث الطبيعية	تأخير الاستجابة لحالات التصحر أو حرائق الغابات أو الفيضانات، مما يزيد من التدهور البيئي [٤٠].	
الهجمات السيبرانية على المؤسسات الحكومية	مثل التسلل الإلكتروني أو هجمات DDOS التي قد تؤدي إلى تعطيل عمل المؤسسات الحكومية الأساس، مما يعرقل تقديم الخدمات العامة.	السلام والعدل والمؤسسات القوية
التلاعب بالانتخابات الرقمية	الهجمات على الأنظمة الانتخابية عبر الإنترنت أو التشويش على العملية الانتخابية قد يهدد النزاهة الديمقراطية ويقلل من ثقة المواطنين في المؤسسات السياسية [٤١].	

## استراتيجية الأمن الوطني العراقي في تعزيز التنمية المستدامة.....

الهجمات السيبرانية لنشر الأخبار المزيفة يمكن ان تخلق الفوضى وتثير الاضطرابات الاجتماعية، يضر بالعدالة والسلام في المجتمعات.	انتشار المعلومات المضللة والأخبار الكاذبة	
ضعف تشريعات الأمن السيبراني أو غيابها في العراق قد يؤدي إلى اضعاف المؤسسات العامة والأمن القانوني، ويعزز المخاطر المرتبطة بالجرائم السيبرانية.	عدم فاعلية قوانين الأمن السيبراني	
الهجمات الموجهة ضد المؤسسات القضائية أو الحقوقية قد تقوض سيادة القانون وتضعف قدرة هذه المؤسسات على تطبيق العدالة وحماية الحقوق [٤٢].	تهديدات الهجمات الموجهة	
الهجمات التي تستهدف المعلومات الاستراتيجية للعراق قد تهدد الاستقرار السياسي والاقتصادي وتعوق جهود التنمية المستدامة.	القرصنة السياسية والاقتصادية	
الهجمات على الأنظمة المصرفية والبنية التحتية المالية في العراق قد تعطل تدفق التمويل من الجهات الدولية، مما يؤثر على قدرة على تحقيق هذا الهدف.	تهديدات ضد الأنظمة المالية والمصرفية	الشركات من أجل أهداف
الهجمات التي تستهدف المنظمات غير الحكومية التي تعمل في مجالات التنمية والإنسانية قد يعرقل المشاريع بين العراق والدول والمنظمات الدولية	استهداف المنظمات غير الحكومية	
استهداف التجارة الالكترونية في العراق يؤدي إلى الاضرار بالتعاون التجاري مع الدول الأخرى ويؤثر على المشاريع الاقتصادية الموجهة نحو تحقيق التنمية المستدامة [٤٣].	الهجمات على التجارة الإلكترونية العراقية	



## استراتيجية الأمن الوطني العراقي في تعزيز التنمية المستدامة.....

المحور الثالث: دور استراتيجية الأمن السيبراني في تحقيق أهداف التنمية المستدامة في العراق.

على الرغم من الجهود المبذولة في بناء الأمن الوطني العراقي سيبرانياً، إلا أنه يواجه تحديات غير مرئية وهي (التهديدات السيبرانية) في مجالاته المختلفة، فهو ما يزال يعاني من عدم الاستقرار العام، ولا يملك القدرات المطلوبة للتكيف مع تلك التحديات التي يفرضها الفضاء السيبراني. فالتطور التكنولوجي الذي شهده العراق في مجال المعلومات بعد العام ٢٠٠٣ تزامن معه ضعف الأمانة الالكترونية، وهشاشة البنية التحتية أدى إلى أن يصبح العراق منكشفاً استراتيجياً للعديد من الدول، يسهل اختراقه والتجسس على المعلومات المؤسسية. ومن الملاحظ أن أكثر المؤسسات العراقية تتعاقد لتجهيز معلوماتها من أقمار اصطناعية ذات مورد خارجي واقع خارج الحدود العراقية الذي يؤدي إلى مرور تلك المعلومات في خوادم تلك الدول ورجوعها إلى العراق [٤٤]. إذ نجد موقع العراق وفقاً لمؤشر الأمن السيبراني العالمي للعام ٢٠٢٤ ضمن الطبقة الرابعة من أصل الطبقات الخمس في الالتزام بالأمن السيبراني، وحصل على درجة (53.7) وكذلك موضح في الجدول رقم (٢) [٤٥].

### الجدول (٢):

#### موقع العراق في مؤشر الأمن السيبراني

النتيجة الكلية	إجراءات التعاون	بناء القدرات	الإجراءات التنظيمية	الإجراءات التقنية	الإجراءات القانونية
53.7	8.11	8.38	15.77	9.6	11.21

المعضلة السيبرانية التي يعاني منها العراق يمثل عقبة أمام تحقيق أهداف التنمية المستدامة، وهي بحاجة إلى إمكانيات ووسائل احترازية (وقائية واستباقية) عبر وضع استراتيجية للأمن الوطني السيبراني، والتي يقصد بها "كافة التدابير المتعلقة بسرية المعلومات والبيانات التي يتم معالجتها وتخزينها وإبلاغها عن طريق وسائل إلكترونية أو مشابهها، وحمايتها والنظم المرتبطة بها من التهديدات الخارجية أو الداخلية".

## استراتيجية الأمن الوطني العراقي في تعزيز التنمية المستدامة.....

ويظهر دور الأمن السيبراني في تحقيق أهداف التنمية المستدامة عبر النقاط الآتية [٤٦]، [٤٧]:

١. القضاء على الفقر: يسهم الأمن السيبراني في القضاء على الفقر عبر حماية أمن وسلامة الخدمات المالية الرقمية، والتي يمكن أن تساعد في الحد من الفقر بواسطة منح الأفراد إمكانية الوصول إلى الخدمات المالية، وحماية أمن وسلامة منصات التجارة الالكترونية، والتي يمكن أن تسهم في زيادة النمو الاقتصادي والحد من الفقر عبر تسهيل على الأفراد شراء وبيع السلع والخدمات عبر الأنترنت، وحماية أمن وسلامة الموارد التعليمية الرقمية، والتي يمكن أن تسهم في تحسين التعليم.
٢. القضاء على الجوع: يُمكن للزراعة الاستفادة من التقنيات الرقمية لزيادة الإنتاجية والكفاءة والاستدامة، إذ يمكن للأمن السيبراني في منع استخدام التقنيات الرقمية لتعطيل أو تدمير الأنظمة الزراعية، عبر حماية الأمن الغذائي، وتشجيع استخدام التكنولوجيا الرقمية في الزراعة، وتمكين صغار المزارعين وتعزيز الثقة في الزراعة الرقمية.
٣. الصحة الجيدة والرفاهية: يسهم الأمن السيبراني في تحسين ورفاهية الصحة في العراق عبر حماية البيانات الصحية من الوصول غير المصرح أو الكشف عنها أو تعطيلها، أو تعديلها أو تدميرها، وضمان توفر البنية التحتية الصحية الحيوية، وتشجيع استخدام التطبيب عن بعد لتقديم الرعاية الطبية عن بعد، ودعم البحث والتطوير لتقنيات الرعاية الصحية الجديدة التي قد تؤدي إلى تطوير علاجات جديدة وعلاجات للأمراض.
٤. التعليم الجيد: يُسهم الأمن السيبراني في تحقيق هذا الهدف عبر توفير حماية للبنية التحتية الرقمية للمؤسسات التعليمية العراقية، ويمنع التهديدات التي تعطل التعلم الالكتروني، أو سرقة بيانات الطلبة، وتشجيع الاستخدام المسؤول والأمن للتكنولوجيا دون المساس بأمنهم.

## استراتيجية الأمن الوطني العراقي في تعزيز التنمية المستدامة.....

٥. المساواة بين الجنسين: يعزز الأمن السيبراني الحماية الإلكترونية للنساء والفتيات العراقيات من التنمر الإلكتروني، والهجمات السيبرانية المستهدفة، وتعزيز استخدامهن المجال التقني للحصول على حقوقهن، والحصول على الوظائف وفرص العمل، والمشاركة في صنع القرار التقني.
٦. المياه النظيفة والنظافة الصحية: يُسهم الأمن السيبراني في حماية البنية التحتية للمياه والصرف الصحي من الهجمات السيبرانية، بما يضمن توفير المياه النظيفة ومعالجة الصرف الصحي بأمان. كذلك يحمي البيانات المتعلقة بجودة المياه ويدعم التخطيط للطوارئ والتعاون الدولي، مما يعزز الاستدامة ويحد من التكاليف التشغيلية.
٧. طاقة نظيفة وأسعار معقولة: يسهم الأمن السيبراني في تحقيق الهدف السابع من أهداف التنمية المستدامة، المتعلق بالطاقة النظيفة، عبر حماية البنية التحتية المتجددة من الهجمات السيبرانية، مما يضمن استقرار التوزيع وكفاءة الإنتاج. كذلك يدعم الأمن السيبراني حماية بيانات أنظمة الطاقة الذكية وانترنت الأشياء، مما يعزز دقة المراقبة والتحكم. هذا يُسهم في استدامة الطاقة وتقليل التكاليف والمخاطر.
٨. العمل اللائق ونمو الاقتصاد: يعزز الأمن السيبراني في تحقيق الهدف المتعلق بالعمل اللائق عبر حماية الشركات والمؤسسات من الهجمات السيبرانية التي تهدد استمرارية الأعمال وتؤدي إلى خسائر اقتصادية. كذلك يعزز ثقة المستثمرين والعملاء عبر تأمين البيانات والخصوصية، ويدعم توظيف الكوادر المؤهلة في مجال الأمن السيبراني، مما يخلق فرص عمل جديدة ويُسهم في نمو الاقتصاد الرقمي.
٩. الصناعة والابتكار والهياكل الأساسية: يدعم الأمن السيبراني تحقيق الهدف المتعلق بالصناعة والابتكار والبنية التحتية، عبر حماية الأنظمة الصناعية والتكنولوجية من الهجمات السيبرانية، مما يضمن استمرارية الإنتاج واستقرار سلاسل الإمداد. كذلك يعزز الأمن السيبراني الثقة في البنية التحتية الرقمية، مما يشجع على تبني تقنيات

## استراتيجية الأمن الوطني العراقي في تعزيز التنمية المستدامة.....

مبتكرة وإنترنت الأشياء في الصناعة. كذلك، يسهم في توفير بيئة آمنة للابتكار الرقمي، مما يعزز في تطوير صناعات جديدة وتحفيز النمو الاقتصادي.

١٠. الحد من أوجه عدم المساواة: يدعم الأمن السيبراني تحقيق الهدف المتعلق بتقليل أوجه عدم المساواة، عبر توفير بيئة رقمية آمنة تحمي جميع الأفراد، بما في ذلك الفئات المهمشة، من التمييز والهجمات الإلكترونية. يسهم الأمن السيبراني في ضمان فرص متساوية للوصول إلى الخدمات والموارد الرقمية بأمان، مما يقلل من الفجوة الرقمية. كذلك يعزز التوزيع العادل للمعلومات والفرص الرقمية، وبذلك يعزز الشمولية الاجتماعية والاقتصادية.

١١. مدن ومجتمعات محلية مستدامة: للأمن السيبراني الدور في تحقيق الهدف المتعلق بالمدن والمجتمعات المستدامة، عبر حماية البنية التحتية الذكية للمدن من الهجمات السيبراني التي قد تؤثر على الخدمات الأساسية مثل النقل، والطاقة، والمياه. كذلك يضمن الأمان الرقمي لبيانات السكان والمجتمعات، مما يعزز من ثقة المواطنين في استخدام تقنيات المدن الذكية، فضلاً عن ذلك، يُسهم في تأمين أنظمة الرصد والتحليل التي تعزز التخطيط الحضري والاستدامة البيئية.

١٢. الإنتاج والاستهلاك المستدام: يعزز الأمن السيبراني في تحقيق هدف الاستهلاك والإنتاج المسؤولين، عبر حماية الأنظمة الرقمية التي تدير عمليات الإنتاج المستدام وإدارة الموارد. كذلك يساعد في تأمين البيانات المتعلقة بتتبع استهلاك الموارد وإنتاج السلع بشكل آمن، والحد من توليد النفايات وتحفيز النمو الاقتصادي طويل الأجل.

١٣. العمل المناخي: يحقق الأمن السيبراني هذا الهدف عبر تعزيز البنية التحتية الرقمية ضد الهجمات السيبرانية التي قد تؤثر على نظم الطاقة والمناخ. فضلاً عن تعزيز استدامة الحلول التكنولوجية الموجهة لتقليل الانبعاثات، مما يؤدي إلى مجتمع عراقي أكثر مرونة واستدامة، وقادر على الاستجابة للمشاكل التي يفرضها التغير المناخي.

## استراتيجية الأمن الوطني العراقي في تعزيز التنمية المستدامة.....

١٤. الحياة تحت الماء: يحقق الأمن السيبراني هذا الهدف عبر حماية البيانات البيئية، وأنظمة مراقبة المحيطات من التلاعب والهجمات، مما يدعم دقة الأبحاث والحفاظ على النظم البيئية. كذلك يحيي الأنظمة الرقمية المستخدمة في الرقابة على الصيد والتقنيات البحرية الذكية، مما يدعم استدامة الموارد البحرية.

١٥. الحياة في البر: يتحقق هذا الهدف عبر حماية النظم البيئية البرية، وضمان التشغيل الآمن لجهود الحفاظ على البيئة المعتمدة على التكنولوجيا، وتسهيل التعاون الدولي، وتحسين المبادرات الرامية إلى حماية النظم البيئية الأرضية والتنوع البيولوجي.

١٦. السلام والعدل والمؤسسات القوية: تساعد تدابير الأمن السيبراني على حماية البنية التحتية الرقمية للعدالة والقضاء من الهجمات السيبرانية، مما يضمن نزاهة وشفافية البيانات القضائية. كذلك يعزز الثقة في مؤسسات الدولة عبر حماية أنظمة الخدمات العامة، ويدعم مكافحة الفساد عبر حماية المعلومات الحساسة من الهجمات، ويخلق بيئة دولية أكثر استقراراً عبر منع الهجمات السيبرانية بين الدول.

١٧. الشراكات من أجل الأهداف: أن وجود أمن سيبراني متين يعزز التعاون الدولي، عبر تأمين تبادل البيانات والمعلومات الحساسة بين الدول والمنظمات، وخلق بيئة رقمية آمنة لتحقيق الشراكات العالمية.

### الخاتمة والتوصيات:

تختتم الدراسة، وعن طريق ما ذكر من طرح في محاورها الرئيسة، ومحاولتها لتغطية الموضوع بشكل تام، فقد تم إثبات الفرضية التي انطلق منها البحث كأساس منهجي عام سار عليه، وبناء على ذلك فقد تم التوصل إلى إن العراق يعاني من عدة تحديات تحول دون تحقيق منظومة أمن سيبراني فعّالة تدعم أهداف التنمية المستدامة. مما يبرز الحاجة إلى استراتيجيات وطنية شاملة ومتعددة القطاعات لتعزيز الأمن السيبراني وحماية المكتسبات التنموية في العراق. وتشمل هذه التحديات:

## استراتيجية الأمن الوطني العراقي في تعزيز التنمية المستدامة.....

١. ضعف البنية التحتية التكنولوجية: تفتقر الكثير من المناطق العراقية إلى بنية تحتية رقمية متطورة، مما يجعلها عرضة للهجمات الإلكترونية، ومن ثم تعطيل الخدمات الإلكترونية مثل التعليم الرقمي، والخدمات الصحية الإلكترونية.
٢. نقص التشريعات والقوانين المتخصصة: عدم وجود قوانين شاملة لحماية البيانات وتنظيم الأمن السيبراني، وهذا الغياب القانوني يشجع الجرائم الإلكترونية، مما يعف ثقة المواطنين في الخدمات الرقمية.
٣. تصاعد الهجمات الإلكترونية: العراق هدف مستمر للهجمات الإلكترونية سواء من جماعات إرهابية أم جهات دولية، هذه الهجمات تؤثر على الأمن القومي والاقتصاد.
٤. نقص الامكانيات المالية والبشرية: نقص الكفاءات المتخصصة في الأمن السيبراني، مما يستدعي استثمارات كبيرة في التعليم والتدريب لتعزيز القدرات المحلية. فضلاً عن ذلك، يفتقر العراق إلى التمويل الكافي لتطوير بنية تحتية رقمية متينة وصيانة الأنظمة بشكل مستدام.
٥. ضعف التعاون الدولي: يعاني العراق من ضعف التعاون مع الدول الأخرى لمواجهة التهديدات السيبرانية، مما يقلل من فرص تبادل المعرفة وأفضل الممارسات، ومن ثم تعطل جهود بناء أنظمة أمنة.

### التوصيات:

١. تعزيز الأطر التشريعية والمؤسسية: العمل على تطوير قوانين ولوائح وطنية تُعنى بالأمن السيبراني، مع مراعاة التوافق مع المعايير الدولية، وإنشاء هيئة مختصة بالأشراف على الأمن السيبراني، وتقديم دولة (سلطنة عُمان) تجربة متميزة بهذا الصدد، عبر تشريع قانون المعاملات الإلكترونية عام ٢٠٠٨، وقانون الجرائم الإلكترونية عام ٢٠١١، فضلاً عن قانون تنظيم الخدمات البريدية عام ٢٠١٢. أما على مستوى الأطر المؤسسية تأسيس المركز الوطني للسلامة المعلوماتية، والمختبر الوطني للأدلة الرقمية للتعامل مع الجرائم

## استراتيجية الأمن الوطني العراقي في تعزيز التنمية المستدامة.....

الإلكترونية وتقديمها للعدالة وتطبيق القانون، إذ تمكن المركز من التعامل مع (١١٤٣٥٥٩٦) محاولة اختراق مشبوه، و٦٤ برنامج تجسس[٤٨].

٢. ربط استراتيجية الأمن السيبراني بأهداف التنمية المستدامة: الاستثمار في التكنولوجيا لتعزيز البنية التحتية الحيوية مثل (الصحة، التعليم، والطاقة) مع ضمان حمايتها من المخاطر السيبرانية، ودعم الابتكارات الرقمية التي تخدم أهداف التنمية المستدامة، مثل حلول التعليم الإلكتروني والحكومة الرقمية، وتقديم دولة (المملكة العربية السعودية) تجربة لها خصوصياتها ذات الأبعاد الوطنية والإقليمية، وكذلك العالمية المرتبطة بعضويتها في مجموعة العشرين (G20)، إذ تم صياغة استراتيجية الأمن السيبراني السعودي وربطها بالرؤية الاستراتيجية للمملكة ٢٠٣٠ لدعم الوطن، والاقتصاد الرقمي، والتمكين الرقمي للمواطنين [٤٩].

٣. تنمية رأس المال البشري: دعم الأنشطة البحثية التكنولوجية والكوادر البشرية في مجال الأمن السيبراني لسد الفجوة في الكوادر المؤهلة، عبر إنشاء مراكز بحثية لتنمية الكوادر الاحترافية، وتخصيص موارد لدعم الأبحاث، وتحفيز الجامعات لتطوير تقنيات محلية تلبي حاجات العراق، وإدراج الأمن السيبراني ضمن المناهج الدراسية في المدارس لتعزيز الوعي الرقمي.

٤. الدبلوماسية السيبرانية، وتعزيز التعاون والشراكات الإقليمية والعالمية للتعاون مع المخاطر السيبرانية: تعزيز وبناء تحالفات ومبادرات إقليمية وعالمية، وبما يخدم أمن البنى التحتية واستمرارية عمل هذه القطاعات، ويمكن للعراق الاستفادة من تجربة الولايات المتحدة في هذا المجال، إذ ركزت استراتيجية الأمن السيبراني على أهمية بناء نظام رقمي بيئي مفتوح وشامل (عبر رفع مستويات التنسيق الدولي في تطوير التكتيكات المشتركة)، وفي هذا الإطار أقر قانون (الدبلوماسية السيبرانية لعام ٢٠٢١ Cyber

(Diplomacy Act of 2021) والذي ينص على تأسيس مكتب خاص للسياسة الدولية في مجال الأمن السيبراني داخل وزارة الخارجية السيبرانية [٥٠].

## References:

- [1] D. Schatz, R. Bashroush, and J. Wall, 'Towards a More Representative Definition of Cyber Security', *The Journal of Digital Forensics, Security and Law*, vol. 12, no. 2, pp. 53–54, 2017, doi: 10.15394/jdfsl.2017.1476.
- [2] 'National Cybersecurity Awareness Month | whitehouse.gov'. Accessed: Nov. 14, 2024. [Online]. Available: <https://obamawhitehouse.archives.gov/blog/2009/10/01/national-cybersecurity-awareness-month>
- [3] Z. M. salah mahdi, 'Cybersecurity as a new pillar in the Iraqi strategy', *Political Issues*, vol. 62, no. 12, p. 277, 2020.
- [4] Institute of National planning, *The developmental and strategic dimensions of cyber security and its role in supporting digital and crypto economies - Egyptian Experience Paths in the Light Global Experiences*. cario: Institute of National planning, 2021.
- [5] 'What is Cyber Security? Definition & Best Practices'. Accessed: Nov. 15, 2024. [Online]. Available: <https://www.itgovernance.co.uk/what-is-cybersecurity>
- [6] 'Understanding Denial-of-Service Attacks | CISA'. Accessed: Nov. 15, 2024. [Online]. Available: <https://www.cisa.gov/news-events/news/understanding-denial-service-attacks>
- [7] Joseph S. Nye Jr, *Soft Power the means to success in world politics*. Riyadh: obekan, 2007.
- [8] J. S. Nye, 'Cyber Power', Cambridge, May 2010. [Online]. Available: <http://belfercenter.org>



- [9] Raad Khudair Salibi, 'Strengthening Cybersecurity in Iraq: Challenges and Opportunities', *Journal of International studies*, vol. 99, no. 99, p. 511, Oct. 2024.
- [10] E. Khalifa, 'Deterrence mechanisms in cyberspace', Cario, Jan. 2023. [Online]. Available: <https://www.researchgate.net/publication/366965740>
- [11] A. M. Colarik, *Cyber Terrorism: Political and Economic Implications*. London: IDEA Group Publishing, 2006. [Online]. Available: <http://www.eurospanonline.com>
- [12] A. Mustafa Ibrahim Salman, 'Cyber Security and its Impact on the Iraqi National Security', *Journal of Juridical and Political Science*, vol. 10, no. 1, pp. 174–175, 2021.
- [13] Dhiyab Musa al-Badayinah, 'Cybercrimes: Concept and Causes', Amman, 2014.
- [14] W. Commission on Environment, 'Report of the World Commission on Environment and Development: Our Common Future Towards Sustainable Development 2. Part II. Common Challenges Population and Human Resources 4', Oslo, Mar. 1987. Accessed: Nov. 16, 2024. [Online]. Available: <https://sustainabledevelopment.un.org/content/documents/5987our-common-future.pdf>
- [15] B. Abdul Rahman, 'The role of renewable energy in achieving sustainable development', *Journal of sustainable studies*, vol. 6, no. 3, Aug. 2024.

- [16] 'Argentina Economy: Milei Decides against Dollarization | National Review'. Accessed: Mar. 18, 2024. [Online]. Available: <https://www.nationalreview.com/2024/03/hankes-2023-misery-index/>
- [17] M. Madden, M. Gilman, K. Levy, and A. Marwick, 'Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans Americans Recommended Citation Recommended Citation', *Washington University Law Review*, vol. 95, no. 1, pp. 53–125, 2017, [Online]. Available: [https://openscholarship.wustl.edu/law\\_lawreviewhttps://openscholarship.wustl.edu/law\\_lawreview/vol95/iss1/6](https://openscholarship.wustl.edu/law_lawreviewhttps://openscholarship.wustl.edu/law_lawreview/vol95/iss1/6)
- [18] S. Masiero and A. Prakash, 'The Politics of Anti-Poverty Artefacts: Lessons from the Computerization of the Food Security System in Karnataka', in *ACM International Conference Proceeding Series*, Association for Computing Machinery, May 2015. doi: 10.1145/2737856.2738011.
- [19] O. Demidov and G. P. Paoli, 'Supply Chain Security in the Internet Age', 2022.
- [20] N. O'Brien, J. Martin, and A. Jaras, 'Protecting healthcare systems', London, 2020.
- [21] 'SingHealth cyber attack: How it unfolded | The Straits Times'. Accessed: Nov. 19, 2024. [Online]. Available: <https://graphics.straitstimes.com/STI/STIMEDIA/Interactives/2018/07/sing-cyber-breach/index.html>
- [22] 'A Look at 2024's Health Care Cybersecurity Challenges | AHA News'. Accessed: Nov. 19, 2024. [Online]. Available:

<https://www.aha.org/news/aha-cyber-intel/2024-10-07-look-2024s-health-care-cybersecurity-challenges>

- [23] L. S. van Boven *et al.*, 'Hacking Acute Care: A Qualitative Study on the Healthcare Impacts of Ransomware Attacks Against Hospitals', Feb. 21, 2023. doi: 10.1101/2023.02.13.23285854.
- [24] I. Singh and Y. Singh, 'CYBER-SECURITY KNOWLEDGE AND PRACTICE OF NURSES IN PRIVATE HOSPITALS IN NORTHERN DURBAN, KWAZULU-NATAL', *J Theor Appl Inf Technol*, vol. 15, no. 1, pp. 246–267, 2022, [Online]. Available: [www.jatit.org](http://www.jatit.org)
- [25] A. Fakher and M. Alalwai, 'Iraqi cyber security : Reality and future prospects', *The International and political Journal*, no. 58, pp. 287–308, Mar. 2024.
- [26] L. Shawwa, 'The Use of Telemedicine in Medical Education and Patient Care', *Cureus*, vol. 15, no. 4, Apr. 2023, doi: 10.7759/cureus.37766.
- [27] S. Ghanem, 'E-learning in Higher Education to Achieve SDG 4: Benefits and Challenges', *2020 2nd International Sustainability and Resilience Conference: Technology and Innovation in Building Designs*, Nov. 2020, doi: 10.1109/IEEECONF51154.2020.9319981.
- [28] M. Zaenul Muttaqin and N. T. Ambarwati, 'Cyberbullying and Woman Oppression', *Education and Humanities Research*, vol. 510, pp. 545–553, 2020.
- [29] J. McCarthy, B. Stea, and D. Faatz, 'CYBERSECURITY FOR THE WATER AND WASTEWATER SECTOR A Practical Reference Design for Mitigating Cyber Risk in Water and Wastewater Systems', 2023. [Online]. Available: <https://www.nccoe.nist.gov/>.

- [30] 'Water challenges and conflict dynamics in Southern Iraq An in-depth analysis of an under-researched crisis', Feb. 2022.
- [31] D. P. Saraswati, N. Nidatya, M. Kamil, and G. Abdurrahman, 'Securitisation of Ukrainian Critical Infrastructures: The Case of the Failure of SCADA System in Protecting the Power Grids', *Jurnal Ilmu Hubungan Internasional*, vol. 5, no. 2, pp. 152–172, Dec. 2022.
- [32] A. Al-Basousi, 'International Efforts to Combat Cyber Attacks on the Energy Sector: Selected Cases', *The Journal of the Faculty of Economics and Political Science*, vol. 24, no. 4, pp. 150–178, Oct. 2023.
- [33] S. Ray, S. Chatterjee, J. A. Grace, M. Sunil Kumar, and G. Ahluwalia, 'A Systematic Review of Artificial Intelligence (AI) And Impact on Human Resource Management (HRM): Challenges, Risks and Opportunities', *NATURALISTA CAMPANO*, vol. 28, no. 1, pp. 558–591, 2024, [Online]. Available: <https://museonaturalistico.it>
- [34] D. Halbert, 'Intellectual property theft and national security: Agendas and assumptions', *The Information Society*, vol. 32, no. 4, pp. 256–268, Aug. 2016, doi: 10.1080/01972243.2016.1177762.
- [35] D. R. A. Schallmo and J. Tidd, *Digitalization Approaches, Case Studies, and Tools for Strategy, Transformation and Implementation Management for Professionals*. Grewerbestrasse, 2021. [Online]. Available: <http://www.springer.com/series/10101>
- [36] E. E. D. M. K. Abdul Hamid, 'Cyber-Attacks on Smart City: Infrastructure, Legal Challenges and Confrontation Strategy', *Dirasat: Shari'a and Law Sciences*, vol. 50, no. 3, pp. 54–70, Sep. 2023, doi: 10.35516/law.v50i3.2864.

- [37] M. Al Hadi, 'Towards a sustainable digital society', *ESISACT*, no. 29, Sep. 2022.
- [38] G. R. Abhijith, E. Salomons, and A. Ostfeld, 'Enhancing the Reliability of a Contamination Detection Sensors' Network in Water Distribution Systems during a Cyber-Attack', *World Environmental and Water Resources Congress 2023: Adaptive Planning and Design in an Age of Risk and Uncertainty - Selected Papers from World Environmental and Water Resources Congress 2023*, pp. 1–12, 2023, doi: 10.1061/9780784484852.001.
- [39] Nitin. Goyal, Luxmi. Sapra, and J. Kaur. Sandhu, *Energy-efficient underwater wireless communications and networking*. Hershey: Engineering Science Reference, an imprint of IGI Global, 2021.
- [40] T. C. Haas, 'Adapting cybersecurity practice to reduce wildlife cybercrime', *J Cybersecr*, vol. 9, no. 1, 2023, doi: 10.1093/cybsec/tyad004.
- [41] 'الأمن السيبراني وتحدياته على انتخابات عام (٢٠٢١) في العراق – كتابات'. Accessed: Nov. 19, 2024. [Online]. Available: <https://kitabab.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/>
- [42] M. Salim, 'Previewing Iraqi cybersecurity and its impact on state power', *Journal of Educational and Human Science*, vol. 18, pp. 70–84, Sep. 2022.

- [43] N. Ali Saki, 'Iraqi national security in light of cyber-infiltration (Information security)', *the college of law and political science journal*, vol. 8–20, no. 11, pp. 13–39, 2021.
- [44] H. Mousa, 'Strategic Vision for Iraqi National Security in Cyberspace ((Approach between the security dilemma and performance machinery))', *Journal of Algerian Legal and Political Sciences*, vol. 57, no. 5, pp. 548–564, Dec. 2020.
- [45] D. Sector, 'Global Cybersecurity Index 2024', 2024.
- [46] J. Fulwood and et al, 'CYBERSECURITY AND SUSTAINABLE DEVELOPMENT An Intersectional Analysis', 2022.
- [47] J. O. Odumesi and B. S. Sanusi, 'Achieving Sustainable Development Goals from a Cybersecurity Perspective', in *Cyber Security Experts of Nigeria*, Nigeria: Nigerian Army ResourceCentre, Jul. 2023, pp. 1–10. doi: 10.22624/aims/csean-smart2023p3.
- [48] Ministry of Technology and Communications, 'Annual Report', Sultanate of Oman, 2019.
- [49] 'https://nca.gov.sa/national\_cybersecurity\_strategy-ar.pdf', National Cybersecurity Authority.
- [50] M. T. [R-T.-10] Rep. McCaul, 'H.R.1251 - 117th Congress (2021-2022): Cyber Diplomacy Act of 2021', 2021, Accessed: Nov. 20, 2024. [Online]. Available: <https://www.congress.gov/bill/117th-congress/house-bill/1251>