السنة الثالثة والعشرون ملحق 1 العدد 85 / شهر حزيران / السنة
https://doi.org/10.31272/ijes.v23 i85.1263

المجلة العراقية للعلوم الاقتصادية
Iraqi Journal For
Economic Sciences

PISSN : 1812-8742 EISSE ONLIN : 2791-092X Arcif : 0.375

Enhancing Cybersecurity Strategies in Iraq and Arab Countries and Aligning them with Sustainable Development Goals: Ensuring a Safe and Sustainable Future

تعزيز استراتيجيات الأمن السيبراني في العراق والدول العربية وموائمتها مع أهداف التنمية المستدامة: ضمان لمستقبل آمن ومستدام

د. ثابت سلطان محمد
Thabit Sultan Mohammed
thabit.sultan@alqalam.edu.iq
قسم هندسة تقنيات الحاسوب كلية القلم الجامعة كركوك

Abstract

The research aims to explore the relationship between cybersecurity and sustainable development goals, focusing on how cybersecurity strategies can be enhanced to support the achievement of these goals and ensure a safe and sustainable future. Cybersecurity refers to the protection of systems, networks, and data from cyberattacks and unauthorized access. With the increasing reliance on digital technology, cybersecurity has become a strategic issue affecting economic, social, and environmental development. Cybersecurity plays a vital role in achieving many sustainable development goals, such as protecting critical infrastructure, ensuring privacy, supporting economic growth, and promoting environmental sustainability. There is significant overlap between cybersecurity and goals such as good health, quality education, decent work, and sustainable cities.Cybersecurity strategies in Iraq and some Arab countries have been analyzed, focusing on the challenges and available opportunities, and highlighting the importance of enhancing international cooperation and knowledge exchange to improve cybersecurity and overcome challenges and obstacles. The challenges include a lack of resources, weak societal awareness, and insufficient legislation. There is a need to develop integrated policies that address cyber threats while considering environmental and social dimensions. Cybersecurity supports economic growth by protecting digital infrastructure and intellectual property rights, promoting sustainable innovation by providing a safe environment for research and development, and protecting smart systems that support resource management and urban services. It also contributes to enhancing the digital resilience

of cities, supporting the achievement of Goal 11 of the Sustainable Development Goals.Cybersecurity is not just a technical issue; it is an essential element for achieving sustainable development. Based on this fact, there is an urgent need to enhance cybersecurity strategies and align them with sustainable development goals to ensure a secure and sustainable future. This includes activating international cooperation, exchanging expertise, and securing it at the global level. Additionally, it involves developing national cybersecurity strategies that align with sustainable development goals, raising societal awareness of the importance of cybersecurity and its role in achieving sustainability, and encouraging investment in scientific research to develop sustainable security technologies.

Keywords: Cybersecurity; Cybersecurity Strategies; Sustainable Development Goals (SDGs).

المستلخص

يهدف البحث إلى استكشاف العلاقة بين الأمن السيبراني وأهداف التنمية المستدامة، مع التركيز على كيفية تعزيز استراتيجيات الأمن السيبراني لدعم تحقيق هذه الأهداف، وضمان مستقبل آمن ومستدام. يشير الأمن السيبراني إلى حماية الأنظمة والشبكات والبيانات من الهجمات الإلكترونية والوصول غير المصرح به. ومع تزايد الاعتماد على التكنولوجيا الرقمية، أصبح الأمن السيبراني قضية استراتيجية تؤثر على التنمية الاقتصادية والاجتماعية والبيئية. ويلعب الأمن السيبراني دورًا حيويًا في تحقيق العديد من أهداف التنمية المستدامة، مثل حماية البنية التحتية الحيوية، وضمان الخصوصية، ودعم النمو الاقتصادي، وتعزيز الاستدامة البيئية. وهناك تداخل كبير بين مفهوم الأمن السيبراني وأهداف مثل الصحة الجيدة، والتعليم الجيد، والعمل اللائق، والمدن المستدامة. وتم في هذا البحث تحليل استراتيجيات الأمن السيبراني في العراق وبعض الدول العربية، مع التركيز على التحديات والفرص المتاحة، وتسليط الضوء على أهمية تعزيز التعاون الدولي وتبادل الخبرات لتحسين الأمن السيبراني لغرض تجاوز التحديات والمعوقات، والتي من بينها، نقص الموارد، وضعف الوعي المجتمعي، وعدم وجود تشريعات كافية. وهناك حاجة إلى تطوير سياسات متكاملة تعالج التهديدات السيبرانية مع مراعاة البعد البيئي والاجتماعي. يدعم الأمن السيبراني النمو الاقتصادي من خلال حماية البنية التحتية الرقمية وحقوق الملكية الفكرية، وتعزيز الابتكار المستدام من خلال توفير بيئة آمنة للبحث والتطوير، وحماية الأنظمة الذكية التي تدعم إدارة الموارد والخدمات الحضرية. ويساهم في تعزيز المرونة الرقمية للمدن، مما يدعم تحقيق الهدف 11 من أهداف التنمية المستدامة. الأمن السيبراني ليس مجرد قضية تقنية، بل هو عنصر أساسي لتحقيق التنمية المستدامة، وبناء على هذه الحقيقة تبرز الحاجة الماسة لتعزيز استراتيجيات الأمن السيبراني ومواءمتها مع أهداف التنمية المستدامة لضمان مستقبل آمن ومستدام، وتفعيل التعاون الدولي وتبادل الخبرات وتأمينها على المستوى العالمي. يضاف الى ذلك تطوير استراتيجيات وطنية للأمن السيبراني تتوافق مع أهداف التنمية المستدامة، وتعزيز الوعي المجتمعي بأهمية الأمن السيبراني ودوره في تحقيق الاستدامة، ورفع مستوى التكامل بين القطاعين العام والخاص، وتشجيع الاستثمار في البحث العلمي لتطوير تقنيات أمنية مستدامة.

الكلمات الرئيسية: الأمن السيبراني؛ ستراتيجيات الامن السيبراني؛ أهداف التنمية المستدامة.(SDGs)

المقدمة

يشير مفهوم الأمن السيبراني Cybersecurity، أو أمن الكمبيوتر ComputerSecurity ، إلى ممارسة حماية أنظمة الكمبيوتر والشبكات والأجهزة والبيانات من الهجمات الإلكترونية أو الأضرار أو الوصول غير المصرح به. والأمن السيبراني مجال ذو أهمية كبيرة حيث تُستخدم أنظمة المعلومات والشبكات بشكل متزايد في العديد من القطاعات، بما في ذلك التجارة والمالية والصحة والتعليم والحكومة. وقد بات الأمر أكثر أهمية في عالم متصل بشكل متزايد، حيث تُنفذ العديد من أنشطتنا اليومية عبر الإنترنت. لذلك يصبح من الضروري ضمان أمان التقنيات الرقمية المستخدمة لتحقيق أهداف مهمة، مثل حماية خصوصية المستخدم، ومنع انتشار المعلومات المضللة والمحتوى الضار، وحماية البنية التحتية الحيوية مثل شبكات الكهرباء والمياه والنقل. وينضوي تحت مفهوم الأمن السيبراني استخدام تقنيات وأدوات الأمان، مثل التشفير Encryption ، وجدران الحماية Firewalls ، ومضادات الفيروسات Antivirus Software ، وأنظمة اكتشاف التسلل Intrusion

Detection Systems، والمصادقة على المستخدمين , and User Authentication علاوة على ذلك، فأن تعريف سياسات الأمان Security Policies ، وتدريب المستخدمين User Training ، وإدارة المخاطر Risk Management ، من أجل حماية أنظمة الكمبيوتر والشبكات من التهديدات الخارجية والداخلية، هي من بين متطلبات الامن السيبراني. مع تزايد الاعتماد على التكنولوجيا الرقمية وتزايد ترابط العالم من خلال الشبكات الرقمية، في مختلف مجالات الحياة، أصبحت التهديدات السيبرانية واحدة من أكبر التحديات التي تواجه الأفراد والمؤسسات والدول. حيث لم يعد الأمن السيبراني مسألة تقنية فقط بل بات قضية استراتيجية تؤثر على التنمية الاقتصادية والاجتماعية والبيئية. ويحتم هذا الواقع تدابير ضرورية لتعزيز الأمن السيبراني من اجل حماية البنية التحتية الحيوية والخدمات الأساسية والبيانات الشخصية، وكل هذه التدابير ضرورية لتحقيق أهداف التنمية المستدامة . ونظرا لهذا الواقع، برزت الحاجة إلى تعزيز استراتيجيات الأمن السيبراني ومواءمتها مع أهداف التنمية المستدامة لضمان مستقبل آمن ومستدام.وقد أدى التحول الرقمي السريع للمجتمع إلى خلق العديد من الفرص للتنمية المستدامة. ومع ذلك، فقد أدخلت أيضًا العديد من التحديات، لا سيما في مجال الأمن السيبراني. ولضمان استمرارية وموثوقية الخدمات التي تدعم النمو الاقتصادي والشمول الاجتماعي والاستدامة البيئية ، من الضروري حماية البنية التحتية الرقمية ضد التهديدات السيبرانية. ومن دواعي التدابير المطلوبة لتعزيز الامن السيبراني ايضا النظر بجدية الى الترابط بين الأمن السيبراني والتنمية المستدامة من خلال ربط مبادرات الأمن السيبراني بأهداف التنمية المستدامة. أن التداخل بين الأمن السيبراني والتنمية المستدامة هو مجال حيوي يتطلب اهتمامًا وتركيزًا على العمل (Pallardy, 2024). حيث أن حماية البنية التحتية الرقمية والبيانات ليست مجرد مسألة أمنية فحسب، بل هي أيضًا شرط أساسي للتنمية المستدامة، فالعالم الذي يواصل التنقل عبر تعقيدات العصر الرقمي، مطالب وباهمية بالغة لدمج تدابير الأمن السيبراني في جهود التنمية المستدامة. الشكل (1) يوضح ا(2015/9/25. https://www.un.org/sustainabledevelopment/ar/2015/09)اهداف الامم المتحدة للتنمية المستدامة. ويتضمن هذا الشكل، 17 هدفا (اهداف التنمية المستدامة ، 2025) ، وهي التي تم اعتمادها من قبل جميع دول الأعضاء في الأمم المتحدة في عام 2015 ولها موعد نهائي في عام 2030، وتتضمن : (1) لا للفقر (القضاء على الفقر)، (2) القضاء على الجوع ، (3) الصحة الجيدة والرفاهية، (4) التعليم الجيد ، (5) المساواة بين الجنسين (6) المياه النظيفة والصرف الصحي، (7) طاقة ميسورة ونظيفة ، (8) العمل اللائق والنمو الاقتصادي ، (9) الصناعة والابتكار والبنية التحتية ، (10) تقليل الفوارق ، (11) المدن والمجتمعات المستدامة ، (12) الاستهلاك والإنتاج المسؤول ، (13) العمل المناخي ، (14) الحياة تحت الماء ، (15) الحياة على اليابسة ، (16) السلام والعدالة والمؤسسات القوية ، (17) الشراكات من أجل الأهداف.

شكل (1) اهداف الامم المتحدة للتنمية المستدامة (SDGs)

تمثل أهداف الامم المتحدة للتنمية المستدامة (SDGs) دعوة عالمية للعمل من أجل إنهاء الفقر وحماية الكوكب، وضمان تمتع جميع الناس بالسلام والازدهار بحلول عام 2030. وفي هذا الإطار يبرز محور الأمن السيبراني كعنصر محوري، بالرغم من انه غير مذكور بشكل صريح ولكنه بطبيعته محور حاسم لتحقيق العديد من أهداف التنمية المستدامة. من بين الاهداف الاساسية لهذا البحث هو تحديد نطاق الأمن السيبراني في سياق أهداف التنمية المستدامة، مع تسليط الضوء على أهميته في تسهيل تحقيقها عبر مختلف القطاعات، حيث يبرز دور الأمن السيبراني بشكل أساسي من خلال دوره في حماية تكنولوجيا المعلومات والاتصالات Information and Communication Technology (ICTs) التي تشكل أساس الاقتصاديات والمجتمعات الحديثة. تستطيع تدابير الأمن السيبراني ضمان نزاهة البيانات وسريتها وتوافرها، وهو أمر بالغ الأهمية لتعزيز النمو الاقتصادي (الهدف 8 من أهداف التنمية المستدامة)، وضمان حياة صحية (الهدف 3 من أهداف التنمية المستدامة)، وتمكين التعليم الجيد الشامل والعادل (الهدف 4 من أهداف التنمية المستدامة). علاوة على ذلك، لا يمكن تجاهل دور الأمن السيبراني في الاستدامة البيئية (الأهداف 13، 14، و15). حماية البيانات المتعلقة بمراقبة المناخ وحماية البيئة أمر حيوي لاتخاذ قرارات مستنيرة واتخاذ إجراءات بشأن تغير المناخ والحفاظ على التنوع البيولوجي. لذلك، فإن تدابير الأمن السيبراني ضرورية لحماية المستودعات الرقمية للمعرفة والبيانات الأساسية لاستدامة الموارد الطبيعية والنظم البيئية. أن العلاقة التداخلية المتمثلة بتقاطع الأمن السيبراني مع أهداف التنمية المستدامة تمثل مجالًا متعدد الأوجه حيث تدعم تدابير الأمن الرقمي وتمكن من تحقيق الأهداف العالمية. ومع استمرار تطور المشهد الرقمي، سيظل دمج الأمن السيبراني ضمن إطار أهداف التنمية المستدامة مجالًا حيويًا للسياسات والممارسات والبحث، مما يضمن أن تساهم افاق التطور في التقنيات الرقمية بشكل إيجابي في تحقيق نتائج التنمية المستدامة، (Odumesi, & Sanusi, 20232)، و(Fallah, et, al., 2022) .

أهداف البحث : الهدف من هذه الدراسة هو استكشاف التقاطع الحاسم بين الأمن السيبراني والتنمية المستدامة، مع التركيز على فهم كيفية دعم وتعزيز تدابير الأمن السيبراني لتحقيق أهداف التنمية المستدامة (SDGs). يهدف إلى تحديد دور الأمن السيبراني في حماية البنية التحتية الرقمية، وحماية البيانات الشخصية، وضمان سلامة الأنظمة التي تدعم الجوانب الرئيسية للتنمية المستدامة عبر الأبعاد الاقتصادية والاجتماعية والبيئية. زمن اهداف البحث ايضا تحليل واقع الأمن السيبراني في العراق والدول العربية بموجب تقارير التقييم الوطنية والعالمية. وتناقش الدراسة في هذا البحث الاتجاهات الناشئة في الأمن السيبراني، وتقييم التحديات والفرص في الأمن السيبراني.

المبحث الاول

التكامل بين اوجه الأمن السيبراني والاستدامة: تمثل مسيرة تطور الأمن السيبراني في عصر.الاستدامة تفاعلاً ديناميكياً بين التقدم التكنولوجي والفهم المتطور للاستدامة وهي نتاج للتطوير الحاصل في التقنيات الرقمية مصحوبا في السعي العالمي نحو التنمية المستدامة. وقد سجلت لحظات محورية في هذه المسيرة شكلت المشهد الحالي لمفهوم الأمن السيبراني في سياق التنمية المستدامة، والذي يتميز بالتوازن بين تلبية الاحتياجات الحالية دون المساس بقدرة الأجيال المستقبلية على تلبية احتياجاتها.
ويمكن تتبع التطور التاريخي للأمن السيبراني في سياق الاستدامة بالعودة إلى الأيام الأولى للإنترنت حيث كان التركيز بشكل أساسي على حماية محيطات الشبكة وتأمين البيانات من الوصول غير المصرح به. ومع تطور الإنترنت حيث اصبح منصة عالمية للتجارة والتواصل والحكم، توسع نطاق الأمن السيبراني ليشمل حماية البنية التحتية الحيوية، والخصوصية الشخصية، وسلامة المعاملات الرقمية. ويعكس هذا التطور اعترافًا متزايدًا بترابط الأمن الرقمي والتنمية المستدامة، حيث لا يقتصر الأمن السيبراني على حماية المعلومات فحسب، بل يشمل أيضًا ضمان مرونة الأنظمة التي تدعم الرفاهية الاقتصادية والاجتماعية. يقدم (Zharova, & Chechel, 2020) تحليلاً عميقاً للجوانب التاريخية للتنمية المستدامة، متتبعين تطورها جنباً إلى جنب مع التغيرات الاقتصادية. إن دمج الأمن السيبراني ضمن إطار أهداف التنمية المستدامة (SDGs) هو مسعى حيوي يهدف لضمان مرونة وأمان البنى التحتية الرقمية، التي تعد محورية في تحقيق التنمية المستدامة على مستوى العالم، ويمكن رؤية الرابط بين الأمن السيبراني وأهداف التنمية المستدامة من وجهات نظر مختلفة(يماني, 2020) ، ومنها:
حماية خصوصية وأمان المعلومات الشخصية: يمكن للأمن السيبراني أن يساعد في حماية خصوصية وأمان المعلومات الشخصية، وهو هدف مهم للعديد من أهداف التنمية المستدامة. على سبيل المثال، الهدف 3 من أهداف التنمية المستدامة يتعلق بتعزيز الصحة والرفاهية، والذي قد يشمل جمع المعلومات الشخصية عن المرضى. يمكن للأمن السيبراني أن يساعد في حماية هذه المعلومات من الوصول غير المصرح به.
مكافحة الجرائم الإلكترونية: يمكن للأمن السيبراني أن يساعد في مكافحة الجرائم الإلكترونية، مثل الاحتيال عبر الإنترنت والتنمر الإلكتروني، والتي يمكن أن تشكل تهديدًا لسلامة الأفراد والمجتمعات. مكافحة الجرائم الإلكترونية مهمة للعديد من أهداف التنمية المستدامة، بما في ذلك الهدف 16 الذي يتعلق بتعزيز المجتمعات السلمية والشاملة.
تعزيز الاستدامة البيئية: يمكن للأمن السيبراني أن يساعد في تعزيز البنى التحتية والاستدامة البيئية وهو مطلب مهم للعديد من أهداف التنمية المستدامة ، ومنها الاهداف 7 ، و 9، و 11. وفي هذا السياق يمكن استخدام الأمن السيبراني لحماية البنية التحتية الحيوية، مثل الطاقة والمياه، من الهجمات السيبرانية التي قد تسبب أضرارًا بيئية.
العمل اللائق والنمو الاقتصادي : الأمن السيبراني ضروري لحماية البيانات الشخصية والمالية للعمال والشركات. بدون أنظمة الأمن السيبراني المناسبة، يمكن أن تكون المعلومات الحساسة عرضة للهجمات السيبرانية، مما يتسبب في أضرار مالية ويؤثر على سمعة الشركات. (الهدف 8)
التعليم الجيد: تعليم الأمن السيبراني في المدارس والجامعات مهم لرفع الوعي بالأمن السيبراني ولإعداد الأجيال القادمة للتعامل مع التكنولوجيا بشكل آمن. (الهدف الرابع للتنمية المستدامة) وهذه تمثل أمثلة قليلة على كيفية ربط الأمن السيبراني بأهداف التنمية المستدامة. مع تزايد استخدام تكنولوجيا المعلومات والاتصالات، تزداد أيضًا تهديدات الهجمات الإلكترونية، مثل سرقة البيانات

الشخصية، وانتشار البرمجيات الخبيثة، وبرامج الفدية، والهجمات الإلكترونية الأخرى التي يمكن أن تعرض أمن وخصوصية وثقة المستخدمين للخطر.

المبحث الثاني

دور الأمن السيبراني في تعزيز بعض الجوانب الاساسية للاستدامة: في ظل التحول الرقمي المتسارع الذي يشهده العالم، أصبح الأمن السيبراني عنصرًا حيويًا لا غنى عنه لضمان استدامة المجتمعات والاقتصادات. يلعب الأمن السيبراني دورًا محوريًا في حماية البنية التحتية الرقمية والبيانات الحساسة مما يدعم تحقيق العديد من أهداف التنمية المستدامة. من خلال تأمين الأنظمة الرقمية، يسهم الأمن السيبراني في تعزيز النمو الاقتصادي، ودعم الابتكار المستدام، وحماية البيئة، وضمان استقرار المدن الذكية والمجتمعات الرقمية. في هذا السياق، يبرز الأمن السيبراني كأداة أساسية لتحقيق التوازن بين التطور التكنولوجي والمتطلبات البيئية والاجتماعية، مما يضمن مستقبلًا آمنًا ومستدامًا للأجيال القادمة.

المطلب الاول : دور الأمن السيبراني في تعزيز النمو الاقتصادي المستدام

ان حماية البيانات والأنظمة المختلفة من التهديدات الإلكترونية ضرورة ملحّة لتحقيق استقرار الأعمال وضمان استمرارية العمليات في مختلف القطاعات. ومع تزايد الاعتماد على التقنيات الرقمية والابتكارات التكنولوجية، يبرز دور الأمن السيبراني كعامل حاسم في تعزيز النمو الاقتصادي المستدام.يُسهم الأمن السيبراني في توفير بيئة آمنة للاستثمار والابتكار، مما يعزز من ثقة الشركات والمستثمرين في الأسواق الرقمية. كما يساعد في حماية المؤسسات من التكاليف المرتفعة المرتبطة بالاختراقات الأمنية، مثل فقدان البيانات، والانقطاع عن العمل، والإضرار بالسمعة. علاوةً على ذلك،يُحفّز الأمن السيبراني على تطوير المهارات التقنية وبناء القدرات البشرية، مما يُعزز فرص العمل ويساهم في دفع عجلة التنمية الاقتصادية. إن استثمار الدول والشركات في تعزيز البنية التحتية للأمن السيبراني لا يقتصر على الحماية فحسب، بل يُعد استثمارًا استراتيجيًا لتحقيق استدامة اقتصادية طويلة الأمد في ظل عالم رقمي مليء بالتحديات والفرص. يضاف الى ذلك ان التكامل بين الأمن السيبراني وأهداف التنمية المستدامة (SDGs) أمر محوري يعزز النمو الاقتصادي المستدام. يلعب الأمن السيبراني دورًا حيويًا في حماية البنية التحتية الرقمية التي تدعم الأنشطة الاقتصادية في العالم الحديث. (Vasiu , & Vasiu., 2018) يسلطان الضوء على الدور الحاسم للأمن السيبراني في تحقيق أهداف التنمية المستدامة، مشيرين إلى أن حماية البنية التحتية الحيوية والخدمات الأساسية والبيانات الشخصية أمر ضروري للتنمية المستدامة وضمان موثوقية ونزاهة الأنظمة الرقمية التي تدعم النمو الاقتصادي والشمولية الاجتماعية والاستدامة البيئية. علاوة على ذلك، يقدم العصر الرقمي فرصًا مستحدثة وفعالة للوصول الى الناس والدعوة للمساهمة بجمع التبرعات التي يمكن أن ترفد خطط التنمية المستدامة للمجتمعات. يؤكد (Martz2025) بأن مشهد جمع التبرعات يتواصل في التطور، مدفوعًا بالتقدم التكنولوجي، وتغير توقعات المانحين، والأهمية المتزايدة لإنشاء تجارب ذات مغزى وشخصية، بالنسبة للمنظمات غير الربحية. ولغرض الاسهام في دعم اهداف التنمية المستدامة التي تخدم المجتمع من الضروري تبني استراتيجيات مبتكرة تشرك المتبرعين وتلهمهم للعمل. وتؤكد الدراسة على أهمية الأمن السيبراني في ضمان نزاهة وأمان منصات جمع التبرعات الرقمية، التي تعد ضرورية لتعبئة الموارد لمبادرات التنمية المستدامة.

المطلب الثاني : دور الأمن السيبراني في تعزيز التصنيع المستدام والابتكار

يعتبر الأمن السيبراني أساسي لحماية البنية التحتية الحيوية وحماية حقوق الملكية الفكرية، وكلاهما ضروري للتصنيع المستدام والابتكار. في عصر التحول الرقمي، ومع الاعتماد المتزايد على التقنيات الذكية مثل إنترنت الأشياء والذكاء الاصطناعي والتحليلات الضخمة، يواجه قطاع التصنيع تحديات جديدة تتعلق بأمن البيانات والأنظمة. يلعب الأمن السيبراني دورًا محوريًا في حماية هذه الأنظمة الرقمية، مما يضمن استمرارية العمليات الصناعية ويعزز الابتكار المستدام. فهو لا يقتصر على حماية المعلومات فقط، بل يمتد لدعم المرونة التكنولوجية، وتحفيز الثقة في الابتكارات، والحد من المخاطر التي قد تعيق تحقيق الأهداف المستدامة. في هذا السياق، يعد الأمن السيبراني أساسًا ضروريًا لبناء مستقبل صناعي آمن ومستدام (Obasi, et, al. 2024). توصلت بعض الدراسات الى وجود علاقة بين طول عمر الشركات، والمسؤولية الاجتماعية، وأصول الملكية الفكرية في سياق الاستدامة، وبالتحديد فيما يتعلق بالهدف 9 من أهداف التنمية المستدامة (Denoncourt, et al., 2020). واكدت هذه الدراسة الطلب المتزايد على الشفافية في الشركات وتفحص استجابة القطاع الخاص للعمل بشكل مستدام على المدى الطويل. وجرى التأكيد على أهمية الابتكار، والملكية الفكرية، والاستدامة والعلاقة الحيوية بين هذه العناصر ودور الأمن السيبراني، مما يدعم التصنيع المستدام والابتكار. ومع ظهور الثورة الصناعية الرابعة أدخلت تقنيات جديدة، مثل الروبوتات المستقلة ذاتية التحكم، التي لديها القدرة على التأثير بشكل كبير على التنمية المستدامة (Aymerich-Franch, et, al., 2022) ، والتي اثبتت دورها المهم كأحد تقنيات الثورة الصناعية الرابعة وخاصة خلال مواجهة جائحة كوفيد-19. وبشكل عام من الضروري وجود استراتيجيات شاملة للأمن السيبراني لحماية هذه التقنيات من التهديدات السيبرانية، مما يضمن مساهمتها الفعالة في التنمية المستدامة، وبالنتيجة تعزيز التصنيع المستدام والابتكار.

المطلب الثالث : دور الأمن السيبراني في ضمان مدن ومجتمعات مستدامة

مع التقدم التكنولوجي السريع والتحول نحو المدن الذكية والمجتمعات الرقمية، أصبح الأمن السيبراني عنصراً حيوياً لضمان استدامة هذه البيئات الحديثة. تعتمد المدن المستدامة على بنية تحتية رقمية متكاملة تشمل أنظمة إدارة الموارد، والنقل الذكي، والرعاية الصحية الرقمية، والخدمات الحكومية الإلكترونية. هذه الأنظمة تتطلب حماية قوية ضد التهديدات السيبرانية التي قد تؤدي إلى تعطيل العمليات الحيوية أو انتهاك خصوصية الأفراد. يلعب الأمن السيبراني دوراً محورياً في تأمين البيانات الحساسة، وضمان استمرارية الخدمات، والحفاظ على ثقة المواطنين في التكنولوجيا المستخدمة. بالإضافة إلى ذلك، يساهم في تعزيز كفاءة إدارة الموارد وتقليل الأثر البيئي من خلال حماية الأنظمة الذكية التي تعتمد على التكنولوجيا لتقليل استهلاك الطاقة والمياه وتحسين جودة الحياة. من خلال الاستثمار في سياسات أمنية قوية وبناء قدرات بشرية وتقنية قادرة على مواجهة التهديدات المستجدة، يمكن تحقيق التوازن بين التطور التكنولوجي والاحتياجات الأمنية، مما يدعم رؤية المجتمعات المستدامة ويضمن مستقبلًا أكثر أماناً وازدهاراً. إن دمج الأمن السيبراني ضمن إطار أهداف التنمية المستدامة (SDGs)، ولا سيما الهدف 11 الذي يهدف إلى جعل المدن والمجتمعات شاملة وآمنة وقادرة على الصمود ومستدامة، هو أمر بالغ الأهمية ويبرز فيه دور المرونة الرقمية في تعزيز الاستدامة الحضرية. ومفهوم المرونة في التنمية الحضرية ، الذي يمكن تعريفه بانه يمثل القدرة على الاستشعار والاستعداد الوقائي لمواجهة التهديدات السيبرانية ومقاومتها والرد عليها سواء كانت متوقعة او غير متوقعه ،أساسي لتحقيق الهدف 11 من أهداف التنمية المستدامة

(عبدالصادق، 2022)[1]، و(Shahid, & Ahmed. 2022) وبموجب ذلك من الضروري تضمين مؤشرات المرونة في إطار التنمية وبنية السياسات لجعل المدن والمجتمعات مستدامة. الأمن السيبراني هو جزء لا يتجزأ من هذه المرونة، حيث يضمن حماية البنية التحتية الرقمية وأنظمة المعلومات التي تعتبر حيوية لعمل المدن الحديثة. يلعب الأمن السيبراني دورًا حيويًا في هذا السياق من خلال حماية الأدوات والمنصات الرقمية التي تدعم جهود التخطيط والتطوير الحضري، مما يسهل تنفيذ السياسات الحضرية المستدامة. علاوة على ذلك، فإن تطبيق تقنيات الاستشعار عن بعد في مراقبة وتطوير المدن والمجتمعات المستدامة يبرز أهمية الأمن السيبراني (Ekmen,&Kocaman, 2023).ستظل أهمية الأمن السيبراني في تحقيق الهدف 11 من أهداف التنمية المستدامة ذات أهمية قصوى، وإن ضمان المرونة الرقمية من خلال تدابير فعالة للأمن السيبراني أمر ضروري لتعزيز التنمية الحضرية المستدامة وخلق مدن ومجتمعات شاملة وآمنة ومرنة ومستدامة. وهذا ماتؤكده دراسات تضمنت رؤى قيمة حول دور الأمن السيبراني في تعزيز المرونة الحضرية والاستدامة (Bouteche, & Bougdah, 2023)، و(Ekmen, & Kocaman, 2023).

المبحث الثالث

استراتيجيات الأمن السيبراني الوطنية والأجندة العالمية للاستدامة

المطلب الاول: استراتيجيات الأمن السيبراني الوطنية للعراق وبعض الدول العربية: أن اعداد استراتيجيات وطنية محددة وموثقة للأمن السيبراني واعتمادها يعتبر امرا مهمًا لضمان التوافق مع الأجندة العالمية للاستدامة، وحماية البنى التحتية المختلفة من الهجمات الإلكترونية التي قد تعرقل تحقيق أهداف الاستدامة. علاوة على ذلك فأن الاعتماد على التكنولوجيا الرقمية ضروري لتحقيق التقدم في مجالات مثل الشمول المالي والصحة الرقمية[2] ، وكذلك لتحقيف أهداف مثل التعليم الجيد (الهدف 4)، الصناعة والابتكار (الهدف 9)، والعمل اللائق والنمو الاقتصادي (الهدف 8). وتعزز استراتيجيات الأمن السيبراني الوطنية الثقة في الأنظمة الرقمية، اضافة الى تفعيل التعاون الدولي والمحلي، وهو ما يتماشى مع الهدف 17 من أهداف التنمية المستدامة (عقد الشراكات لتحقيق الأهداف) ، والتي يمكن من خلالها تبادل الخبرات وأفضل الممارسات في مجال الأمن السيبراني. ومع تزايد أهمية البيانات في تطوير سياسات مستدامة، يتطلب الأمر وجود استراتيجيات قوية لحمايتها. هذا يتماشى مع الهدف 16 (السلام والعدل والمؤسسات القوية)، الذي يدعو إلى حماية حقوق الأفراد وضمان العدالة. ويساهم الأمن السيبراني في تقليل الهجمات التي قد تعطل الأنظمة الرقمية، مما يقلل من الهدر في الموارد والطاقة المستخدمة في استعادة الأنظمة، وبالتالي دعم الهدف 13 (العمل المناخي). يؤكد (Donalds, et, al., 2022) على ضرورة تطوير وتنفيذ استراتيجية وطنية للأمن السيبراني، لحماية البنى التحتية الرقمية الحيوية وضمان التقدم الآمن نحو التنمية المستدامة. وتؤكد دراستهم على الترابط بين الأمن السيبراني والأهداف الأوسع لمبادئ التنمية

1عبدالصادق، عادل. (2022). المرونة السيبرانية والتنمية المستدامة في العصر الرقمي. 2 نوفمبر 2022. المركز العربي لابحاث الفضاء الالكتروني .
https://accronline.com/article_detail.aspx?id=37896&srsltid=AfmBOopZEpcIQEgQEgNPoNCTLYIn9Tg0_SZfonddPfP17gn-pi05Spc4

2الشمول المالي : إتاحة مختلف الخدمات المالية للاستخدام من قبل جميع فئات المجتمع، من خلال القنوات الرسمية بجودة وتكلفة مناسبة مع حماية حقوق المستفيدين من تلك الخدمات، بما يمكنهم من إدارة أموالهم بشكل سليم.
الصحة الرقمية : هي التقاء التقنيات الرقمية مع الصحة والرعاية الصحية والمعيشة والمجتمع لتعزيز كفاءة تقديم الرعاية الصحية وجعل الأدوية أكثر تخصيصًا ودقة.

المستدامة، داعين إلى نهج متكامل ينسجم مع استراتيجيات الأمن السيبراني الوطنية والأجندة العالمية للاستدامة. علاوة على ذلك، فإن التعقيد والطبيعة الديناميكية للتهديدات السيبرانية تتطلب إطار حوكمة يكون متكيفا ومرناً في الوقت نفسه. يقترح (Melaku, 2023) إطار حوكمة ديناميكي وتكيفي للأمن السيبراني يعالج قيود الأطر الحالية من خلال دمج مكونات مثل البحث والتطوير، والتعاون بين القطاعين العام والخاص، والامتثال للقوانين واللوائح. تم تصميم هذا الإطار لتوفير التوجيه الاستراتيجي، وإدارة مخاطر الأمن بشكل فعال، وتحسين استخدام الموارد التنظيمية، مما يدعم التنمية الآمنة والمستدامة للبنى التحتية الرقمية الحيوية لتحقيق أهداف التنمية المستدامة. مع استمرار تطور المشهد الرقمي، سيصبح دور الأمن السيبراني في دعم التنمية المستدامة أكثر أهمية، مما يستلزم البحث المستمر والتعاون والابتكار لمعالجة التحديات المعقدة عند تقاطع الأمن السيبراني والاستدامة. وتماشيا مع هذا الواقع ، فأن دول العالم المختلفة اصدرت وتبنت ستراتجيات وطنية واقليمية للامن السيبراني. وفي العراق اصدرت مستشارية الامن الوطني في العام 2022 (استراتيجية الامن السيبراني العراقي) لتوفير خارطة طريق متماسكة ومبادرات وآليات لتنفيذ و لتحقيق الرؤية الوطنية بشأن الأمن السيبراني وعلى مديات قصيرة ومتوسطة وطويلة الامد. وتضمنت هذه الاستراتيجية عناصرالاستعداد الوطني لغرض توفير تدابير متماسكة وإجراءات استراتيجية لضمان أمن وحماية الوجود العراقي في الفضاء السيبراني، وحماية البنية التحتية الحيوية للمعلومات، وبناء ورعاية مجتمع إنترنت موثوق به.وتعرف استراتيجية الامن السيبراني العراقي المخاطر السيبرانية بأنها "احتمال وجود تهديد وهشاشة داخل الفضاء الإلكتروني للبلد يضر بأمن وسلامة نظم المعلومات وهياكل البنى التحتية المعلوماتية الأساسية. وعلاوة على ذلك، فإن التهديدات يمكن ان تستغل الثغرات الحالية الموجودة وبشكل يؤثر على سلامة وأمن نظام المعلومات أو شبكات المعلومات أو البنى التحتية للشبكات."وبموجب هذه الاستراتيجية، حددت الاهداف التالية بكونها تمثل أهداف الاستراتيجية الوطنية العراقية للأمن السيبراني:

- وضع تشريعات شاملة لمكافحة الجريمة السيبرانية والتدابير المضادة للتهديد السيبراني التي يمكن اعتمادها على الصعيد الوطني، والإقليمي والعالمي ذات الصلة في سياق تأمين الفضاء السيبراني للبلاد.
- توفير التدابير التي تحمي البنية التحتية الحيوية للمعلومات، فضلا عن الحد من مواطن الضعف والثغرات الوطنية من خلال إطار ضمان الأمن السيبراني.
- وضع الية فعالة للاستجابة لحالات الطوارئ في الحاسوب.
- العمل على تحسين قدرة وتطوير فريق الاستجابة لحالات الطوارئ في الحاسوب العراقي (CERT).
- إن الآليات الوطنية لبناء القدرات والتوعية العامة وتمكين المهارات ضرورية للمساعدة في تعزيز القدرة على الاستجابة السريعة والفعالة للهجمات السيبرانية.
- وضع آلية موثوقة لإشراك أصحاب المصالح المتعددين والوطنيين والدوليين من أجل التصدي بشكل جماعي للتهديدات السيبرانية.
- ردع وحماية الحكومة من جميع أشكال الهجمات السيبرانية.
- تنسيق مبادرة الأمن السيبراني على جميع مستويات الحكومة في البلاد.

ومما تجدر الاشارة اليه أن بين اهداف الاستراتيجية الوطنية العراقية والعديد من الاهداف العالمية للتنمية المستدامة تداخلا مضمن بصورة تخدم التكامل لغرض السير بخطوات الى الامام نحو تحقيق الخطط الاممية لأهداف التنمية المستدامة.

وبالنظر الى الدول العربية الاخرى، فأن أغلبها لديها ذات الاهتمام الذي توليه مستشارية الامن الوطني العراقية، وقد اعتمدت هذه الدول ستراتيجيات وطنية واولت الموضوع اهمية قصوى في نواحي التنفيذ والتوعية والمتابعة، وفي الجدول (1) ، بعض المعلومات والاحصاءات المتعلقة بالستراتيجات الوطنية للامن السيبراني للمجموعة من الدول العربية.

جدول (1): أحصاءات وبيانات متعلقة بالستراتيجيات الوطنية للامن السيبراني للعراق ومجموعة من الدول العربية

الدولة	الاستراتيجية الوطنية للأمن السيبراني، و (سنة الاصدار)	عدد الحوادث السيبرانية المسجلة (2023) ، وأنواعها.	المبادرات والتدابير	التحديات، ونسبة الوعي المجتمعي بالأمن السيبراني (%)	الترابط مع أهداف التنمية المستدامة (SDGs)
العراق	خطة تعزيز الأمن السيبراني ضمن برامج التحول الرقمي. (2022).	(+60) - اختراق المواقع الحكومية.- هجمات الحرمان من الخدمة.- التصيد الاحتيالي.	- تشكيل لجان مختصة للأمن السيبراني.- مشاريع لتطوير البنية التحتية الرقمية.- تعزيز التعاون الإقليمي.	- نقص الكوادر المؤهلة.- تحديات التمويل.- تطور الهجمات الإلكترونية. (35%)	- تعزيز الشراكات الإقليمية (الهدف 17).- بناء مؤسسات قوية (الهدف 16).
السعودية	الهيئة الوطنية للأمن السيبراني (NCA) أصدرت استراتيجية وطنية متكاملة. (2022)	(+250) - هجمات برامج الفدية.- التصيد الاحتيالي.- اختراق أنظمة الشركات.	- إنشاء الأكاديمية الوطنية للأمن السيبراني.- مبادرات تأهيل الكوادر الوطنية.- منصات لإدارة المخاطر.	- تطور التهديدات.- نقص الكفاءات المتخصصة.- تأمين البنى التحتية الحيوية. (85%)	- دعم الابتكار (الهدف 9).- تعزيز البنية التحتية الرقمية المستدامة (الهدف 11).
الإمارات	سياسة الأمن السيبراني للدولة. (2019)	(+180) - سرقة البيانات.- هجمات الحرمان من الخدمة (DDoS).- التصيد الاحتيالي.	- مركز الاستجابة لطوارئ الحاسب (aeCERT).- حملات التوعية المجتمعية.- شراكات عالمية.	- الهجمات المتطورة.- تكامل الأنظمة بين القطاعات. (80%)	- تحقيق الشراكات العالمية (الهدف 17).- تعزيز التعليم التقني (الهدف 4).
مصر	استراتيجية الأمن السيبراني ضمن رؤية مصر 2030. (2017)	(+200) - القرصنة المالية.- اختراق البريد الإلكتروني.- هجمات البرمجيات الخبيثة.	- مركز الأمن السيبراني الوطني.- تعزيز الحوكمة الرقمية.- قوانين حماية البيانات.	- ضعف الوعي المجتمعي.- تمويل المشاريع المتعلقة بالأمن السيبراني. (60%)	- دعم الصناعة والابتكار (الهدف 9).- بناء مؤسسات قوية (الهدف 16).
قطر	استراتيجية الأمن السيبراني 2022-2026. (2022)	(+100) -هجمات على البنية التحتية الحيوية.- التصيد الاحتيالي.- الاختراقات.	- مركز قطر للاستجابة لحوادث الحاسب (Q-CERT).- مبادرات التدريب والتأهيل.- حماية كأس العالم 2022.	- زيادة الاعتماد على التكنولوجيا.- حماية الفعاليات الكبرى. (75%)	- حماية البنى التحتية المستدامة (الهدف 11).- تعزيز القدرات الوطنية (الهدف 8).
الأردن	استراتيجية الأمن السيبراني الوطنية 2018-2023. (2018)	(+50) التصيد الاحتيالي.- استهداف الأنظمة الحكومية.- هجمات البرمجيات الخبيثة.	- تعزيز البنية التحتية الرقمية.- إطلاق برامج تدريبية.- إنشاء مراكز استجابة للحوادث السيبرانية.	- نقص التمويل.- قلة الوعي لدى بعض القطاعات. (50%)	- تحسين التعليم التقني (الهدف 4).- تعزيز الشراكات الإقليمية (الهدف 17).
سلطنة عمان	الاستراتيجية الوطنية للأمن السيبراني. (2021)	(+90) - سرقة البيانات.- التصيد الاحتيالي.- هجمات الحرمان من الخدمة.	- مركز الدفاع الإلكتروني.- برامج تدريبية مستمرة.- شراكات إقليمية ودولية.	- التهديدات الناشئة.- تحديات تطوير البنية التحتية. (70%)	- بناء مجتمعات آمنة (الهدف 16).- تعزيز الابتكار (الهدف 9).
المغرب	خطة وطنية للأمن السيبراني تركز على الحوكمة وحماية البيانات. (2020)	(+120) - هجمات البرمجيات الخبيثة.- اختراق الحسابات البنكية.- التصيد الاحتيالي.	- إنشاء المركز المغربي للأمن السيبراني.- قوانين لحماية البيانات الشخصية.- تدريب الكوادر.	- تطور الهجمات السيبرانية.- الحاجة للتعاون الإقليمي. (65%)	- تعزيز حماية البيانات (الهدف 16).- تحقيق التنمية الصناعية المستدامة (الهدف 9).
تونس	إطار وطني لتطوير الأمن السيبراني. (2019)	(+40) - القرصنة.- التصيد الاحتيالي.- هجمات على المواقع الإلكترونية.	- قوانين حماية البيانات.- مراكز الاستجابة للطوارئ الرقمية.- حملات التوعية.	- نقص الموارد التقنية.- قلة التنسيق بين القطاعات المختلفة. (55%)	- تعزيز التعليم (الهدف 4).- دعم البنية التحتية الرقمية (الهدف 9).
الكويت	استراتيجية الأمن السيبراني الوطنية بالتعاون مع الهيئة العامة للاتصالات. (2021)	(+70) - اختراق أنظمة البنوك.- هجمات البرمجيات الخبيثة.- سرقة البيانات.	- إنشاء مركز الكويت للأمن السيبراني.- حملات تدريب وتوعية.- قوانين لحماية البيانات الشخصية.	- التهديدات المتقدمة.- ضعف الوعي في بعض القطاعات.- نقص التعاون الإقليمي والدولي. (60%)	- بناء البنية التحتية الرقمية المستدامة (الهدف 9).- دعم الحوكمة الرقمية (الهدف 16).

أما بعض الدول العربية التي لم تذكر في الجدول (1) مثل : اليمن ، وجزر القمر ، وجيبوتي ، والصومال والسودان، فهي اجمالا تعاني من نقص في الأطر القانونية والتنظيمية المتعلقة بالأمن السيبراني، مما يجعلها أكثر عرضة للهجمات الإلكترونية. واضافة الى بعض التحديات الاقتصادية والسياسية ، فأن نسبة الوعي المجتمعي بالأمن السيبراني منخفضة في هذه الدول، مما يسهم في زيادة المخاطر والتهديدات الإلكترونية.

المطلب الثاني: واقع الامن السيبراني في العراق وبعض الدول العربية حسب تقارير الاتحاد الدولي للاتصالات

يقوم الاتحاد الدولي للاتصالات International Telecommunication Union بتقديم نظرة شاملة حول جهود الدول في تعزيز الأمن السيبراني. ويبين تقرير الاتحاد الدولي للاتصالات، الذي يصدرسنوياً منذ العام 2021 ، التقدم المحرز في سياسات وتدابير الأمن السيبراني، ويُسلط الضوء على التهديدات السيبرانية المتزايدة والمتطورة التي تواجه الدول في العالم الرقمي الحديث. يقوم التقرير بتقييم التزامات الدول في خمسة محاور رئيسية: الإطار القانوني: (Legal) ، الإطار الفني: (Technical) ، الإطار التنظيمي (Organizational):، تنمية القدرات (Capacity Building):، التعاون الدولي: (Cooperation) . كما يقدم تحليلًا جديدًا قائمًا على خمسة مستويات، مما يوفر تركيزًا أكبر على التطورات التي أحرزتها كل دولة وتأثيراتها في مجال الأمن السيبراني. من خلال تقديم تقييمات إقليمية ووطنية، يوفر التقرير خارطة طريق للدول لتعزيز قدراتها السيبرانية وضمان إدارة

آمنة وموثوقة للتهديدات السيبرانية في المستقبل.يقدم التقرير لعام 2024 تحليلًا من خمسة فئات (Tiers) لتصنيف الدول بناءً على مدى التزامها وتقدمها في مجال الأمن السيبراني. تشمل الفئات الدول "النموذجية" (Tier 1) والدول "في مرحلة البناء" (Tier 5). هذا التحليل يوفر تركيزًا أكثر وضوحًا على الفجوات والتقدم الذي تحققه الدول. حيث صنفت 46 دولة في المستوى الأول، وهو الأعلى بين المستويات الخمسة، والذي يُحتفظ به للدول "النموذجية" التي تظهر التزامًا قويًا في جميع محاور الأمن السيبراني الخمسة. وقد اظهر التقرير تفاوتا في الالتزام بشكل كبير بين الدول العربية. حيث صنفت دولا مثل الإمارات والسعودية مع المجموعة التي تعتبر نموذجًا يُحتذى به في الأمن السيبراني (خطاب،هبة، 2024)[3]، في الوقت الذي لا تزال دولا اخرى تعمل على تعزيز بنيتها التحتية للأمن السيبراني. وفي الجدول (2): تقييم الدول العربية وفقًا لتقرير الاتحاد الدولي للاتصالات 2024 مرتبة حسب قوتها والنتيجة التي حصلت عليها في حساب مؤشر الامن السيبراني العالمي، (الدماطي رامي.، 2024)[4]، ويظهر العراق في الفئة الربعة T4 – الدول المتطورة (Evolving) – (Score of20–55) . وهذه المجموعة توصف بكونها تعمل على تطوير سياساتها وبنيتها التحتية، لكنها بحاجة إلى مزيد من الجهود للوصول إلى مستويات أعلى من النضج السيبراني.

جدول (2): تقييم الدول العربية ومنها العراق وفقًا لتقرير الاتحاد الدولي للاتصالات 2024

الفئة	الدولة	الملاحظات
الفئة T1 – الدول الرائدة – (Role-Modelling) (Score of 95–100)	الإمارات	تُعتبر من الدول الرائدة عالميًا في الأمن السيبراني، مع تركيز على تعزيز التشريعات، التعاون الدولي، ووجود بنية تحتية قوية واستراتيجيات وطنية متقدمة.
	السعودية	طورت بنية تحتية متقدمة في مجال الأمن السيبراني، واستراتيجيات فعّالة تعزز القدرات الوطنية مع التركيز على التعاون الدولي.
	قطر	تمتلك منظومة أمن سيبراني شاملة، تشمل تدابير قانونية وتقنية قوية، بالإضافة إلى استراتيجية وطنية فعّالة.
	سلطنة عمان	لديها استراتيجيات وطنية فعالة، وفرق استجابة للحوادث السيبرانية، مع تركيز على تنمية القدرات والبنية التحتية.
	البحرين	تمتلك بنية تحتية قوية للأمن السيبراني، واستراتيجيات متقدمة تشمل تدابير قانونية وتنظيمية.
	مصر	تطورت بشكل ملحوظ في مجال الأمن السيبراني مع تعزيز التدابير القانونية، التقنية، والاستراتيجيات الوطنية.
	الأردن	تركز على تطوير أطر تنظيمية وتقنية متكاملة، وتعزيز التعاون الدولي في مجال الأمن السيبراني.
	المغرب	استثمرت في تعزيز بنيتها التحتية الرقمية، مع سياسات أمن سيبراني قوية وإجراءات تنظيمية متقدمة.
الفئة T2 – الدول المتقدمة – (Advancing) Score) (of 85–95		لم تُدرج أي من الدول العربية في هذه الفئة (T2) في تقرير "مؤشر الأمن السيبراني العالمي لعام 2024". هذه الفئة عادةً تشمل الدول التي لديها برامج وسياسات أمن سيبراني متقدمة وتعمل بجد للوصول إلى الريادة، ولكنها لا تصل بعد إلى مستوى الدول الرائدة في الفئة T1.
الفئة T3 – الدول النامية – (Establishing) (Score of 55–85)	الجزائر	تعمل على تطوير استراتيجيات وطنية للأمن السيبراني وتعزيز التدابير التقنية والاستجابة للحوادث.
	الكويت	بدأت في تطوير السياسات الوطنية، لكنها تحتاج إلى تعزيز الجهود في الجوانب التقنية والتنظيمية.
	تونس	بدأت في تعزيز بنيتها التحتية الرقمية وتطوير سياسات الأمن السيبراني، مع التركيز على التدابير القانونية.
	ليبيا	تواجه تحديات في البنية التحتية، لكنها تعمل على بناء أطر قانونية وتقنية لتعزيز الأمن السيبراني.
الفئة T4 – الدول المتطورة – (Evolving) Score of) (20–55	فلسطين	تعمل على بناء أطر قانونية وتقنية لحماية الفضاء السيبراني، مع جهود لتعزيز القدرات وتنمية الوعي.
	لبنان	تواجه تحديات في البنية التحتية، لكنها تسعى لتعزيز السياسات والتنظيمات الخاصة بالأمن السيبراني.
	العراق	يعمل على تعزيز بنيته التحتية للأمن السيبراني وتحسين التعاون الدولي، مع التركيز على الاستجابة للحوادث.
	جيبوتي	بدأت في تعزيز الأمن السيبراني، لكنها بحاجة إلى تحسين قدراتها التقنية والتنظيمية.
	موريتانيا	بدأت في وضع الأسس اللازمة للأمن السيبراني، لكنها تحتاج لدعم إضافي في بناء القدرات التقنية.
	السودان	تعمل على تطوير بنيتها الرقمية، وتحتاج إلى تحسين قدراتها التقنية وبناء الأطر التنظيمية.
	سوريا	تسعى لتعزيز قدراتها في الأمن السيبراني، لكنها تحتاج لدعم في مجال التعاون الدولي وتنمية القدرات.
	الصومال	تواجه تحديات كبيرة في بناء البنية التحتية الرقمية، وتعمل على تطوير استراتيجيات وطنية للأمن السيبراني.
	جزر القمر	تظهر تطورًا تدريجيًا في مجال الأمن السيبراني، مع الحاجة لتعزيز البنية التحتية والتدابير التقنية.
الفئة T5 – الدول في مرحلة	اليمن	تواجه تحديات كبيرة في مجال الأمن السيبراني بسبب نقص الموارد والبنية التحتية. تحتاج إلى دعم كبير لتعزيز القدرات

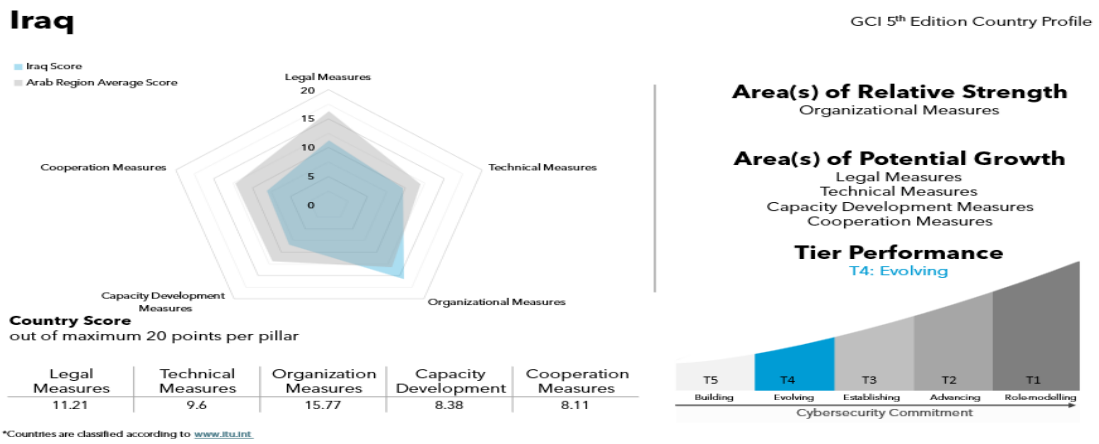
3خطاب، هبة .(2024). ترتيب الدول في الامن السيبراني 2024 : 3 دول عربية في المقدمة. المشهد. 14 سبتمبر 2024. https://almashhad.com/article/738996299126409-technology/ /

4الدماطي، رامي. (2024). دليل تحليلي عن: المؤشر العالمي للأمن السيبراني 2024 خاص بالدول العربية. ميتا سيرف اكاديمي. 14 سبتمبر 2024. https://www.metaserv.me/academy/resources/guides2/global-cybersecurity-index-2024-middle-east-countries-only/

البناء (Building):		وبناء بنية تحتية سيبرانية فعّالة.

ويفرد التقرير ملف تعريفي لكل دولة يحتوي على مؤشر الأمن السيبراني العالمي GlobalCybersecurity Index- 2024 لتلك الدولة ويتضمن نقاط التقييم ودرجة لمستوى الاداء وتحديد نقاط القوة والنقاط التي تحتاج الى المزيد من العمل واتخاذ الاجراءات المطلوبة. وفي الشكل (2)، الملف التعريفي لمؤشر الأمن السيبراني العالمي 2024 للعراق. ويتضح من المعوملوت الخاصة بالعراق الواردة في الشكل (2) انه مصنف ضمن الفئة الرابعة (Tier 4) وأن النتيجة لمؤشر الامن السيبراني والمكونة من درجات التقييم للمحاور الخمسة هو(Iraq Score GCI Index = 53.07 = 11.21+9.6+15.77+8.38+8.11) .

شكل (2) : الملف التعريفي لمؤشر الأمن السيبراني العالمي(Global Cybersecurity Index) 2024 للعراق.



ويتفاوت تسلسل العراق في مستوى مؤشر الامن السيبراني العالمي خلال الاعوام الماضية، حيث ظهر تسلسله 129 في قائمة دول العالم للعام 2020، في حين انه كان بالتسلسل 107 في التقرير الذي سبقه. وفي معرض الاسباب التي جعلت العراق في تلك المراكز بينت التقارير أن العراق لم يقدم اجابات عن الاستبيان الذي جمعه فريق GCI والذي تضمن بعض المعلومات والبيانات، حيث لاتوجد مؤسسة متخصصة بالأمن السيبراني في العراق، بل هي أقسام في دوائر مختلفة تفتقد للتنسيق أو التعاون المحترف في هذا الجانب، وكل جهة منها تعمل بمفردها. ودعت التقارير الحكومة العراقية إلى تشكيل مؤسسة أو هيئة خاصة تُعنى بقضايا الأمن السيبراني وكل ما يتعلق به في هذا الجانب،خصوصاً في اوقات الانتخابات حيث يكون للأمن السيبراني تأثيراً مباشراً على نتائجها .

المبحث الرابع

التحديات والعقبات التي تواجه دمج الأمن السيبراني مع جهود الاستدامة: يواجه دمج تدابير الأمن السيبراني مع جهود الاستدامة مجموعة متنوعة من التحديات والحواجز مما يعيق التقدم نحو تحقيق أهداف التنمية المستدامة (SDGs). . ومع التطور المتسارع للتكنولوجيا الرقمية، أصبح الأمن السيبراني والاستدامة من القضايا المحورية التي تؤثر على مستقبل المجتمعات والبيئة. ويهدف الأمن السيبراني إلى حماية المعلومات والأنظمة من التهديدات والهجمات، بينما تسعى جهود الاستدامة إلى تحقيق توازن بين التنمية الاقتصادية، الاجتماعية، والبيئية لضمان مستقبل مستدام للأجيال القادمة. ورغم أهمية كلا المجالين، فإن دمج الأمن السيبراني مع جهود الاستدامة يواجه العديد من التحديات والعقبات.

المطلب الاول : الأمن السيبراني والاستدامة: عقبات وتوصيات لتعزيز التكامل في عالم رقمي متغير

بالنظر الى التحديات الى تواجه الامن السيبراني، فأنه يتطلب تعزيز استخدام بنى تحتية وتقنيات متطورة وتخصيص موارد كبيرة، لغرض الحد من تأثيرات البصمة الكربونية (منصور, 2023).

والبصمة الكربونية مصطلح يشير الكمية الإجمالية من انبعاثات غاز ثاني أكسيد الكربون(CO_2) والغازات الدفيئة الأخرى التي تسهم في تغير المناخ والتي يمكن ربطها بشكل مباشر أو غير مباشر بأنشطة الأفراد، المؤسسات، و حتى الدول. وهي تتعلق بتقدير الأثر البيئي للأنشطة اليومية واستهلاك الموارد. كما تبرز الحاجة إلى تطوير سياسات واستراتيجيات توازن بين متطلبات الأمان واستدامة العمليات، وهي مهمة ليست بالسهلة في ظل تضارب الأولويات بين تحقيق الربحية الاقتصادية وتقليل الأثر البيئي. إضافة إلى ذلك، تواجه المؤسسات تحديات تتعلق بنقص الوعي والتكامل بين الفرق المختصة، حيث غالباً ما يتم التعامل مع الأمن السيبراني والاستدامة كموضوعين منفصلين، وقد تؤدي التشريعات غير الموحدة على الصعيدين المحلي والعالمي إلى تعقيد الجهود الرامية لدمج هذين المجالين بشكل فعال. في دراسة منشورة، يشير الباحثون (Norris, e al.,2018) إلى التهديد المستمر للهجمات السيبرانية والصعوبات في منع الهجمات الناجحة وتبحث الدراسة في التحديات المتعلقة بالأمن السيبراني التي تواجهها الحكومات المحلية الأمريكية، وتحدد عدة عوائق أمام توفير مستويات عالية من إدارة الأمن السيبراني، بما في ذلك نقص التمويل والموارد البشرية، ومشاكل الحوكمة، ونقص أو ضعف تطبيق سياسات الأمن السيبراني. تؤكد هذه التحديات على الصعوبات الملحوظة في عملية دمج الأمن السيبراني مع جهود الاستدامة، لا سيما في القطاع العام، حيث تعد حماية البنية التحتية الرقمية أمرًا بالغ الأهمية لتقديم الخدمات العامة وتحقيق أهداف التنمية المستدامة. ويعد النقص في الموارد المتاحة من التحديات والعوائق الكبيرة، ولابد من وضع اليات شاملة للمعالجة . وفي هذا الصدد توصي الدراسة المعدة من الباحثين (Chisty,et,al.,2022) على أهمية دمج التقنيات الجديدة، ومعالجة الجوانب البشرية، وتشجيع التعاون، والتأكيد على إدارة المخاطر، وقيام المنظمات وصانعي السياسات وأصحاب المصلحة بتعزيز التعاون وتبادل المعلومات، اضافة الى الاستثمار في التقنيات الناشئة، ورفع الوعي حول الأمن السيبراني، وبناء أطر تنظيمية تهدف الى تعزيز التعاون الدولي. إن دمج التعاون الدولي والمعايير العالمية في الأمن السيبراني أمر محوري لتعزيز الاستدامة ودعم تحقيق أهداف التنمية المستدامة (SDGs). تناقش الدراسة المنشورة للباحثين (Marx, & Wouters. 2014) واقع انتشار وتنوع المعايير الطوعية للاستدامة Voluntary Sustainability Standards (VSS) والتحديات الناشئة مثل فجوات المصداقية وزيادة تكاليف الشهادات.

المطلب الثاني: التهديدات والاختراقات وانعكساتها على الانجاز التنموي في العراق.

تشكل التهديدات والاختراقات الامنية بمختلف أنواعها، سواء كانت أمنيةً أو اقتصاديةً أو بيئيةً أو تكنولوجيةً أو اجتماعيةً، تحدياتٍ جسيمةً أمام الإنجاز التنموي للدول والمجتمعات. وتؤثر هذه التهديدات على قدرة الحكومات والمؤسسات على تحقيق أهداف التنمية المستدامة، وتُعطل الاستثمارات، وتُضعف الثقة في الأنظمة، وتُفاقم الفقر وعدم المساواة. حيث تؤدي التهديدات الأمنية ، كالصراعات المسلحة والإرهاب، الى تدمير البنية التحتية وتُهجير السكان، مما يُعيق توفير الخدمات الأساسية. وبسببها غالبا مايتم تُوجيه الموارد المالية نحو الإنفاق العسكري بدلًا من مشاريع الصحة والتعليم. كما وتؤدي الاختراقات الأمنية أو الفساد الى اضعاف شرعية الحكومات، مما يُصعب تنفيذ سياسات تنموية طويلة الأمد

وبنفس السياق تؤدي التهديدات الاقتصادية ، كالأزمات المالية والفساد، إلى انخفاض الاستثمارات وارتفاع البطالة، مما يُقلل من فرص تحسين مستوى المعيشة، ويُقلل من الموارد المتاحة للاستثمار في التعليم والصحة.

وتدمر التهديدات البيئية ، كالتغير المناخي والكوارث الطبيعية، المحاصيل الزراعية وتزيد من ندرة المياه، مما يُهدد الأمن الغذائي. في حين تتعرض البيانات الحساسة للسرقة بسبب التهديدات التكنولوجية ، كالاختراقات الإلكترونية، مما يُهدد الخصوصية ويُضعف الثقة في التحول الرقمي. ولايمكن بناء سياسات تنموية شاملة في ظل تواجد للتهديدات الاجتماعية ،كعدم الاستقرار السياسي والتفكك المجتمعي.

أما بخصوص منظومة الأمن الوطني (الاستراتيجي) للعراق، فأنها تواجه جملة من التحديات التي يمكن تصنيفها بالتحديات المرئية وغير المرئية، وتتجلى أخطرها بتلك التي تتمظهر بالصورة غير المرئية، فلا يمكن التماسها بصورة مباشرة إلا من خلال البحث والاستقراء التحليلي، وتشكل هذه التحديات تهديداً استراتيجياً من شأنها أن تؤثر على الأمن الاستراتيجي (للفرد والدولة)، بمعنى: أن هذه التحديات تشمل معظم القطاعات والمؤسسات الحكومية وغير الحكومية، التي تتمحور حول البنية التحتية للدولة وتتراوح هذه التحديات ما بين التهديدات السيبرانية للمنظومة الرقمية للدولة، وزيادة عدد السكان من دون أن يصيب هذه الزيادة تخطيطٌ استراتيجيٌ يواكب التطورات والتحديات المحدقة بمؤسسات الدولة الرسمية وغير الرسمية، فتشكل تحدياً كبيراً لمنظومة الأمن الاستراتيجي للعراق؛ وبالتالي باتت الضرورة الملحة تركز الجهود البحثية والاستشرافية وتسلطها في هذا المجال، ولاسيما في ظل الزيادة الملحوظة للتحديات المحدقة بمنظومة الأمن الاستراتيجي للعراق. وقد اعتمدت الحكومة العراقية سلسلة من الإجراءات لتعزيز فرص التمكين والتقدم في أجندة التنمية المستدامة وأهدافها بشكل عام. واعتبرت رؤية العراق بأن الشمول والوعي والمشاركة هي المفتاح الرئيس لتحقيق اهداف التنمية المستدامة، وذلك بالوصول إلى ما هو ابعد.

بالاضافة الى مفهوم الامن السيبراني، الذي تم توضيحه في هذا البحث ، نحتاج الى تحديد بعض المفاهيم الاخرى ذات الصلة ومن بينها، الجريمة السيبرانية ويتعرف بأنها أي مخالفة ترتكب ضد أفراد أو جماعات بدافع جرمي ونية الإساءة لسمعة الضحية أو لجسدها أو عقليتها، سواءً كان ذلك بطريقة مباشرة أو غير مباشرة، وأن يتم ذلك باستخدام وسائل الاتصالات الحديثة مثل الإنترنت، غرف الدردشة، البريد الإلكتروني أو المجموعات. وكذلك مفهوم الارهاب السيبراني والذي يشير الى استخدام التقنيات الرقمية لإخافة وإخضاع الآخرين أو هو القيام بمهاجمة نظم المعلومات على خلفية دوافع سياسية أو عرقية أو دينية.

المطلب الثالث : الانجازات التي تحققت في العراق وربطها بمظلة اهداف التنمية المستدامة

شهد العراق في السنوات الأخيرة تحولات كبيرة على الصعيدين السياسي والاقتصادي، رغم التحديات الأمنية والاقتصادية التي واجهها. وقد أسهمت هذه التحولات في تحقيق بعض الإنجازات التي يمكن ربطها بأهداف التنمية المستدامة (SDGs) التي أقرتها الأمم المتحدة عام 2015. وكما اسلفنا في المباحث والمطالب السابقة ، فأن الاهداف العالمية تتناول طيفا متعدد المجالات والتي من بينها القضاء على الفقر وحماية البيئة وغيرها، وتهدف إلى تحقيق تنمية شاملة ومستدامة بحلول عام 2030. والجدول (3)، يستعرض أبرز الإنجازات التي تحققت في العراق ويربطها بأهداف التنمية المستدامة (السيد ، محمد محسن) ، مع الاشارة الى التحديات التي رافقت انجازها.

جدول (3): أبرز الإنجازات التي تحققت في العراق والمرتبطة بأهداف التنمية المستدامة

الهدف	الإنجازات المتحققة في العراق	العلاقة بأهداف التنمية المستدامة	التحديات
الهدف 1: القضاء على الفقر	- انخفاض معدلات الفقر من 22.9% في 2007 إلى 20% في 2020. - برامج الحماية الاجتماعية مثل شبكة الأمان الاجتماعي.	يسعى العراق لتحقيق الهدف 1 من خلال تحسين الدخل وتوفير فرص العمل، لكن التحديات الأمنية والاقتصادية تعيق التقدم.	- ارتفاع معدلات الفقر بسبب النزاعات والأزمات الاقتصادية. - ضعف تنفيذ برامج الحماية الاجتماعية.
الهدف 2: القضاء	- تحسين الإنتاج الزراعي في بعض	العراق يعمل على تحقيق الأمن الغذائي، لكنه	- نقص الاستثمار في القطاع

على الجوع	المناطق. - برامج دعم المزارعين.	بحاجة إلى استثمارات أكبر في البنية التحتية الزراعية.	الزراعي. - تأثير التغير المناخي على الزراعة.
الهدف 3: الصحة الجيدة والرفاه	- تحسين الوصول إلى الخدمات الصحية الأساسية. - حملات التطعيم ضد الأمراض المعدية.	العراق يعمل على تحسين الصحة العامة، لكن الأزمات المالية والأمنية تحد من التقدم.	- ضعف البنية التحتية الصحية. - نقص الكوادر الطبية المؤهلة.
الهدف 4: التعليم الجيد	- زيادة معدلات الالتحاق بالمدارس الابتدائية. - إعادة تأهيل المدارس المتضررة.	العراق يعمل على تحسين التعليم، لكن التحديات الأمنية والاقتصادية تعيق تحقيق الهدف 4.	- نقص المدارس والكوادر التعليمية. - انخفاض جودة التعليم.
الهدف 5: المساواة بين الجنسين	- زيادة تمثيل المرأة في البرلمان (نسبة 25% من المقاعد). - تشريعات لدعم حقوق المرأة.	العراق يحقق تقدماً في تمكين المرأة، لكن التحديات الاجتماعية والثقافية تبقى عائقاً.	- التمييز الاجتماعي والثقافي ضد المرأة. - ارتفاع معدلات العنف القائم على النوع الاجتماعي.
الهدف 6: المياه النظيفة والنظافة الصحية	- مشاريع لتحسين إدارة المياه. - بناء محطات معالجة المياه.	العراق يعمل على تحسين إدارة المياه، لكن التحديات البيئية والمالية تعيق التقدم.	- نقص الاستثمار في البنية التحتية للمياه. - تأثير التغير المناخي على موارد المياه.
الهدف 7: طاقة نظيفة وبأسعار معقولة	- زيادة استخدام الطاقة المتجددة (مشاريع الطاقة الشمسية). - تحسين كفاءة الطاقة.	العراق يسعى لتحسين استخدام الطاقة النظيفة، لكنه بحاجة إلى استثمارات أكبر في هذا القطاع.	- الاعتماد الكبير على النفط كمصدر رئيسي للطاقة. - نقص الاستثمار في الطاقة المتجددة.
الهدف 8: العمل اللائق ونمو الاقتصاد	- تحسين بيئة الأعمال. - دعم المشاريع الصغيرة والمتوسطة.	العراق يعمل على تحسين الاقتصاد، لكن التحديات الأمنية والسياسية تعيق النمو.	- ارتفاع معدلات البطالة. - ضعف الاستثمار الأجنبي.
الهدف 9: الصناعة والابتكار والهياكل الأساسية	- إعادة بناء البنية التحتية المتضررة. - مشاريع لتحسين النقل والاتصالات.	العراق يعمل على تحسين البنية التحتية، لكنه بحاجة إلى استثمارات أكبر في الابتكار.	- نقص الاستثمار في الابتكار والتكنولوجيا. - ضعف البنية التحتية.
الهدف 10: الحد من أوجه عدم المساواة	- برامج لدعم الفئات الضعيفة. - تحسين الخدمات الاجتماعية.	العراق يعمل على تقليل الفوارق، لكن التحديات الاقتصادية والاجتماعية تبقى عائقاً.	- ارتفاع معدلات الفقر والبطالة. - التمييز الاجتماعي.
الهدف 11: مدن ومجتمعات محلية مستدامة	- إعادة إعمار المدن المتضررة. - تحسين خدمات النقل العام.	العراق يعمل على تحسين المدن، لكن التحديات البيئية والاقتصادية تعيق التقدم.	- نقص التخطيط الحضري. - ارتفاع معدلات التلوث.
الهدف 12: الاستهلاك والإنتاج المسؤولان	- تشجيع إعادة التدوير. - تحسين إدارة النفايات.	العراق يعمل على تحسين الاستهلاك والإنتاج، لكنه بحاجة إلى مزيد من الوعي والاستثمار.	- نقص الوعي البيئي. - ضعف إدارة النفايات.
الهدف 13: العمل المناخي	- المشاركة في الاتفاقيات الدولية للمناخ. - مشاريع للتكيف مع التغير المناخي.	العراق يعمل على التكيف مع التغير المناخي، لكن التحديات البيئية والمالية تبقى عائقاً.	- نقص الاستثمار في مشاريع المناخ. - تأثير التغير المناخي على الموارد المائية.
الهدف 14: الحياة تحت الماء	- تحسين إدارة الموارد المائية. - مشاريع لحماية الأنهار والبحيرات.	العراق يعمل على حماية الموارد المائية، لكن التحديات البيئية تعيق التقدم.	- تلوث المياه. - نقص الوعي البيئي.
الهدف 15: الحياة في البر	- مشاريع لاستعادة الأراضي المتدهورة. - حماية التنوع البيولوجي.	العراق يعمل على تحسين إدارة الأراضي، لكن التحديات البيئية تبقى عائقاً.	- التصحر. - نقص الاستثمار في حماية البيئة.
الهدف 16: السلام والعدل والمؤسسات القوية	- إصلاحات في القضاء. - تعزيز سيادة القانون.	العراق يعمل على تعزيز العدل والسلام، لكن التحديات السياسية والأمنية تعيق التقدم.	- الفساد. - ضعف المؤسسات الحكومية.
الهدف 17: عقد الشراكات لتحقيق الأهداف	- تعزيز التعاون الدولي. - المشاركة في المبادرات الإقليمية.	العراق يعمل على تعزيز الشراكات، لكن التحديات المالية والسياسية تبقى عائقاً.	- ضعف التنسيق بين الجهات الحكومية. - نقص التمويل.

وتجدر الاشارة الى ان مصادر المعلومات المذكورة في الجدول (3) متعددة وفقا لطبيعة الهدف العالمي ومن بين هذه المصادر هي الطوعية الوطنية الاول والثاني للمتحقق من اهداف التنمية المستدامة (التقرير الطوعي الاول) والتي أصدرتها اللجنة الوطنية للتنمية المستدامة التابعة لوزارة التخطيط العراقية للاعوام 2019، و 2021 . يضاف اليها البيانات الصادرة من مؤسسات الامم المتحدة (مثل: البنك الدولي، ومنظمة الأغذية والزراعة (FAO)، ومنظمة الصحة العالمية (WHO)،وبرنامج الأمم المتحدة الإنمائي (UNDP)، ومنظمة اليونسكو، والوكالة الدولية للطاقة المتجددة (IRENA)، وصندوق النقد الدولي (IMF)، وبرنامج الأمم المتحدة للمستوطنات البشرية

(UN-Habitat)، وإتفاقية الأمم المتحدة الإطارية بشأن تغير المناخ (UNFCCC)، والإتحاد الدولي لحفظ الطبيعة (IUCN)، ومؤشر الشفافية العالمي (Transparency International).

المطلب الرابع : النجاحات المتحققة ذات الصلة بالامن السيبراني واهداف التنمية المستدامة

ينظر الى الأمن السيبراني بكونه مجموعة من الوسائل التقنية والتنظيمات الإدارية والتشريعات القانونية من شأنها الحد من خطر الهجوم على البرامجيات وأجهزة الحاسوب والشبكات، وتشتمل كذلك على الأدوات المستخدمة في مواجهة القرصنة الإلكترونية ، وكشف الفيروسات وتوفير الاتصالات المشفرة. ويعتبر تعزيز الوعي من المبادئ الاساسية للأمن السيبراني، إذ يتوجب على جميع الجهات المعنية في القطاعات المختلفة فهم المخاطر التي تهدد أمنها، ومدى تأثير تلك المخاطر عليها وعلى الآخرين في النظام البيئي المختص بالبنى التحتية لشبكة الانترنت واستخداماتها، كما وينبغي على جميع الجهات المعنية تحمل مسؤوليَّة مواجهة المخاطر الأمنية التي تهدد أمنها.

ومن بين النجاحات التي يمكن الاشارة اليها في مجالات تحسين واقع الامن السيبراني والتنمية المستدامة ضمن مجالات متعددة في العراق، مايلي:

الفرع الاول: اهم النجاحات للارتقاء بواقع الامن السيبراني في العراق على المستوى الوطني

- اعتماد (ستراتيجية الأمن السيبراني) ، والتي اشار اليها البحث مسبقا، والتي اعدتها مستشارية الأمن الوطني العراقي، لغرض توفير التدابير المتماسكة والإجراءات الستراتيجية لضمان أمن وحماية الوجود العراقي في الفضاء السيبراني، وحماية البنية التحتية الحيوية للمعلومات، وبناء ورعاية مجتمع انترنت موثوق فيه، وتحديد مفاهيم التهديدات السيبرانية ، والإرهاب الإلكتروني، والصراع السيبراني، والتجسس السيبراني. وشددت الستراتيجية 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.

- اعتماد خريطة طريق تفصيلية وضعتها الستراتيجية الوطنية، تهدف ضمان الجاهزية لحوادث الأمن السيبراني،[5] الى جانب التعاون الدولي. وقد جرى الإعلان عن تشكيل فريق وطني مشترك مختص للاستجابة للحوادث السيبرانية وحماية البنية التحتية للانترنت ونشر الوعي في مجال حماية الخصوصية والحماية الذاتية للأفراد والمؤسسات على الانترنت يعمل تحت إشراف مستشارية الأمن الوطني العراقي.

- تحديد مسؤليات الفريق الوطني للاستجابة للحوادث السيبرانية وفقا للستراتجية الوطنية، والتي تشتمل على طيف واسع من المهام ومن بينها، تأمين وحماية الشبكات ومراكز البيانات الوطنية والمواقع الرسمية التي تعمل في مجال الفضاء السيبراني العراقي ،وتنسيق الجهود الوطنية ودعم المؤسسات في القطاعين العام والخاص في حماية نفسها وخدماتها في الفضاء السيبراني، وتحقيق الرصانة والموثوقية للأنظمة الالكترونية، وتعزيز ثقة المواطن بالمؤسسات والارتقاء بمستوى العراق دولياً في مجال الامن السيبراني لتشجيع تطوير الخدمات الالكترونية ودعم مشروع أتمتة الخدمات والحكومة الالكترونية. اضافة الى تشجيع التعاون بين القطاعين العام والخاص وتبادل المعلومات، وزيادة الثقة في استخدام الخدمات الإلكترونية الحكومية، وتعزيز الوعي الأمني لمستخدمي انظمة تكنولوجيا المعلومات والإنترنت، وتحليل التهديدات الأمنية وتأثيرها وتوفير معلومات عن آخر الحوادث وطرق تجنبها، وبناء مركز معتمد لتسلم البلاغات عن الحوادث السيبرانية، وتشجيع البحث والتطوير في مجال الأمن السيبراني، والتعاون المشترك مع فرق الاستجابة والمنظمات على الصعيدين الإقليمي والدولي.

الفرع الثاني: اهم النجاحات للارتقاء بواقع الامن السيبراني في العراق على مستوى المؤسسات الامنية

- أما في وزارة الداخلية فقد تم قطع أشواطاً متقدمة في مجال إرساء قواعد الأمن السيبراني في العراق وانشاء مركز متخصص هو مركز الامن السيبراني. ولهذا المركز وللوزارة بشكل عام نجاحات متميزة فيما يتعلق بمحوري الجريمة الإلكترونية، والإرهاب الإلكتروني، وتمكنت الوزارة من توفير عناصر متدربة على المهارات الرقمية المتقدمة لمواجهة تلك الجرائم، في مديرياتها بجميع المدن العراقية، ووفرت متطلبات الإبلاغ السريع عن تلك الجرائم، فضلاً عن قيامها بحملات توعية الشرائح العراقية المختلفة بمخاطرها، ووسائل تجنبها من قبل الأفراد العاديين، عن طريق الحملات الإعلامية والإلكترونية والندوات الحواريَّة والتثقيفيَّة.

- اطلق جهاز الأمن الوطني، أول منصة للأمن السيبراني في العراق.تهدف لمحاربة كافة الظواهر التي تهدد الأمن المجتمعي والأمن الوطني. هذا اضافة الى واجبات الجهاز الجوهرية المتمثلة بإستخدام الوسائل الاستخبارية والأمنية بطرق علمية وفنية ومنهجية واضحة للمحافظة على الدولة من التهديدات التي ترمي إلى النيل من كيان الدولة و أمن المجتمع واستقراره وتنمية مصالحه الأساسية الأخرى، بالتعاون مع أجهزة الدولة المعنية الأخرى.

الفرع الثالث: اهم النجاحات للارتقاء بواقع الامن السيبراني والتنمية المستدامة في العراق على مستوى المؤسسات التعليمية

يتطلب واقع الأمن السيبراني العراقي، والمخاطر والتهديدات المستمرة التي تعترضه، تشجيع البحث العلمي، عن طريق افتتاح أقسام أو فروعٍ علمية في الجامعات العراقية، الى جانب تحفيز الباحثين لإجراء دراسات الأمن السيبراني، وبحسبٍ ارتباطه بتخصصاتهم العلمية، وتدريب وتنمية المهارات الرقمية بشكل مستمر، لمواكبة المستجدات الإلكترونية، على مستوى المنطقة والعالم.

وبعد ان كانت مناهج الأمن السيبراني تدرَس ضمن البرامج العلمية لكليات علوم الحاسبات وهندستها، بادرت وزارة التعليم العالي والبحث العلمي في العام الدراسي 2022- 2023 باستحداث أقسام الأمن السيبراني في ثلاثة جامعات، هي الجامعة المستنصرية، والجامعة التقنية الشمالية، وجامعة الموصل. ، وهذه هي المرة الأولى التي يتم استحداث أقسام بهذا التخصص في العراق. كما وتم استحداث دراسات عليا (دبلوم عالٍ مهني وماجستير في تقنية الأمن السيبراني في جامعات (بغداد، والتكنولوجية، والموصل) للعام الدراسي 2022-2023، استكمالًا للجهود الكبيرة بالتعاون مع وزارة التعليم العالي وجهاز المخابرات الوطني وعدد من الجهات المختصة. وتلت هذه الخطوة التوسع في استحداث اقسام علمية اخرى لاختصاص الامن السيبراني في العديد من الجامعات الحكومية والاهلية.

وفي جانب اخر، حققت مؤسسات التعليم العلمي العراقية المرتبة الأولى عربيا والسابعة عالميا في تصنيف التايمز للتنمية المستدامة (Times Higher Education Impact Rankings 2024) من حيث عدد الجامعات المشاركة في نسخة العام 2024 التي شهدت تنافس 2152 من 125 دولة حول العالم. واستنادا الى النتائج المتحققة التي أظهرت العراق في ترتيب متميز. ويعتبر هذا النجاح من المؤشرات الدالة على ان مؤسسات التعليم العالي والبحث العلمي العراقية ماضية بكل ثقة في الارتقاء بجودة الأداء الجامعي وتوفير بيئة تعليمية إيجابية تلبي متطلبات المعرفة العلمية والمهارات التقنية التي تقتضيها خدمة المجتمع ومقاييس التعليم الجيد والاعتماد الأكاديمي التي تتظافر معها أهداف التنمية المستدامة للأمم المتحدة.

الخاتمة

في ختام هذا البحث، يمكننا التأكيد على أن تعزيز استراتيجيات الأمن السيبراني ومواءمتها مع أهداف التنمية المستدامة يمثل ركيزة أساسية لضمان مستقبل آمن ومستدام. لقد أظهرت الدراسة أن الأمن السيبراني ليس مجرد

قضية تقنية، بل هو عنصر حيوي يدعم تحقيق العديد من أهداف التنمية المستدامة، بدءًا من حماية البنية التحتية الحيوية ومرورًا بدعم النمو الاقتصادي والابتكار، ووصولًا إلى تعزيز المرونة الرقمية للمدن والمجتمعات المستدامة. من خلال تحليل واقع الأمن السيبراني في العراق وبعض الدول العربية، تبين أن هناك جهودًا كبيرة تُبذل لتعزيز البنية التحتية الرقمية ومواجهة التهديدات السيبرانية. ومع ذلك، لا تزال هناك تحديات كبيرة تتطلب مزيدًا من الاهتمام، مثل نقص الموارد، وضعف الوعي المجتمعي، والحاجة إلى تطوير تشريعات وسياسات متكاملة. كما أظهرت الدراسة أن التعاون الدولي وتبادل الخبرات يلعبان دورًا محوريًا في تعزيز الأمن السيبراني على المستوى الإقليمي والعالمي. لقد أكد البحث على أن الأمن السيبراني يدعم بشكل مباشر أهداف التنمية المستدامة، مثل حماية البيانات الشخصية، وتعزيز النمو الاقتصادي، ودعم الابتكار المستدام، وحماية البيئة من خلال أنظمة إدارة الموارد الذكية. ومع تزايد الاعتماد على التكنولوجيا الرقمية، أصبح من الضروري تعزيز الوعي بأهمية الأمن السيبراني ودمجه في السياسات الوطنية والإقليمية لتحقيق الاستدامة.وفي نهاية هذا البحث مجموعة من التوصيات ومن ابرزها ضرورة تطوير استراتيجيات وطنية للأمن السيبراني تتوافق مع أهداف التنمية المستدامة، وتعزيز الوعي المجتمعي بأهمية الأمن السيبراني، ودعم الشراكة بين القطاعات الخاصة والعامة، وتشجيع الاستثمار في البحث العلمي لتطوير تقنيات أمنية مستدامة. كما نؤكد على أهمية تعزيز التعاون الدولي وتبادل الخبرات لمواجهة التحديات السيبرانية المشتركة، مما يسهم في بناء مستقبل رقمي آمن ومستدام للجميع.

المصادر References

1. Aymerich-Franch, L., & Ferrer, I. (2022). Liaison, safeguard, and well-being: Analyzing the role of social robots during the COVID-19 pandemic. Technology in Society, 70, 101993. https://doi.org/10.1016/j.techsoc.2022.101993
2. Bouteche, B., & Bougdah, H. (2023). Sustainable cities and precarious housing: The case of Algeria. Management of Sustainable Development, 15(2), 28-35. https://doi.org/10.54989/msd-2023-0014
3. Chisty, N. M. A., Baddam, P. R., & Amin, R. (2022). Strategic approaches to safeguarding the digital future: Insights into next-generation cybersecurity. Engineering International, 10(2), 69-84. https://doi.org/10.18034/ei.v10i2.689
4. Denoncourt, J. (2020). Companies and UN 2030 sustainable development goal 9 industry, innovation and infrastructure. Journal of Corporate Law Studies, 20(1), 199-235. https://doi.org/10.1080/14735970.2019.1652027
5. Donalds, C. M., Barclay, C., & Osei-Bryson, K.-M. A. (2022). An integrated framework for developing and implementing a national cybersecurity strategy for Global South countries. In Cybercrime and cybersecurity in the Global South. https://doi.org/10.1201/9781003028710-16
6. Ekmen, O., & Kocaman, S. (2023). From pixels to sustainability: Trends and collaborations in remote sensing for advancing sustainable cities and communities (SDG 11). Sustainability, 15(22), 16094. https://doi.org/10.3390/su152216094
7. Fallah, S. N., Mohabbati-Kalejahi, N., Alavi, S., & Zahed, M. A. (2022). Sustainable development goals (SDGs) as a framework for corporate social responsibility (CSR). Sustainability, 14(3), 1222. https://doi.org/10.3390/su14031222
8. International Telecommunication Union. (2024). Global Cybersecurity Index 2024 (5th ed.). https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx
9. Martz, B. (2025, January 6). Fundraising in 2025: Creative strategies to engage donors in a digital age. Brady Martz. https://www.bradymartz.com/news/fundraising-in-2025-creative-strategies-to-engage-donors-in-a-digital-age/
10. Marx, A., & Wouters, J. (2014). Competition and cooperation in the market of voluntary sustainability standards (SSRN Working Paper No. 2431191). https://ssrn.com/abstract=2431191
11. Melaku, H. M. (2023). A dynamic and adaptive cybersecurity governance framework. Journal of Cybersecurity and Privacy, 3(3), 327-350. https://doi.org/10.3390/jcp3030017
12. Norris, D. F., Mateczun, L., Joshi, A., & Finin, T. (2018). Cybersecurity at the grassroots: American local governments and the challenges of internet security. Journal of Homeland Security and Emergency Management, 15(3), 20170048. https://doi.org/10.1515/JHSEM-2017-0048
13. Obasi, C., Solomon, N., Adenekan, O., & Simpa, P. (2024). Cybersecurity's role in environmental protection and sustainable development: Bridging technology and sustainability goals. Computer Science & IT Research Journal, 5(5), 1145-1177. https://doi.org/10.51594/csitrj.v5i5.1140
14. Odumesi, J. O., & Sanusi, B. S. (2023). Achieving sustainable development goals from a cybersecurity perspective. Proceedings of the Cyber Secure Nigeria Conference (pp. 1-10). https://doi.org/10.22624/aims/csean-smart2023p3

15. Pallardy, C. (2024, June 6). How cybersecurity and sustainability intersect: Cybersecurity and sustainability might have more in common than enterprise leaders think. InformationWeek. https://www.informationweek.com/cyber-resilience/how-cybersecurity-and-sustainability-intersect
16. Shahid, R., & Ahmed, B. (2022). Embedding four indicators of resilience to make cities and communities sustainable in Pakistan. Global Journal for Management and Administrative Sciences, 3(2), 63-73. https://doi.org/10.46568/gjmas.v3i2.131
17. Vasiu, L., & Vasiu, L. (2018). Cybersecurity as an essential sustainable economic development factor. European Journal of Sustainable Development, 7(4), 171-178. https://doi.org/10.14207/ejsd.2018.v7n4p171
18. Zharova, L., & Chechel, A. (2020). Historical aspects of sustainable development and economic evolution interconnection. Skhid, 2(166), 21-28. https://doi.org/10.21847/1728-9343.2020.2(166).201399
19. ما واقع الأمن السيبراني في العراق؟ جريدة الصباح العراقية 8/6/2021 . https://alsabaah.iq/48007-.html
20. 1 الأمم المتحدة تعتمد الأهداف العالمية الجديدة، لتحقيق التنمية المستدامة للبشرية والكوكب بحلول عام 2030 . 2015/9/25. https://www.un.org/sustainabledevelopment/ar/2015/09
21. يماني، ايمان. (2020). هل يحقق الأمن السيبراني أهداف التنمية المستدامة؟ جريدة مكة . 28 مايو 2020. https://makkahnewspaper.com/article/
22. عبدالصادق، عادل. (2022). المرونة السيبرانية والتنمية المستدامة في العصر الرقمي. 2 نوفمبر 2022. المركز العربي لابحاث الفضاء الالكتروني . https://accronline.com/article_detail.aspx?id=37896&srsltid=AfmBOopZEpcIQEgQEgNPoNCTLYIn9Tg0_SZfonddPfP17gn-pi05Spc4
23. خطاب، هبة .(2024). ترتيب الدول في الامن السيبراني 2024 : 3 دول عربية في المقدمة. المشهد. 14 سبتمبر 2024. https://almashhad.com/article/738996299126409-technology/ /
24. 1الدماطي، رامي. (2024). دليل تحليلي عن: المؤشر العالمي للأمن السيبراني 2024 خاص بالدول العربية. ميتا سيرف اكاديمي. 14 سبتمبر 2024. https://www.metaserv.me/academy/resources/guides2/global-cybersecurity-index-2024-middle-east-countries-only/
25. منصور، محمد. (2023). كيف يُمكن الحد من البصمة الكربونية؟. جريدة الشرق، دبي . 2 ديسمبر 2023. https://asharq.com/reports/73329
26. 1المعايير الطوعية للاستدامة: (VSS) مجموعة من المتطلبات الاجتماعية والاقتصادية و/أو البيئية التي يمكن للجهات الفاعلة الأقتصادية الأمتثال لها طواعية حتى تكون ممارساتها في مجال الإنتاج والمعالجة أكثر استدامة. https://unctad.org/system/files/official-document/ditctab2022d8_ar.pdf .
27. السيد ، محمد محسن، نحو تحقيق أهداف التنمية المستدامة في العراق. وزارة التخطيط العراقية https://www.unescwa.org/sites/default/files/inline-files/afsd2019-plenary1-presentation-mohamad-elsayyed-iraq-ar.pdf
28. التقرير الطوعي الاول والثاني للمتحقق من اهداف التنميةالمستدامة
29. https://www.arabdevelopmentportal.com/ar/publication/first-national-voluntary-review-sustainable-development-goals-iraq