



دور الآليات السيبرانية في ضمان الأمن الوطني وتعزيز التنمية المستدامة: العراق نموذجا

دور الآليات السيبرانية في ضمان الأمن الوطني وتعزيز التنمية المستدامة: العراق نموذجا

م.م. زينب حسان خلف

جامعة بغداد، كلية الطب، شعبة الاعلام والاتصال الحكومي.

البريد الإلكتروني Email : zainab.h@comed.uobaghdad.edu.iq

الكلمات المفتاحية: (الأمن السيبراني، الأمن الوطني، التنمية المستدامة، الآليات السيبرانية، العراق)

كيفية اقتباس البحث

خلف، زينب حسان ، دور الآليات السيبرانية في ضمان الأمن الوطني وتعزيز التنمية المستدامة: العراق نموذجا، مجلة مركز بابل للدراسات الانسانية، تشرين الأول ٢٠٢٦، المجلد: ١٦، العدد: ١٠.

هذا البحث من نوع الوصول المفتوح مرخص بموجب رخصة المشاع الإبداعي لحقوق التأليف والنشر (Creative Commons Attribution) تتيح فقط للآخرين تحميل البحث ومشاركته مع الآخرين بشرط نسب العمل الأصلي للمؤلف، ودون القيام بأي تعديل أو استخدامه لأغراض تجارية.

مسجلة في
ROAD

مفهرسة في
IASJ

Journal Of Babylon Center For Humanities Studies 2026 Volume :16 Issue : 10
(ISSN): 2227-2895 (Print) (E-ISSN):2313-0059 (Online)

The Role of Cyber Mechanisms in Ensuring National Security and Promoting Sustainable Development: Iraq as a Case Study

Asst. Lect. Zainab Hassan Khalaf

University of Baghdad, College of Medicine, Media and Government
Communication Division.

Keywords : Cybersecurity, National Security, Sustainable Development, Cyber Mechanisms, Iraq.

How To Cite This Article

Khalaf, Zainab Hassan, The Role of Cyber Mechanisms in Ensuring National Security and Promoting Sustainable Development: Iraq as a Case Study, Journal Of Babylon Center For Humanities Studies, October 2026, Volume:16, Issue 10.



This is an open access article under the CC BY-NC-ND license
(<http://creativecommons.org/licenses/by-nc-nd/4.0/>)

[This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.](#)

•Abstract:

The methods of IT-enabled organizational transformation have created an emerging reality in which cyber threats have become among the most significant obstacles confronting nations, rendering cybersecurity an essential element of national security. The role of the nation is not confined to protecting its territorial borders but has grown to include safeguarding its information infrastructure and virtual environment.

From this perspective, cyber mechanisms become indispensable frameworks for managing digital risks via system fortification, data security, and ensuring the flow of services, consequently improving governmental stability and its ability to regulate resources effectively. This is directly connected to the trajectory of cyber resilience, as the supply of a secure digital environment results in enhancing public



services, driving digital transformation, and fostering trust in government bodies.

The situation in Iraq reveals obvious difficulties in this field, including a deficient regulatory framework, Inadequate digital infrastructure, and scarcity of specialized knowledge that influences government authority to maximize the use of cyber mechanisms. This enables the evolution of this field a vital component for promoting sustainability and reinforcing national security.

● الملخص:

فرضت التحولات الرقمية واقعاً جديداً أصبحت فيه التهديدات السيبرانية من أبرز التحديات التي تواجه الدول، الأمر الذي جعل من الأمن السيبراني جزءاً لا يتجزأ من منظومة الأمن الوطني، ولم يعد دور الدولة مقتصرًا على حماية حدودها التقليدية، بل امتد ليشمل حماية فضاءها الرقمي وبناءها التحتية المعلوماتية.

في هذا السياق، تبرز الآليات السيبرانية كأدوات أساسية في مواجهة المخاطر الرقمية، من خلال تأمين الأنظمة، وحماية البيانات، وضمان استمرارية الخدمات، بما يعزز من استقرار الدولة وقدرتها على إدارة مواردها بكفاءة، كما يرتبط ذلك بشكل مباشر بمسار التنمية المستدامة، إذ إن توفير بيئة رقمية آمنة يسهم في دعم الاقتصاد الرقمي، وتحسين الخدمات العامة، وتعزيز الثقة بالمؤسسات.

ويكشف الواقع العراقي عن تحديات واضحة في هذا المجال، تتمثل في محدودية البنية التحتية الرقمية، وضعف الإطار التشريعي، ونقص الكفاءات المتخصصة، مما ينعكس على قدرة الدولة في توظيف الآليات السيبرانية بشكل فاعل، وهو ما يجعل من تطوير هذا القطاع ضرورة أساسية لتعزيز الأمن الوطني ودعم التنمية المستدامة.

● المقدمة:

شهد العالم خلال العقود الأخيرة ثورة رقمية متسارعة غيرت من طبيعة العلاقات الدولية، وأنماط التفاعل الاقتصادي والاجتماعي، وأعادت تشكيل مفاهيم القوة والأمن، وفي خضم هذا التحول، برز الفضاء السيبراني كمجال حيوي جديد تتداخل فيه المصالح، وتتقاطع فيه التحديات، الأمر الذي دفع الدول إلى إعادة النظر في استراتيجياتها الأمنية بما يتلاءم مع طبيعة البيئة الرقمية.

دور الآليات السيبرانية في ضمان الأمن الوطني وتعزيز التنمية المستدامة: العراق نموذجا

ولم يعد الأمن في هذا السياق مفهوماً تقليدياً قائماً على الحماية المادية فحسب، بل أصبح يرتبط بقدرة الدولة على تأمين منظوماتها الرقمية، وحماية تدفق المعلومات، وضمان سلامة البنى التحتية الحيوية من التهديدات الإلكترونية المتنامية، ومن هنا، أخذ الأمن السيبراني مكانة متقدمة ضمن أولويات السياسات العامة، باعتباره أحد المرتكزات الأساسية لاستقرار الدول واستمرارية مؤسساتها.

وتتطلب مواجهة هذه التحديات تبني مقاربات شاملة تقوم على التكامل بين التطور التكنولوجي والإطار المؤسسي والتشريعي، بما يسمح ببناء منظومة قادرة على الاستجابة للمخاطر المتغيرة والتكيف معها، كما أن تعزيز القدرات في هذا المجال لا ينعكس على الجانب الأمني فقط، بل يمتد ليشمل دعم مسارات التنمية، من خلال تمكين الاقتصاد الرقمي، ورفع كفاءة الخدمات، وتعزيز ثقة الأفراد والمؤسسات في البيئة الرقمية.

وفي ضوء ذلك، تبرز أهمية دراسة واقع الأمن السيبراني في الدول النامية، ومنها العراق، للوقوف على التحديات البنيوية التي تواجه هذا القطاع، واستكشاف السبل الكفيلة بتعزيز جاهزيته، بما يسهم في تحقيق توازن فعال بين متطلبات الأمن الوطني وأهداف التنمية المستدامة.

● أهمية البحث:

تتبع أهمية البحث من تناوله موضوع الأمن السيبراني بوصفه أحد المرتكزات الأساسية للأمن الوطني في ظل التحول الرقمي المتسارع، إذ لم تعد حماية الدولة تقتصر على حدودها التقليدية، بل امتدت إلى حماية فضاءها السيبراني وبناءها التحتية الرقمية وخدماتها الإلكترونية.

كما تبرز أهمية البحث في بيان دور الآليات السيبرانية القانونية والمؤسسية والتقنية والبشرية في الحد من المخاطر الرقمية، وتعزيز قدرة الدولة على الوقاية والاستجابة والتعافي، وتزداد هذه الأهمية في الحالة العراقية، لما يواجهه العراق من تحديات تشريعية ومؤسسية وتقنية، مما يجعل تطوير منظومة سيبرانية فاعلة ضرورة لحماية الأمن الوطني ودعم التنمية المستدامة.

● إشكالية البحث:

تتمثل إشكالية البحث في أن التحول الرقمي المتسارع جعل الفضاء السيبراني مجالاً مؤثراً في الأمن الوطني والتنمية المستدامة، إلا أن قدرة الدول، ولا سيما العراق، على توظيف الآليات السيبرانية بفاعلية ما تزال تواجه تحديات قانونية ومؤسسية وتقنية وبشرية، ومن هنا يطرح البحث



إشكالية رئيسة مفادها: إلى أي مدى تسهم الآليات السيبرانية في تعزيز الأمن الوطني ودعم التنمية المستدامة في العراق في ظل التحديات القائمة؟

● فرضية البحث:

ينطلق البحث من فرضية مفادها أن توظيف الآليات السيبرانية بصورة متكاملة، قانونياً ومؤسسياً وتقنياً وبشرياً، يسهم في تعزيز الأمن الوطني العراقي، ويدعم مسارات التنمية المستدامة، إلا أن فاعلية هذه الآليات تبقى مرتبطة بمدى قدرة الدولة على معالجة التحديات التشريعية والمؤسسية والتقنية وبناء القدرات الوطنية.

● منهجية البحث:

اعتمد البحث على المنهج الوصفي التحليلي، من خلال وصف المفاهيم المرتبطة بالأمن السيبراني والأمن الوطني والتنمية المستدامة، وتحليل دور الآليات السيبرانية القانونية والمؤسسية والتقنية والبشرية في تعزيز الأمن الوطني، كما اعتمد البحث على منهج دراسة الحالة من خلال تناول العراق أنموذجاً، وتحليل واقع الأمن السيبراني فيه بالاستناد إلى الاستراتيجيات الوطنية، والتقارير والمؤشرات ذات الصلة، للوقوف على أبرز التحديات والفرص المتاحة في هذا المجال.

● هيكلية البحث:

سيتم تناول هذا البحث عبر عدد من الموضوعات الرئيسة، إلى جانب المقدمة والخاتمة والتوصيات، وذلك على النحو الآتي:

أولاً: الإطار المفاهيمي والتحول الاستراتيجي للأمن في العصر السيبراني.

ثانياً: الآليات السيبرانية ودورها في تعزيز الأمن الوطني.

ثالثاً: الآليات السيبرانية والتنمية المستدامة في العراق: الواقع والتحديات.

أولاً: الإطار المفاهيمي والتحول الاستراتيجي للأمن في العصر السيبراني

يُعرّف الأمن السيبراني وفقاً للمعهد الوطني للمعايير والتكنولوجيا (NIST) بأنه عملية حماية المعلومات من خلال منع الهجمات الإلكترونية، والكشف عنها، والاستجابة لها، وهو ما يعكس الطبيعة الوقائية والاستباقية لهذا المجال في مواجهة التهديدات الرقمية (المعهد الوطني للمعايير والتكنولوجيا [NIST]، ٢٠٢٤)، كما يعرفه (Edward Amoroso) الباحث والمتخصص في الأمن السيبراني، بأنه: "تقليل مخاطر الهجمات التي تستهدف الحواسيب أو

الشبكات أو البرمجيات" (Amoroso, 2017)، ويُعرّف الأمن السيبراني وفقاً لمعيار ISO/IEC ٢٧٠٣٢ بأنه: "الحفاظ على سرية المعلومات وسلامتها وتوافرها في الفضاء السيبراني" (المنظمة الدولية للتقييس [ISO]، ٢٠١٢).

يُفهم الأمن السيبراني، وفقاً للمركز الوطني للأمن السيبراني العراقي، بوصفه منظومة تهدف إلى حماية الفضاء السيبراني الوطني من خلال تطوير القدرات الأمنية وتعزيز الوعي وتقديم الخدمات المتخصصة، بما يضمن استمرارية الأعمال وحماية البيانات الحساسة (المركز الوطني للأمن السيبراني العراقي، بدون تاريخ).

يقوم الأمن السيبراني على مجموعة من المفاهيم الأساسية المرتبطة بأمن المعلومات، وفي مقدمتها مبادئ السرية والسلامة والتوافر، إلى جانب آليات الحماية مثل التوثيق والتخويل، فضلاً عن استخدام تقنيات التشفير وأنظمة الحماية كالجدران النارية، والتي تسهم مجتمعة في تعزيز أمن الأنظمة والشبكات (Graham et al., 2011, pp. 1-5).

الجدران النارية (Firewalls) هي أنظمة أو أدوات أمنية، برمجية أو مادية، تُستخدم لمراقبة وتنظيم حركة البيانات الواردة والصادرة بين الشبكات، وذلك من خلال تطبيق مجموعة من القواعد والسياسات الأمنية التي تهدف إلى منع الوصول غير المصرح به وحماية الأنظمة من التهديدات والهجمات السيبرانية (Graham et al., 2011, p. 25).

تعد التهديدات السيبرانية من أبرز أشكال التهديدات الأمنية الحديثة، وذلك لارتباطها الوثيق بنظم المعلومات وشبكات الاتصال، إذ جاءت كنتيجة مباشرة للتطور التكنولوجي المتسارع الذي شهدته تكنولوجيا الإعلام والاتصال بمختلف أشكالها وأنواعها، وقد أصبحت هذه التهديدات تشكل خطراً متزايداً على أمن المعلومات وسلامتها، سواء على المستوى الفردي أو على مستوى المؤسسات والنظم السياسية والدول وتأتي هذه التهديدات بأشكال مختلفة أبرزها (الفتلاوي، ٢٠١٦، ص ٦١٤):

١- الحرمان من الخدمة * (Denial of Service).

٢- التجسس السيبراني (Cyber Espionage).

٣- الإرهاب السيبراني (Cyber Terrorism).

٤- الاستيلاء على المعلومات والبيانات العسكرية.

٥- تزيف المعلومات وإتلافها أو تدميرها إلكترونياً.



الحرمان من الخدمة (Denial of Service): تُعد هجمات الحرمان من الخدمة الموزعة (DDoS) من أبرز التهديدات السيبرانية التي تستهدف تعطيل الأنظمة والخدمات الإلكترونية من خلال إغراقها بطلبات تفوق قدرتها التشغيلية، وغالباً ما تُنفذ عبر شبكات الروبوتات (Botnets)، مما يؤدي إلى استنزاف الموارد وتعطيل الخدمات الإلكترونية (Alomari, 2012, p. 24).
أسهّم التطور التكنولوجي وفضاء المعلومات في إحداث تحول في الجغرافيا السياسية ومفهوم الأمن التقليدي، إذ لم تعد الحدود الجغرافية وحدها تمثل مجال السيادة والحماية، بل امتد ذلك إلى الفضاء المعلوماتي والرقمي، مما جعل أمن المعلومات جزءاً أساسياً من الأمن القومي للدول (المشهدي، ٢٠١٩، ص ٢٤٤).

وبالتالي أدى ذلك إلى إحداث تحول استراتيجي في مفهوم الأمن، حيث لم يعد الأمن بمفهومه التقليدي مقتصرًا على حماية الحدود الجغرافية للدولة أو مواجهة التهديدات العسكرية التقليدية، بل امتد ليشمل حماية الفضاء السيبراني والأنظمة المعلوماتية وشبكات الاتصال، وقد ارتبط هذا التحول بظهور خصائص جديدة للبيئة الأمنية المعاصرة، من أبرزها بروز فواعل من غير الدول، كالجماعات المنظمة والناشطين والجهات العابرة للحدود، التي استطاعت توظيف الفضاء الإلكتروني في تنفيذ الهجمات والتأثير في الأمن والاستقرار، الأمر الذي أدى إلى تراجع احتكار الدولة التقليدي لعناصر القوة والردع، كما أن طبيعة الفضاء السيبراني تختلف عن الفضاء التقليدي، فهو فضاء غير ملموس وعابر للحدود، يعتمد على البنى التحتية الرقمية وشبكات المعلومات، مما أدى إلى تغير المفاهيم التقليدية المرتبطة بالسيادة والحدود الجغرافية، وظهر ما يعرف بحدود المعلومات بوصفها جزءاً من الأمن القومي للدول، وفي هذا السياق، شهد مفهوم الردع أيضاً تحولاً واضحاً، إذ أصبحت التهديدات السيبرانية تتسم بعدم الوضوح وصعوبة تحديد مصدر الهجوم، فضلاً عن خاصية إخفاء الهوية، مما جعل أدوات الردع التقليدية أقل فاعلية في مواجهة التهديدات الإلكترونية الحديثة. (سمير، بدون سنة، ص ص. ١٩٢-١٩٤).

ونتيجة لذلك، لم يعد الأمن في العصر الرقمي قائماً فقط على العوامل العسكرية والجغرافية التقليدية، بل أصبح يعتمد بصورة متزايدة على حماية المعلومات والأنظمة الرقمية وتعزيز القدرات السيبرانية لمواجهة التهديدات المستجدة، يتضح مما سبق أن التحول الرقمي والتطور المتسارع للفضاء السيبراني قد أسهما في إعادة تشكيل مفهوم الأمن بصورة جذرية، حيث انتقل من إطاره التقليدي المرتبط بالحدود المادية والقوة العسكرية إلى مفهوم أكثر اتساعاً يركز على حماية المعلومات والأنظمة الرقمية ومواجهة التهديدات السيبرانية المتنامية، الأمر الذي جعل الأمن السيبراني أحد المرتكزات الأساسية للأمن في العصر الحديث.

ثانياً: الآليات السيبرانية ودورها في تعزيز الأمن الوطني

يُعد الأمن الوطني من المفاهيم التي يصعب حصرها في تعريف واحد، نظراً لتأثره بالمتغيرات الداخلية والخارجية التي تواجه الدولة على المستويات السياسية والاقتصادية والاجتماعية والتكنولوجية، ومن هذا المنطلق، تحرص الدول على وضع التشريعات والسياسات الكفيلة بحماية أمنها واستقرارها وصون مصالحها الوطنية في مواجهة مختلف التهديدات، ومع التطور المتسارع في تكنولوجيا المعلومات والاتصالات، برزت تحديات جديدة فرضت نفسها على مفهوم الأمن الوطني، إذ أصبحت وسائل التواصل الاجتماعي والفضاء الرقمي قادرة على التأثير في الرأي العام وتوجيه الحراك المجتمعي، الأمر الذي زاد من أهمية حماية البيئة الرقمية من المخاطر السيبرانية، لذلك لم يعد الأمن السيبراني مجاًلاً منفصلاً عن الأمن الوطني، بل أصبح أحد مرتكزاته الأساسية، مما يستدعي تبني استراتيجيات مرنة وقادرة على مواكبة التطورات التقنية والتهديدات المتجددة في الفضاء السيبراني. (سلمان، ٢٠٢١، ص ١٦١)

يحدد إطار عمل الأمن السيبراني الصادر عن المعهد الوطني للمعايير والتكنولوجيا، في إصداره الثاني، مجموعة من الوظائف الرئيسية لإدارة مخاطر الأمن السيبراني، يمكن النظر إليها بوصفها آليات سيبرانية متكاملة، تتمثل في: الحوكمة، والتحديد، والحماية، والكشف، والاستجابة، والتعافي، وتسهم هذه الوظائف في بناء إطار عملي يساعد المؤسسات على فهم مخاطرها السيبرانية، وتقييمها، وترتيب أولوياتها، والتواصل بشأنها، فضلاً عن تعزيز قدرتها على حماية أصولها الرقمية، واكتشاف الحوادث السيبرانية، والاستجابة لها، واستعادة العمليات والخدمات المتأثرة بها. (المعهد الوطني للمعايير والتكنولوجيا [NIST]، ٢٠٢٤، ص ٣، ١٥)

وتأسيساً على ما تقدم، فإن أهمية هذه الوظائف لا تقتصر على كونها تصنيفاً فنياً لإدارة المخاطر السيبرانية، بل تتجلى في قدرتها على التحول إلى آليات وطنية عملية تعتمد عليها الدولة لحماية أمنها ومصالحها الحيوية في البيئة الرقمية، فالآليات السيبرانية، بهذا المعنى، لا تنحصر في الوسائل التقنية وحدها، وإنما تمتد لتشمل الجوانب القانونية والتنظيمية والمؤسسية والأمنية والتوعوية والتعاونية، بما يجعلها جزءاً من منظومة الأمن الوطني الحديثة، وفي الإطار العراقي، تبرز استراتيجية الأمن السيبراني العراقي بوصفها نموذجاً وطنياً لتوظيف هذه الآليات، إذ تنطلق من إدراك أن الفضاء السيبراني أصبح مجاًلاً مؤثراً في الأمن القومي والاقتصاد والخدمات الحكومية والبنى التحتية الحيوية. (مستشارية الأمن الوطني، بدون تاريخ، ص ٢، ٦-٧)



ومن ثم، فإن مواجهة المخاطر السيبرانية لا تتحقق عبر إجراء منفرد، بل من خلال منظومة متكاملة تشمل الحكومة الفعالة، والإطار التشريعي والتنظيمي، وإطار تكنولوجيا الأمن السيبراني، وثقافة الأمن السيبراني وبناء القدرات، والبحث والتطوير، والامتنال والتنفيذ، والجاهزية لحوادث الأمن السيبراني، فضلاً عن التعاون الدولي، وبذلك تتحول الآليات السيبرانية من مجرد أدوات تقنية إلى منظومة وطنية شاملة تستهدف تقليل المخاطر، وتعزيز قدرة الدولة على الوقاية والاستجابة والتعافي، وحماية الأمن الوطني في مواجهة التهديدات الرقمية المتجددة. (مستشارية الأمن الوطني، بدون تاريخ، ص ص. ٨-٩)

وتتجسد الآليات السيبرانية في مجموعة من المسارات العملية التي تعتمد عليها الدولة لتنظيم الفضاء السيبراني، وتقليل المخاطر الناشئة عنه، وحماية المصالح الوطنية في البيئة الرقمية، ويمكن بيان أبرز هذه الآليات على النحو الآتي:

أولاً: الآليات القانونية والتنظيمية

تُعد الآليات القانونية والتنظيمية من المرتكزات الأساسية التي اعتمدتها استراتيجية الأمن السيبراني العراقي، إذ لا تقتصر مواجهة التهديدات السيبرانية على الجانب التقني فحسب، وإنما تتطلب وجود إطار قانوني ومؤسسي قادر على تنظيم الفضاء السيبراني، وتحديد المسؤوليات، وتنسيق الجهود بين الجهات ذات العلاقة.

فمن الناحية القانونية، أشارت الاستراتيجية إلى أن القوانين النافذة لا تستجيب بصورة كافية لطبيعة الجرائم الإلكترونية الحديثة، إذ إن معالجة هذه الجرائم ما تزال تستند إلى أحكام قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩، في حين أن التطور التقني فرض صوراً جديدة من الجرائم يصعب التعامل معها بالوسائل القانونية التقليدية، كما بينت الاستراتيجية أن التعامل مع الدليل الإلكتروني يثير إشكالات عملية، ولا سيما عند تأخر الإبلاغ أو فقدان فاعلية الدليل مع مرور الوقت، الأمر الذي يستدعي تعزيز الوعي بأهمية الدليل الإلكتروني وآليات الحصول عليه في وقت مبكر، وانطلاقاً من ذلك، أكدت الاستراتيجية ضرورة تحديث التشريعات القائمة، وتشريع قوانين سيبرانية جديدة تعالج الجرائم الرقمية، وتحمي البنى التحتية الحرجة، مع مواعاة القوانين الوطنية مع المعايير والاتفاقيات الدولية ذات الصلة. (المركز الوطني للأمن السيبراني، ٢٠٢٢، ص ص. ١٤، ١٩-٢٠)



أما من الناحية التنظيمية، فقد ركزت الاستراتيجية على ضرورة وجود إدارة مركزية عليا تُعنى بتطبيق الاستراتيجية ومتابعة تنفيذها وتذليل الصعوبات التي تعترضها، مع توفير الموارد المالية والكوادر البشرية اللازمة، وتوزيع المسؤوليات والواجبات بما يحقق أولويات التنفيذ. كما تضمنت مرحلة التنظيم والتخطيط عدداً من الإجراءات، منها دراسة واقع حال الأمن السيبراني وتقييم مستوى الجاهزية، وتحليل نتائج الدراسة، وإعداد الهيكل التنظيمي والحوكمة الفعالة، وإعداد وثيقة الهيكل التنفيذي، فضلاً عن إعداد وتحديث السياسات والتعليمات. (المركز الوطني للأمن السيبراني، ٢٠٢٢، ص ص. ١٨-١٩)

وبذلك، فإن الآليات القانونية والتنظيمية لا تمثل إجراءات إدارية منفصلة، بل تشكلان معاً الإطار الحاكم للأمن السيبراني الوطني، فالقانون يحدد القواعد والالتزامات والعقوبات، بينما يضمن التنظيم المؤسسي تحويل هذه القواعد إلى سياسات وإجراءات قابلة للتنفيذ، ومن دون هذا التكامل، تبقى الاستراتيجيات السيبرانية أقرب إلى التوجهات النظرية، ولا تتحول إلى أدوات عملية قادرة على حماية الأمن الوطني في البيئة الرقمية.

ثانياً: الآليات الأساسية والمهمة

اتجه العراق إلى تبني عدد من الآليات المؤسسية والحكومية لمواجهة التهديدات السيبرانية وتعزيز حماية الفضاء السيبراني الوطني، وقد مثلت الاستراتيجية الوطنية للأمن السيبراني العراقي لعام ٢٠١٧ خطوة أساسية في هذا المجال، إذ ركزت على إيجاد بيئة تشريعية وتنظيمية قادرة على مواجهة الجرائم الإلكترونية، وحماية البنى التحتية الحيوية للمعلومات، وتقليل الثغرات التي قد تستغلها الهجمات السيبرانية، كما أكدت الاستراتيجية أهمية بناء قدرات وطنية للاستجابة للحوادث السيبرانية، من خلال تطوير فرق متخصصة للرصد والمعالجة، وإقرار سياسات ومعايير لأمن المعلومات تساهم في تحديد الأدوار والمسؤوليات داخل المؤسسات وتوحيد إجراءات حماية البيانات والأنظمة الرقمية. (محمد، ٢٠٢٦، ص. ٣٠٩)

وعلى المستوى المؤسسي، برز تشكيل الفريق الوطني للاستجابة للتهديدات السيبرانية بوصفه آلية مهمة لحماية الشبكات ومراكز البيانات والمواقع الرسمية، فضلاً عن دوره في نشر الوعي السيبراني، كما تعزز هذا المسار بتأسيس مركز الأمن السيبراني في ٤ كانون الأول/ديسمبر



٢٠٢٢، لدعم جهود وزارة الداخلية في بناء منظومة متكاملة لحماية الفضاء السيبراني العراقي ورفع مستوى الجاهزية في مواجهة الهجمات الإلكترونية. (مهدي، ٢٠٢٥، ص. ٣٩٢)

ثالثاً: الآليات التقنية والأمنية

وفي الجانب التقني والأمني، تتجه الآليات السيبرانية إلى توظيف الأدوات الفنية المتقدمة في رصد التهديدات وتحليلها، وحماية الشبكات والأنظمة، وتقييم الثغرات، ومنع تسرب البيانات، وتحليل الأدلة الرقمية، وقد أشار حلف شمال الأطلسي إلى تدريب عدد من موظفي فريق الاستجابة العراقي على جوانب عملية في الدفاع السيبراني، شملت تحليل الشفرات، ومنع تسرب البيانات، والجنائيات الرقمية المتقدمة، وتقييم الثغرات، بما يسهم في تعزيز الخبرة الفنية والقدرات الدفاعية الوطنية. (حلف شمال الأطلسي [NATO]، ٢٠١٦)

كما تؤكد استراتيجية الأمن السيبراني العراقي أهمية بناء إطار تكنولوجي وطني، وتعزيز الجاهزية للحوادث السيبرانية من خلال آليات الإبلاغ والتنبيه واستمرارية الأعمال، وهو ما يعكس انتقال الآليات التقنية من مستوى الحماية الوقائية إلى مستوى الرصد والاستجابة والتعافي. (مستشارية الأمن الوطني، بدون تاريخ، ص ص. ٨-٩)

رابعاً: آليات بناء القدرات والجاهزية والاستجابة للحوادث السيبرانية

تُعد آليات بناء القدرات والجاهزية والاستجابة للحوادث السيبرانية من الركائز الأساسية لتعزيز الأمن السيبراني الوطني، إذ إن مواجهة التهديدات الرقمية لا تتحقق بالاعتماد على الأدوات التقنية وحدها، وإنما تتطلب إعداد كوادر بشرية مؤهلة، وبناء ثقافة سيبرانية واعية، وتطوير منظومة قادرة على الرصد المبكر والتعامل السريع مع الحوادث، وتتمثل هذه الآليات في نشر ثقافة الأمن السيبراني داخل المؤسسات والمجتمع، وتنظيم برامج التوعية والتثقيف، وتأهيل العاملين في مجال أمن المعلومات، وتحديد الحد الأدنى من المؤهلات المطلوبة للكوادر المتخصصة، فضلاً عن دعم التعليم الأكاديمي والتخصصي في مجالات الأمن السيبراني والجنائيات الرقمية، كما يسهم التدريب العملي والتقني في رفع كفاءة الكوادر الوطنية، ولا سيما فرق الاستجابة للحوادث السيبرانية، بما يعزز قدرتها على حماية البيانات، وتحليل التهديدات، وفحص الثغرات، والتعامل مع الأدلة الرقمية. (الحدراوي وكاظم، ٢٠٢٣، ص ص. ٦١٤-٦١٦)

دور الآليات السيبرانية في ضمان الأمن الوطني وتعزيز التنمية المستدامة: العراق نموذجا

وفي الإطار العراقي الرسمي، أكدت استراتيجية الأمن السيبراني العراقي أهمية بناء وتطوير ثقافة الأمن السيبراني الوطني، وتنسيق برامج التوعية والتثقيف، ونشر المعلومات المتعلقة بالأمن السيبراني على المستوى الوطني، فضلاً عن تحديد المتطلبات والمؤهلات اللازمة للعاملين في مجال أمن المعلومات، كما ربطت الاستراتيجية ذلك بجانب الجاهزية للحوادث السيبرانية، من خلال تعزيز فريق الاستجابة للحوادث، ووضع آليات فعالة للإبلاغ، ونشر التنبيهات والتحذيرات بشأن الثغرات ونقاط الضعف، وتشجيع الجهات المعنية على تنفيذ برامج دورية لفحص احتمالية التعرض للهجمات، إلى جانب وضع إطار لإدارة استمرارية الأعمال. (مستشارية الأمن الوطني، بدون تاريخ، ص. ٩)

خامساً: آليات التعاون الدولي

تتمثل آليات التعاون الدولي في مجال الأمن السيبراني العراقي في تعزيز مشاركة العراق في الهيئات والمنظمات والمنتديات الدولية ذات الصلة، وبناء شراكات بين فريق الاستجابة الإلكتروني العراقي وفريق الاستجابة الدولية، فضلاً عن التواصل مع الاتحاد الدولي للاتصالات والاستفادة من برامج التدريب والتقييم الدولي (مستشارية الأمن الوطني، بدون تاريخ، ص. ٩-١٠)، وقد تجسد ذلك في التعاون مع حلف شمال الأطلسي لتدريب خبراء عراقيين في الدفاع السيبراني، وكذلك في مراجعة نضج القدرات السيبرانية العراقية التي نفذها المركز العالمي لبناء القدرات السيبرانية في جامعة أوكسفورد بالتعاون مع الجهات العراقية وبمشاركة الناتو، وتدل هذه الآليات على أن الأمن السيبراني لم يعد شأناً داخلياً صرفاً، بل أصبح مجالاً يتطلب تبادل الخبرات والمعلومات والتنسيق عبر الحدود لمواجهة التهديدات السيبرانية المتجددة. (Global Cyber Security Capacity Centre, University of Oxford, 2022)

وخلاصة ما تقدم، يتضح أن الآليات السيبرانية تمثل ركيزة أساسية لتعزيز الأمن الوطني، إذ تجمع بين البعد القانوني والمؤسسي والتقني وبناء القدرات والتعاون الدولي. ويكشف الواقع العراقي أن امتلاك بعض المقومات لا يكفي ما لم تُنظَّم ضمن إطار وطني موحد قادر على الوقاية والاستجابة والتعافي من التهديدات السيبرانية، ويوضح الجدول الآتي قراءة تحليلية لواقع الأمن السيبراني في العراق وفقاً لمؤشر NCSI:

جدول رقم (١): تحليل واقع الأمن السيبراني في العراق وفقاً لمؤشر NCSI

نقاط القوة (S)	نقاط الضعف (W)
١. التعليم والتطوير المهني العالي (٨٠٪): يتوافق مع سعي العراق لبناء القدرات عبر توفير برامج أكاديمية متخصصة في الجامعات. ٢. البحث العلمي والتقني (٥٠٪): وجود حركة جيدة للاستقصاء العلمي والأبحاث السيبرانية. ٣. التمثيل المهني: نشاط مؤسسي تخصصي يثبت وجود الكوادر البشرية المؤهلة.	١. غياب القيادة المركزية الفاعلة (٢٠٪): رغم وجود فرق استجابة، يعاني العراق من غياب هيئة حكومية عليا مستقلة لقيادة الفضاء السيبراني. ٢. غياب الإلزامية في أمن البنى الحيوية (٥٠٪): نقص المعايير الملزمة للقطاع العام والشركات المشغلة. ٣. قصور في آليات التعاون الدولي والمساهمة في بناء القدرات العالمية.
الفرص (O)	التحديات (T)
١. استثمار المخرجات الأكاديمية: تحويل الكفاءات البشرية الشابة وخريجي الجامعات وفرق الاستجابة إلى طاقات تنفيذية في مؤسسات الدولة. ٢. سد الفراغ التشريعي: البناء على مساعي تشريع قانون جرائم المعلوماتية لإقرار سياسات صارمة لحماية البيانات والأمن الرقمي.	١. استهداف البنى التحتية: تزايد احتمالية شل القطاعات الحساسة نتيجة ضعف سياسات الحماية الملزمة. ٢. انتهاك البيانات: استغلال قرصنة الإنترنت لغياب سلطة حماية البيانات الشخصية. ٣. العزلة وقت الأزمات: غياب الدعم الدولي السريع بسبب القصور في الدبلوماسية السيبرانية.

المصدر: إعداد الباحثة بالاستناد إلى بيانات المؤشر الوطني للأمن السيبراني NCSI الخاصة بالعراق.

ثالثاً: الآليات السيبرانية والتنمية المستدامة في العراق: الواقع والتحديات

تقوم العلاقة بين الأمن السيبراني والتنمية المستدامة على الارتباط الوثيق بين حماية المعلومات وتحقيق أهداف التنمية، إذ إن تزايد الاعتماد على تكنولوجيا المعلومات والتحول الرقمي جعل أمن البيانات والبنى التحتية الرقمية مسألة أساسية لجميع القطاعات، فضعف الحماية المعلوماتية لا يهدد الجانب التقني وحده، بل يمتد أثره إلى الأبعاد الاقتصادية والاجتماعية والبيئية للتنمية المستدامة، ومن ثم، فإن الأمن السيبراني يمثل عاملاً مهماً في دعم التنمية المستدامة من خلال حماية المعلومات والبيانات من الهجمات السيبرانية، وتأمين البنية التحتية الرقمية، وضمان



استمرارية الخدمات الإلكترونية بما يعزز الاستقرار والنمو. (Sebkhaoui, 2024, pp. 620-621)

وتُفهم التنمية المستدامة، وفقاً لوثيقة الأمم المتحدة الخاصة بخطة عام ٢٠٣٠، بوصفها خطة عمل عالمية تستهدف الإنسان والكوكب والازدهار، وتسعى إلى تعزيز السلام والشراكة بين الدول، من خلال معالجة التحديات الاقتصادية والاجتماعية والبيئية بصورة مترابطة ومتكاملة، وبذلك لا تقتصر التنمية المستدامة على تحقيق النمو الاقتصادي فحسب، بل تمتد إلى القضاء على الفقر، وحماية البيئة، وتحسين نوعية الحياة، وضمان مستقبل أكثر استقراراً وعدلاً للأجيال الحالية والقادمة. (الأمم المتحدة، الجمعية العامة، ٢٠١٥)

وتظهر آثار الآليات السيبرانية في التنمية المستدامة من خلال تقليص الفجوة الرقمية، وحماية حقوق الأفراد والمؤسسات من الانتهاكات الإلكترونية، وتعزيز الثقة في الخدمات والمعاملات الرقمية، كما تسهم هذه الآليات في دعم الحوكمة الرقمية، وحماية الخصوصية، وتطوير التشريعات والسياسات التي تضمن المشاركة العادلة في الفضاء الرقمي، وبذلك، يمثل الأمن السيبراني ركيزة داعمة للتنمية المستدامة الشاملة، لأنه يربط بين الحماية التقنية والعدالة الاجتماعية والاقتصادية في البيئة الرقمية. (عبد الصاحب، ٢٠٢٦، ص ص. ١٤٠-١٤٧)

تواجه العراق جملة من التحديات في مجال الأمن السيبراني، تتداخل فيها الأبعاد القانونية والمؤسسية والتقنية والبشرية، فعلى مستوى الجاهزية العامة، تكشف المؤشرات الدولية أن مستوى الاستعداد السيبراني ما زال بحاجة إلى تطوير، ولا سيما فيما يتعلق بوضوح السياسات، وتكامل الأطر التنظيمية، وحماية البنى التحتية الرقمية، وإدارة الحوادث السيبرانية، ويشير ذلك إلى أن امتلاك بعض المبادرات أو المؤسسات المتخصصة لا يكفي ما لم يُترجم إلى منظومة وطنية متكاملة قادرة على الوقاية والاستجابة والتعافي. (المؤشر الوطني للأمن السيبراني NCSI، ٢٠٢٦)

وعلى المستوى المؤسسي، يبرز تحدي تحويل الاستراتيجيات الوطنية للأمن السيبراني في العراق من إطار تخطيطي عام إلى برامج تنفيذية واضحة، إذ أن استراتيجية الأمن السيبراني العراقية لعام ٢٠١٧ مثّلت جهداً مهماً في تشخيص أوجه القصور في السياسة السيبرانية الوطنية، كما تضمنت أجندة تنفيذية تقوم على أهداف زمنية تمتد لسنة وثلاث وخمس سنوات، شملت إنشاء وكالة اتحادية للأمن السيبراني، وصياغة قوانين تتعلق بالفضاء السيبراني، وبناء ثقافة وطنية



للأمن السيبراني، فضلاً عن التوجه نحو التعليم الجامعي المتخصص في هذا المجال، ويكشف ذلك أن التحدي الأساسي لا يكمن في غياب التصور الاستراتيجي فحسب، بل في مدى القدرة على ترجمة هذه التصورات إلى مؤسسات فاعلة، وتشريعات نافذة، وبرامج قابلة للتطبيق والقياس. (Shubbar, 2022) وعلى المستوى القانوني والتنظيمي، يتمثل أحد أبرز تحديات الأمن السيبراني في العراق في ضعف القوانين والتشريعات الحكومية الخاصة بالأمن المعلوماتي و السيبراني، فضلاً عن عدم وجود قانون ينظم الأمن الوطني السيبراني بصورة متكاملة، ويزداد هذا التحدي وضوحاً مع تعثر تشريع قانون الجرائم الإلكترونية، على الرغم من طرحه منذ عام ٢٠١١، الأمر الذي يحد من قدرة الدولة على مواكبة تطور الجرائم السيبرانية، ولا سيما مع تنوع هذه الجرائم بين الاحتيال عبر الإنترنت، وغسل الأموال، والقرصنة، والتطفل على الشبكات، والهجمات الإلكترونية التي تستهدف المؤسسات الحكومية. (صالح، ٢٠٢٣، ص ص. ٢٣٠، ٢٤٠)

أما تقنياً وبشرياً، فيواجه العراق تحديات تتعلق بضعف البنى التحتية، وضعف الأمن الإلكتروني، والحاجة إلى بناء منظومة متكاملة لأمن المعلومات قادرة على حماية الشبكات والأجهزة والبرامج والبيانات من الهجمات أو الضرر أو الوصول غير المصرح به، كما يبرز التحدي البشري في افتقار العراق إلى المعلومات والمختصين في مجال الأمن السيبراني مقارنة بالدول الأخرى، الأمر الذي يجعل بناء فرق متخصصة وبرامج تدريب مستمرة ضرورة أساسية لتعزيز القدرة على الاستجابة والتعافي، ولا يقتصر الأمن السيبراني على الوسائل التقنية وحدها، بل يتطلب تكامل المستخدمين والعمليات والتكنولوجيا، فضلاً عن تعزيز التعاون الوطني والدولي وتبادل المعلومات والخبرات لحماية البنى التحتية المعلوماتية الحرجة ومواجهة التهديدات المتغيرة. (الزبيدي والتيمي، ٢٠٢٢)

وبذلك يمكن القول إن التحدي السيبراني في العراق لا يتمثل في جانب واحد، بل في بناء منظومة وطنية متكاملة تجمع بين التشريع، والمؤسسة، والتقنية، والوعي، وبناء القدرات، ومن دون هذا التكامل، تبقى جهود الأمن السيبراني محدودة الأثر في حماية الأمن الوطني ودعم التنمية المستدامة.

•الخاتمة:

خلص البحث إلى أن التحولات الرقمية المتسارعة قد أعادت تشكيل مفهوم الأمن بصورة جوهرية، إذ لم يعد الأمن مقتصرًا على حماية الحدود الجغرافية أو مواجهة التهديدات التقليدية، بل أصبح مرتبطاً بقدرة الدولة على حماية فضاءها السيبراني وبنائها التحتية المعلوماتية وأنظمتها الرقمية، وفي هذا السياق، برز الأمن السيبراني بوصفه أحد المرتكزات الأساسية للأمن الوطني، نظراً لما تمثله التهديدات السيبرانية من مخاطر قادرة على التأثير في استقرار الدولة، وسلامة مؤسساتها، واستمرارية خدماتها الحيوية.

وقد بين البحث أن الآليات السيبرانية لا تنحصر في الجانب التقني وحده، وإنما تمثل منظومة متكاملة تشمل الأبعاد القانونية والتنظيمية، والمؤسسية والحكومية، والتقنية والأمنية، وبناء القدرات والجاهزية والاستجابة للحوادث، فضلاً عن التعاون الدولي. وتكمن أهمية هذه الآليات في أنها تنقل الأمن السيبراني من كونه إجراءً وقائياً محدوداً إلى إطار وطني شامل يسهم في تقليل المخاطر، وحماية البيانات، وضمان استمرارية الخدمات، وتعزيز قدرة الدولة على الوقاية والاستجابة والتعافي من التهديدات الرقمية.

كما توصل البحث إلى أن العلاقة بين الآليات السيبرانية والتنمية المستدامة علاقة وثيقة ومباشرة، إذ إن نجاح التحول الرقمي، وتطوير الحكومة الإلكترونية، وتحسين الخدمات العامة، ودعم الاقتصاد الرقمي، كلها أهداف لا يمكن تحقيقها بصورة مستدامة من دون بيئة رقمية آمنة وموثوقة، فالأمن السيبراني لا يدعم الجانب الأمني فحسب، بل يسهم كذلك في تعزيز الثقة بالمؤسسات، وحماية حقوق الأفراد، وتأمين البيانات، ورفع كفاءة الأداء المؤسسي، الأمر الذي يجعله عاملاً مساعداً في تحقيق أبعاد التنمية المستدامة الاقتصادية والاجتماعية والمؤسسية.

وفي الحالة العراقية، أظهر البحث أن العراق يمتلك خطوات أولية مهمة في مجال الأمن السيبراني، تمثلت في تبني استراتيجية وطنية، وتشكيل فرق للاستجابة، وتأسيس مؤسسات مختصة، والانفتاح على مسارات التعاون الدولي، فضلاً عن وجود اهتمام بالتعليم والتطوير المهني والبحث العلمي في هذا المجال، غير أن هذه الجهود ما تزال بحاجة إلى مزيد من التكامل والتفعيل، إذ تكشف المعطيات عن تحديات واضحة تتعلق بضعف الإطار التشريعي المتخصص، ومحدودية التنسيق المؤسسي، والحاجة إلى قيادة مركزية أكثر فاعلية، فضلاً عن تحديات البنية التحتية الرقمية، ونقص الكوادر المتخصصة، وضعف الوعي السيبراني.



وعليه، فإن بناء منظومة سيبرانية وطنية فاعلة في العراق لا يمثل خياراً تقنياً أو إدارياً فحسب، بل يشكل ضرورة استراتيجية لحماية الأمن الوطني ودعم التنمية المستدامة، فكلما استطاعت الدولة تطوير آلياتها السيبرانية وربطها بخطط التنمية والتحول الرقمي، ازدادت قدرتها على حماية مواردها ومؤسساتها وخدماتها الحيوية، وتعزيز ثقة المواطن بالفضاء الرقمي، وتحويل الأمن السيبراني من مجال دفاعي محدود إلى ركيزة أساسية من ركائز بناء الدولة الحديثة والتنمية المستدامة.

●التوصيات:

١. يوصي البحث بضرورة الانتقال من التعامل مع الأمن السيبراني بوصفه ملفاً تقنياً محدوداً إلى اعتماده كسياسة وطنية عابرة للقطاعات، ترتبط بالأمن الوطني، والتنمية المستدامة، والتحول الرقمي، والحكومة الإلكترونية، وحماية البنى التحتية الحيوية.
٢. الإسراع في إعداد تشريع سيبراني متكامل لا يقتصر على تجريم الأفعال الإلكترونية، بل يشمل حماية البيانات الشخصية، وأمن البنى التحتية الحرجة، وتنظيم الإبلاغ عن الحوادث، وتحديد التزامات المؤسسات العامة والخاصة في مجال أمن المعلومات.
٣. إدماج الأمن السيبراني في خطط التنمية الوطنية والتحول الرقمي، بحيث يصبح شرطاً سابقاً لتنفيذ مشاريع الأتمتة والحكومة الإلكترونية والمنصات الخدمية، وليس إجراءً لاحقاً لمعالجة المشكلات بعد ظهورها.
٤. ربط المناهج الجامعية والتدريب المهني بحاجات الدولة الفعلية في الأمن السيبراني، من خلال استحداث مسارات تطبيقية في الجنائيات الرقمية، تحليل البرمجيات الخبيثة، حماية الشبكات، أمن البيانات، وإدارة الأزمات السيبرانية.
٥. تعزيز الشراكة بين القطاعين العام والخاص في مجال الأمن السيبراني، ولا سيما أن جزءاً مهماً من البنى التحتية والخدمات الرقمية يرتبط بالمصارف، وشركات الاتصالات، ومزودي الخدمات التقنية، الأمر الذي يستدعي بناء مسؤولية مشتركة في الحماية والاستجابة.
٦. تطوير ثقافة سيبرانية مجتمعية مستدامة، لا تقتصر على حملات توعية مؤقتة، بل تشمل برامج مستمرة تستهدف الموظفين، والطلبة، والمواطنين، ومستخدمي الخدمات الرقمية، مع التركيز على مخاطر الاحتيال الإلكتروني، وحماية الخصوصية، والاستخدام الآمن للمنصات الرقمية.
٧. تطوير التعليم والتدريب المتخصص في الأمن السيبراني والجنائيات الرقمية، وربط المخرجات الجامعية بحاجات مؤسسات الدولة والقطاع الخاص.



دور الآليات السيبرانية في ضمان الأمن الوطني وتعزيز التنمية المستدامة: العراق نموذجا

٨. تفعيل الدبلوماسية السيبرانية العراقية من خلال توسيع التعاون مع المنظمات الدولية وفتح الاستجابة العالمية، والمشاركة في التمارين السيبرانية الإقليمية، وتبادل المعلومات حول التهديدات العابرة للحدود، بما يعزز موقع العراق في بيئة الأمن السيبراني الدولية.

المصادر:

- ١- المعهد الوطني للمعايير والتكنولوجيا (NIST). (2024). إطار الأمن السيبراني (NIST Cybersecurity Framework (CSF) 2.0). <https://www.nist.gov/cyberframework>.
- 2-Amoroso, E. (2017). An introduction to cybersecurity (1st ed.). Independently Published.
- ٣- المنظمة الدولية للقياس (ISO). (2012). ISO/IEC 27032:2012 Information technology. Security techniques. Guidelines for cybersecurity. <https://www.iso.org/standard/44375.html>
- ٤- المركز الوطني للأمن السيبراني العراقي. (بدون تاريخ). الصفحة الرسمية للمركز الوطني للأمن السيبراني العراقي. <https://ncc.gov.iq/>
- 5-Graham, J., Howard, R., & Olson, R. (Eds.). (2011). Cyber security essentials. Auerbach Publications.
- ٦- الفتلاوي، أحمد عبيس نعمة. (٢٠١٦). الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر. مجلة المحقق الحلي للعلوم القانونية والسياسية، (٤)، ٦١٤.
- 7-Alomari, E. (2012). Botnet-based distributed denial of service (DDoS) attacks on web servers: Classification and art. International Journal of Computer Applications, 49(7).
- ٨- المشهدي، تغريد معين حسن. (٢٠١٩). الأثر العسكري للأمن السيبراني في الجغرافيا السياسية للدولة. مجلة البحوث الجغرافية، (٣٠)، ١، ص ٢٤٤.
- ٩- سمير، باي. (بدون سنة). التهديدات الأمنية السيبرانية: دراسة في انعكاسات الحرب الإلكترونية على الأمن القومي للدول واستراتيجيات المقاومة. مجلة الرسالة للدراسات والبحوث الإنسانية، (٢)، ص ١٩٢-١٩٤.
- ١٠- سلمان، مصطفى إبراهيم. (٢٠٢١). الأمن السيبراني وأثره في الأمن الوطني العراقي. مجلة العلوم القانونية والسياسية، (١)، ص ١٦١.
- ١١- المعهد الوطني للمعايير والتكنولوجيا (NIST). (٢٠٢٤). إطار عمل الأمن السيبراني: الإصدار الثاني. <https://www.nist.gov/cyberframework>
- ١٢- مستشارية الأمن الوطني، أمانة سر اللجنة الفنية العليا لأمن الاتصالات والمعلومات. (بدون تاريخ). استراتيجية الأمن السيبراني العراقي- https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/00056_06_iraqi-cybersecurity-strategy.pdf



دور الآليات السيبرانية في ضمان الأمن الوطني وتعزيز التنمية المستدامة: العراق نموذجا

- ١٣-المركز الوطني للأمن السيبراني. (٢٠٢٢). (استراتيجية الأمن السيبراني العراقي ٢٠٢٢-٢٠٢٧. <https://ncc.gov.iq/files/%D8%A7%D9%84%D8%A7%D8%B3%D8%AA%D8%B1%D8%A7%D8%AA%D9%8A%D8%AC%D9%8A%D8%A9.pdf>
- ١٤-محمد، حريز عصام. (٢٠٢٦). العراق وتحديات الأمن السيبراني. مجلة آشور للعلوم القانونية والسياسية، ٣٩٢، (٢)، ص ٣٠٩.
- ١٥-مهدي، سيماء علي. (٢٠٢٥). دور الأمن السيبراني في استقرار الدولة. المجلة السياسية الدولية، (٦٤)، ص ٣٩٢.
- ١٦-حلف شمال الأطلسي (NATO). (٢٠١٦). ٩ ديسمبر. (تدريب خبراء عراقيين في الدفاع السيبراني. https://www.nato.int/cps/en/natohq/news_139179.htm
- ١٧-الحدراوي، رافد حميد، وكاظم، حسن جواد. (٢٠٢٣). بناء الاستراتيجية الوطنية للأمن السيبراني بالتركيز على التخطيط الاستراتيجي. مجلة مركز دراسات الكوفة، عدد خاص، ٦١٤-٦١٦.
- ١٨-مستشارية الأمن الوطني. (بدون تاريخ). استراتيجية الأمن السيبراني العراقي. الاتحاد الدولي للاتصالات. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/00056_06_iraqi-cybersecurity-strategy.pdf
- 19-Global Cyber Security Capacity Centre, University of Oxford. (2022). CMM review Iraq 2022. Cybil Portal. <https://cybilportal.org/projects/cmm-review-iraq/>
- ٢٠-المؤشر الوطني للأمن السيبراني NCSI، (٢٠٢٦)، صفحة العراق، متاح على الموقع الرسمي للمؤشر، تاريخ الزيارة: ٢٧ / ٦ / ٢٠٢٦. <https://www.ncsi.ega.ee/country/iq/%D8%8C>
- 21-Sebkhaoui, K. (2024). The role of cyber security in attaining the sustainable development goals. Development and Human Resources Management Review: Researches and Studies, 11(1), 620-621.
- ٢٢- الأمم المتحدة، الجمعية العامة. (٢٠١٥، ٢٥ سبتمبر). (تحويل عالما: خطة التنمية المستدامة لعام ٢٠٣٠ القرار <https://sdgs.un.org/2030agenda> A/RES/70/1).
- ٢٣-عبد الصاحب، تبارك كمال. (٢٠٢٦). الأمن السيبراني وأثره على التنمية المستدامة من جانب تحقيق العدالة والمساواة. المجلة العراقية للعلوم الاقتصادية، (٨٨)، ٢٤، ١٤٠-١٤٧.
- 24-Shubbar, H. (2022, March 19). Constructing an interinstitutional and interministerial effort on cyber security in Iraq. Al-Bayan Center for Planning and Studies. <https://www.bayancenter.org/en/2022/03/3215/>
- ٢٥-صالح، شيماء تركان. (٢٠٢٣). الأمن الوطني العراقي والتحديات السيبرانية: الإرهاب السيبراني أنموذجاً. مجلة تكريت للعلوم السياسية، ٤ (٣٣)، ٢٣٠-٢٤٠.
- ٢٦-الزبيدي، زهير خضير عباس، والتميمي، ظفر عبد مطر. (٢٠٢٢). العراق والأمن السيبراني: الفرص والتحديات. مجلة واسط للعلوم الإنسانية، ١٨ (٢).

•Sources:

- 1--^١National Institute of Standards and Technology (NIST). (2024). NIST Cybersecurity Framework (CSF) 2.0. <https://www.nist.gov/cyberframework>.
- 2--^٢Amoroso, E. (2017). An introduction to cybersecurity (1st ed.). Independently Published.
- 3--^٣International Organization for Standardization (ISO). (2012). ISO/IEC 27032:2012 Information technology. Security techniques. Guidelines for cybersecurity. <https://www.iso.org/standard/44375.html>
- 4--^٤Iraqi National Cybersecurity Center. (n.d.). Official page of the Iraqi National Cybersecurity Center. <https://ncc.gov.iq/>
- 5--^٥Graham, J., Howard, R., & Olson, R. (Eds.). (2011). Cyber security essentials. Auerbach Publications.
- 6--^٦Al-Fatlawi, Ahmed Abees Neama. (2016). Cyberattacks: Their concept and the resulting international liability in light of contemporary international regulation. Al-Muhaqqiq Al-Hilli Journal for Legal and Political Sciences, (4), 614.
- 7--^٧Alomari, E. (2012). Botnet-based distributed denial of service (DDoS) attacks on web servers: Classification and art. International Journal of Computer Applications, 49(7).
- 8--^٨Al-Mashhadani, Taghreed Mueen Hassan. (2019). The military impact of cybersecurity on the state's geopolitics. Journal of Geographical Research, 30(1), p. 244.
- 9--^٩Samir, Bay. (n.d.). Cybersecurity threats: A study on the repercussions of cyber warfare on national security and resistance strategies. Al-Risala Journal for Humanities Studies and Research, 8(2), pp. 192-194.
- 10-Salman, Mustafa Ibrahim. (2021). Cybersecurity and its impact on Iraqi national security. Journal of Legal and Political Sciences, 10(1), p. 161.
- 11-National Institute of Standards and Technology (NIST). (2024). Cybersecurity Framework: Version 2.0. <https://www.nist.gov/cyberframework>



12-National Security Advisory, Secretariat of the Higher Technical Committee for Communications and Information Security. (n.d.). Iraqi Cybersecurity Strategy. [https://www.itu.int/en/ITU-](https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/00056_06_iraqi-cybersecurity-strategy.pdf)

[D/Cybersecurity/Documents/National_Strategies_Repository/00056_06_iraqi-cybersecurity-strategy.pdf](https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/00056_06_iraqi-cybersecurity-strategy.pdf)

13-National Cybersecurity Center. (2022). Iraqi Cybersecurity Strategy 2022-2027. <https://ncc.gov.iq/files/%D8%A7%D9%84%D8%A7%D8%B3%D8%AA%D8%B1%D8%A7%D8%AA%D9%8A%D8%AC%D9%8A%D8%A9.pdf>

14-Mohammed, Hareer Issam. (2026). Iraq and cybersecurity challenges. Ashur Journal for Legal and Political Sciences, 3(2), p. 309.

15-Mahdi, Simaa Ali. (2025). The role of cybersecurity in state stability. International Political Journal, (64), p. 392.

16-North Atlantic Treaty Organization (NATO). (2016, December 9). Training Iraqi experts in cyber defense. https://www.nato.int/cps/en/natohq/news_139179.htm

17-Al-Hadrawi, Rafid Hamid, & Kadhim, Hassan Jawad. (2023). Building the National Cybersecurity Strategy with a Focus on Strategic Planning. *Journal of Kufa Studies Center*, Special Issue, 614-616.

18-National Security Advisory. (n.d.). Iraqi Cybersecurity Strategy. International Telecommunication Union (ITU). https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/00056_06_iraqi-cybersecurity-strategy.pdf

19-Global Cyber Security Capacity Centre, University of Oxford. (2022). CMM review Iraq 2022. Cybil Portal. <https://cybilportal.org/projects/cmm-review-iraq/>

20--٢٠ National Cyber Security Index (NCSI). (2026). Iraq Page. Available on the official NCSI website. Date of access: June 27, 2026. <https://www.ncsi.ega.ee/country/iq/>

- 21--٢١ Sebkhauui, K. (2024). The role of cyber security in attaining the sustainable development goals. *Development and Human Resources Management Review: Researches and Studies*, 11(1), 620-621.
- 22--٢٢ United Nations General Assembly. (2015, September 25). Transforming our world: the 2030 Agenda for Sustainable Development (Resolution A/RES/70/1). <https://sdgs.un.org/2030agenda>
- 23--٢٣ Abdul-Sahib, Tabarak Kamal. (2026). Cybersecurity and its Impact on Sustainable Development: Achieving Justice and Equality. Iraqi Journal of Economic Sciences, 24(88), 140-147.
- 24--٢٤ Shubbar, H. (2022, March 19). Constructing an interinstitutional and interministerial effort on cyber security in Iraq. Al-Bayan Center for Planning and Studies. <https://www.bayancenter.org/en/2022/03/3215/>
- 25--٢٥ Saleh, Shaimaa Turkan. (2023). Iraqi National Security and Cyber Threats: Cyber-terrorism as a Case Study. Tikrit Journal of Political Science, 4(33), 230-240.
- 26--٢٦ Al-Zubaidi, Zuhair Khudair Abbas, & Al-Tamimi, Zafar Abd Matar. (2022). Iraq and Cybersecurity: Opportunities and Challenges. Wasit Journal of Humanities, 18(2).

