مركز المنبر
للدراسات والتنمية المستدامة
ALMANBAR CENTER FOR STUDIES
AND SUSTAINABLE DEVELOPMENT

موقع العراق في مؤشرات الأمن السيبراني الدولية الواقع وآفاق المستقبل

الدكتور: باسم علي خريسان

عن المركز

مركز المنبر للدراسات والتنمية المستدامة، مركز مستقلٌّ، مقرّه الرئيس في بغداد. رؤيته الرئيسة تقديم وجهة نظر ذات مصداقية حول قضايا السياسات العامة والخارجية التي تخصّ العراق بنحو خاصٍ ومنطقة الشرق الأوسط بنحو عام – فضلاً عن قضايا أخرى – ويسعى المركز إلى إجراء تحليل مستقلّ، وإيجاد حلول عمليّة جليّة لقضايا تهمّ الشأن السياسي، الاقتصادي، الاجتماعي، والثقافي.

لا تعبر الآراء الواردة في المقال بالضرورة عن اتجاهات يتبناها المركز وانما تعبر عن رأي كتابها

https://www.almanbar.org

info@almanbar.org

07816776709

موقع العراق في مؤشرات الأمن السيبراني الدولية الواقع وآفاق المستقبل

الدكتور: باسم علي خريسان

يُمارس الفضاء السيبراني تأثيراً بالغاً في مختلف مجالات الحياة، سيما في المجال الأمني، حيث يعيد تشكيل الأبعاد الأمنية محليّاً وعالميّاً من خلال أدواته المتعددة. كما يُسهم في تحويل الوعي والإدراك السياسي والأمني للأفراد والمجتمعات والدول، ليخلق تصوُّراتٍ وهياكل جديدة تختلف جذريّاً عما كانت عليه سابقاً. فلم يعد مفهوم الأمن مقتصراً على العالم المادي المحدود، بل امتد ليشمل الأبعاد الافتراضية غير المحدودة التي يصنعها الفضاء السيبراني، والتي أصبح لها تأثيرٌ واضح في الحقل الأمني.

في ضوء ذلك، برزت مصطلحات مثل:" الأمن السيبراني"، و"الحرب السيبرانية"، و"الردع السيبراني"، و"الهجوم والدفاع السيبراني"، فضلاً عن ظهور مفاهيم أخرى كـ"الجيوش السيبرانية"، و"الأسلحة السيبرانية"، و"الإرهاب السيبراني"، و"الجريمة السيبرانية"، و"المرتزقة والميليشيات السيبرانية"، وغيرها.

وفي مواجهة هذه التحوُّلات، سارعت الدول إلى إنشاء مؤسسات بحثية وأمنية متخصِّصة لدراسة الفضاء السيبراني وتوظيفه لتحقيق مصالحها السياسية والأمنية والاقتصادية. إذ يكمن التحدي المستقبلي في قدرة الدول على التكيُّف مع التغيُّرات المتسارعة التي يُفرضها هذا الفضاء، خاصةً في المجال الأمني، إلى جانب امتلاك البنى التحتية المادية والبشرية التي تُمكِّنها من لعب دور فاعل ومؤثر فيه. ولا يتوقف تأثير الفضاء السيبراني على النطاق المحلي فحسب، بل يمتد ليشمل المحيط الدولي،

مُعيداً تشكيل مفهوم الأمن الدولي ومحدداً أُطراً جديدةً لطبيعة العلاقات بين الدول. ومن هنا، أصبح " مؤشر الأمن السيبراني " أحد أهم الأدوات لقياس مستوى الأمن السيبراني في دول العالم، مما يعكس الأهمية المتزايدة لهذا المجال في رسم ملامح المستقبل الأمني العالمي.

اولاً: مؤشر الأمن السيبراني:

يُصاغ المؤشر العالمي للأمن السيبراني (GCI) استناداً إلى البيانات المُقدَمة من الدول الأعضاء في الاتحاد الدولي للاتصالات(ITU) ، وهو إحدى وكالات منظمة الأمم المتحدة، إضافةً إلى مساهمات الأفراد المهتمين والخبراء وأصحاب المصلحة في القطاع كشركاء مساهمين. ويستمد المؤشر تفويضه من القرار رقم 130 (المعدل في بوخارست، 2022) الصادر عن مؤتمر المندوبين المفوضين للإتحاد الدولي للإتصالات، والذي يهدف إلى تعزيز دور الإتحاد في بناء الثقة والأمان في استخدام تقنيات المعلومات والاتصالات. ويدعو القرار الدول الأعضاء، على وجه الخصوص، إلى دعم مبادرات الإتحاد في مجال الأمن السيبراني، بما في ذلك المؤشر العالمي للأمن السيبراني(GCI) ، وذلك بهدف تعزيز الاستراتيجيات الحكومية، وتبادل المعلومات حول الجهود المبذولة على مستوى الصناعات والقطاعات المختلفة.

منذ إطلاق أول مؤشر عالمي للأمن السيبراني من قبل الإتحاد الدولي للاتصالات (ITU) في العام 2015 ، انضم 2.5 مليار شخص إلى الإنترنت. شهدت السنوات العشر الماضية تطوراً كبيراً في مشهد الأمن السيبراني، مدفوعاً جزئياً بظهور تقنيات جديدة مثل الذكاء الاصطناعي وسلسلة الكتل (بلوك تشين) وإمكانيات الحوسبة الكمية. ومع ذلك، يبقى عنصر واحد ثابتاً: العنصر البشري.

تُعد جهود الأمن السيبراني والاستخدام المسؤول للتكنولوجيا الرقمية من قِبَل الأفراد أمراً بالغ الأهمية في تشكيل مستقبل هذا المجال والعمل نحو تحقيق اتصال ذي مغزى.

إدراكاً لمحورية الأفراد، اعتمدت الدول الأعضاء في الإتحاد الدولي للاتصالات (ITU) "خطة عمل في العام 2022، وشددت على الحاجة إلى توفير اتصالات/تكنولوجيا معلومات واتصالات شاملة وآمنة لتحقيق التنمية المستدامة من خلال دعم مكوّنات مثل الأمن السيبراني، بالإضافة إلى محو الأمية الرقمية، وتعزيز أمان المستخدمين على الإنترنت، ومساعدة الدول الأعضاء في وضع استراتيجيات وطنية للأمن السيبراني وفرق الإستجابة لحوادث الحاسوب، وتنمية المهارات الرقمية وتدريباتها، وإيجاد بنية تحتية آمنة.

يستند الإصدار الخامس من المؤشر العالمي للأمن السيبراني الصادر في العام 2024إلى هذا الإرث ويبني على الإصدارات السابقة. ويتجلى ذلك في مجالات مثل:

- منهجية أكثر دقة
- مشاركة وتعاون أوسع خلال عملية الإعداد
- توافر وصول أسهل للمدخلات ذات الصلة
- تطوير تصميمات الاستبيانات
- وتعزيز جمع وتحليل البيانات القائمة على الأدلة.

من جهة أخرى يُعد المؤشر بمثابة مقياس مُركّب يرصد إجراءات الأمن السيبراني عبر مجالات العمل الخمسة لـ الأجندة العالمية للأمن السيبراني(GCA) ، حيث يقيس:

- نوع ومستوى ومدى تقدم الأنشطة المتعلقة بالأمن السيبراني داخل الدول وبالمقارنة مع دول أخرى.
- التقدم في التزام الدول بالأمن السيبراني من منظور عالمي.
- التقدم في الأنشطة الأمنية من منظور إقليمي.
- الفجوة الأمنية السيبرانية أي الفرق بين الدول والمناطق من حيث مستوى مشاركتها في المبادرات الأمنية.

تمثل هذه المقاييس مجتمعةً مستوى التزام الدولة بالأمن السيبراني [1].

أهداف المؤشر:

يسعى المؤشر إلى تعزيز ثقافة عالمية للأمن السيبراني، بحيث تُدمج تقنيات المعلومات والاتصالات والأمن في تطويرها واعتمادها. كما يهدف إلى مساعدة الدول في تحديد:

- مجالات القوة النسبية في إدارة الأمن السيبراني ومكافحة الجرائم السيبرانية.
- ومجالات التحسين، وتشجيعها على اتخاذ إجراءات استباقية نحو مزيد من التطوير والابتكار في هذه المجالات.

من المتوقع أن يوفِّر هذا المنظور فرصة لرفع مستوى الالتزام العالمي بالأمن السيبراني، ومواءمة الممارسات الجيدة، وتعزيز الثقافة الأمنية على المستويات الوطنية والإقليمية والعالمية . ولهذه الغاية، يشارك المؤشر رؤى عملية

[1] - Global Cybersecurity Index 2024, International Telecommunication Union Development Sector, ITUPublications,2024, https://www.itu.int/epublications/publication/global-cybersecurity-index-2024 .

يمكن أن تكون بمثابة ممارسات جيدة، ودروس، وإرشادات للدول ذات البيئات الوطنية المُماثلة.

تتميز هذه النسخة من المؤشر العالمي للأمن السيبراني للعام 2024 بمشاركة قياسية من الدول وتُعد الأكثر دقة حتى الآن. تم التحقق من كل تقرير قدّمته الدول بشكل مستقل للتأكد من دقته، وفقاً لمعايير وتعريفات متسقة. ونتيجةً لذلك، يمكن للمستخدمين الوثوق بجودة المؤشر وقابليته للتطبيق.

في الواقع، كان من المُشجّع أن نعلم أن الدول الأعضاء تدمج مقاييس مستوحاة من المؤشر العالمي للأمن السيبراني في خططها وأنشطتها الوطنية.

تُسلِّط نتائج هذه النسخة من المؤشر الضوء على تحسينات كبيرة حققتها الدول، مثل إضافة تشريعات أساسية، وإنشاء جهود للاستجابة للحوادث، ووضع خطط وطنية أكثر وضوحاً، وتدريب الأفراد عبر المجتمع، والتعاون مع الشركاء الوطنيين والدوليين. وعلى وجه الخصوص، كثّفت العديد من الدول جهودها الأمنية نحو الفئات الضعيفة والمهمشة.

ومع ذلك، ورغم أن الزيادة في مبادرات الأمن السيبراني مُشجّعة، فإن الخطوة الحاسمة التالية للدول الأعضاء تكمن في ضمان فعالية هذه الجهود. فمجرد الالتزام بالعمل لا يكفي، بل يجب التأكد من تنفيذ الالتزامات السيبرانية من خلال أنشطة عالية الجودة وذات تأثير كبير.

في المدى المنظور، سيكون توفير الدعم للعديد من الدول لتعزيز الخطوات التي اتخذتها بالفعل عبر المؤشر العالمي للأمن السيبراني، حاجة أكثر إلحاحاً من أي وقت

مضى، كما يظهر في هذه النسخة من المؤشر، نظراً لاستمرار الفجوات بين أقل الدول نمواً (LDCs)، والدول الجزرية الصغيرة النامية(SIDS) ، والدول النامية غير الساحلية (LLDCs)، والدول المتقدمة. بينما تعمل الدول على سد هذه الفجوات في طريقها نحو اتصال ذي مغزى، عليها أن تعمل على الاستفادة من الممارسات الجيدة، ووضع أُطر قانونية واضحة وملائمة وقابلة للتطبيق، وإنشاء فرق تقنية للاستجابة للحوادث، لمعالجة نقص الكفاءات الماهرة، وتعزيز التعاون، خاصةً في القضايا التي تؤثر على الفئات الضعيفة.

علاوةً على ذلك، يبرز التعاون الدولي كعنصر لا غنى عنه في مواجهة الطبيعة العابرة للحدود للتهديدات السيبرانية.

تسعى الجهود التعاونية إلى تبادل أفضل الممارسات والذكاء والموارد، مما يعزز المرونة السيبرانية الجماعية. لكن للاستفادة الكاملة من التعاون الدولي، من الضروري دعم تطوير القدرات اللازمة للمشاركة الفعّالة في الجهود المشتركة. إن بناء وتعزيز القدرات الوطنية للأمن السيبراني يضع الأساس للدول للمساهمة بفاعلية في الجهود العالمية للأمن السيبراني والتصدي لتحديات الفضاء السيبراني بثقة وكفاءة.

لا يمثل المؤشر العالمي للأمن السيبراني سوى جزء من الحل لتعزيز التزامات الدول في هذا المجال. وعلى الدول ان تجد طرقاً لاستخدام المؤشر في جهودها لبناء تكنولوجيا معلومات واتصالات آمنة وموثوقة [2].

[2] - مصدر سابق

ثانياً: ترتيب الدول في المؤشر

تختلف مكانة الدول (194) في المؤشر العالمي للأمن السيبراني تبعاً لمستوى تحقيقها للمتطلبات التي يحددها المؤشر لقياس جاهزيتها وقدراتها في هذا المجال الحيوي. لذلك، تسعى الدول جاهدة إلى تلبية تلك المتطلبات وتوفير المقوّمات اللازمة لتعزيز مواقعها في المؤشر، كما هو موضّح في الجدول التالي:

الدول	الفئة
أستراليا، غانا، المغرب، سنغافورة، البحرين، اليونان، هولندا، سلوفينيا، بنغلاديش، آيسلندا، إسبانيا، بلجيكا، الهند، النرويج، السويد، البرازيل، إندونيسيا، سلطنة عمان، تنزانيا، قبرص، إيطاليا، باكستان، تايلند، الدنمارك، اليابان، البرتغال، تركيا، مصر، الأردن، قطر، الإمارات، إستونيا، كينيا، كوريا، المملكة المتحدة، فنلندا، لوكسمبورغ، رواندا، الولايات المتحدة الامريكية، فرنسا،	95–100 الفئة الأولى _ دول نموذجية

ماليزيا، السعودية، فيتنام، ألمانيا، موريشيوس، صربيا	
ألبانيا، الإكوادور، المكسيك، سويسرا ،النمسا، جورجيا، الفلبين، توغو، أذربيجان، المجر، بولندا، أوروغواي، بنين، إيرلندا، رومانيا، أوزبكستان، كندا، إسرائيل، روسيا، زامبيا، الصين، كازاخستان، سلوفاكيا، كرواتيا، ليتوانيا، جنوب أفريقيا، التشيك، مالطا، سريلانكا	95-85 الفئة الثانية _ دول متقدمة
الجزائر، كوبا، ليبيا، بابوا غينيا الجديدة، أندورا، الكونغو الديمقراطية، مالاوي، باراغواي، بيلاروسيا، الدومينيكان،	

مولدوفا، بيرو، بوتان، إسواتيني، موناكو، السنغال، بوتسوانا، إثيوبيا، منغوليا، سيراليون، بروناي، غامبيا، الجبل الأسود، ترينيداد وتوباغو، بلغاريا، غينيا، موزمبيق، تونس، بوركينا فاسو، إيران، ميانمار، أوغندا، الكاميرون، جامايكا، نيبال، أوكرانيا، تشيلي، كيريباس، نيوزيلندا، فانواتو، كولومبيا، الكويت، نيجيريا، كوستاريكا، قيرغيزستان، مقدونيا الشمالية، ساحل العاج، لاتفيا، بنما	85–55 الفئة الثالثة _ دول في طور التأسيس
أنغولا، دومينيكا، ليختنشتاين، سيشل، الأرجنتين، السلفادور، مدغشقر، الصومال، أرمينيا، غينيا الاستوائية، مالي، جنوب السودان، البهاما، فيجي، موريتانيا، فلسطين، بربادوس، الغابون، ناميبيا، السودان، بليز، غرينادا، ناورو، سورينام، بوليفيا، غواتيمالا، نيكاراغوا،	55–20 الفئة الرابعة _ دول في مرحلة التطور

سـوريا، غيانا، النيجر، طاجيكسـتان، البوسـنة والهرسـك، هايتي، سـانت كيتس ونيفيس، تونغـا، الرأس الأخضـر، هندوراس، سـانت لوسـيا، تركمانسـتان، كمبوديـا، العراق، سـانت فنسـنت والغرينـادين، توفـالو، تشـاد، لاوس، فنزويلا، جزر القمر، لبنـان، سـاموا، زيمبابوي، الكونغو، ليسوتو، سان مارينو، جيبوتي، ليبيريا، ساو تومي وبرينسيبي	
أفغانسـتان، كوريا الشـمالية، المالديف، تيمور الشـرقيـة، أنتيغوا وبربودا، جزر مارشـال، الفاتيكان، بوروندي، إريتريا، ميكرونيزيا، اليمن، إفريقيا الوسطى، غينيا بيساو، جزر سليمان	20-0الفئة الخامسة _ دول في مرحلة البناء

.Global Cybersecurity Index 2024

لقد تحقق الكثير من التحسّن منذ الإصدار السابق 2021من المؤشر العالمي للأمن السيبراني(GCI) ، إلا أن هناك حاجة لبذل المزيد من الجهود لمواكبة مشهد التهديدات الرقمية المتطورة.

تُعتبر الهجمات السيبرانية الآن خامس أكثر المخاطر احتمالاً للتسبب في أزمة ملموسة على المستوى العالمي، كما أظهرت الأعطال الفنية العالمية الأخيرة مدى اعتماد العالم على البنية التحتية الرقمية والحاجة إلى تعزيز المرونة. إذا أرادت الدول أن تستفيد من تقنيات المعلومات والاتصالات، فلا بد لها أن تولي الأمن السيبراني الاهتمام الذي يستحقه.

من خلال ركائز المؤشر العالمي للأمن السيبراني (القانونية، الفنية، التنظيمية، تنمية القدرات، والتعاون)، يتعيّن على الدول أن تُركِّز جهودها على الأنشطة ذات الأثر الكبير بدلاً من الوثائق أو الحملات السطحية. وقد ترغب الدول في النظر في الجهود التالية:

- **تنفيذ إجراءات قانونية** يمكن تطبيقها بوضوح وعدالة عبر جميع القطاعات.
- **تعزيز الجهود المشتركة** التي تتجاوز مجرد معالجة الجانب التكنولوجي.
- **الحفاظ على مؤسسات وطنية ذات تدريب جيد** وقادرة على الاستجابة، بما في ذلك فرق الاستجابة لحوادث الحاسوب.
- **إشراك مجموعة واسعة من أصحاب المصلحة** في جميع مبادرات الأمن السيبراني.
- **وضع وتحديث الاستراتيجية الوطنية للأمن السيبراني** بانتظام، مصحوبةً بخطة عمل قابلة للتنفيذ.
- **تنفيذ إجراءات فعّالة** لحماية الأطفال على الإنترنت.

- **معالجة التحديات الأمنية** التي تواجه البنية التحتية الحرِجة.
- **إطلاق حملات توعية** تتناول القضايا ذات الصلة.
- **توفير فرص التدريب** للمحترفين في الأمن السيبراني، والعاملين في البنية التحتية الحرجة، والشباب لبناء وتعزيز المهارات الأمنية.
- **إنشاء آليات تحفيزية** لتشجيع تنمية القدرات في الأمن السيبراني والبحث والتطوير.
- **تعزيز التعاون المحلي والدولي** في تبادل المعلومات وتنمية القدرات.

من جهة اخرى لا يزال الأمن السيبراني في تطور مستمر. بالنسبة للدول التي تسعى لتحقيق اتصال ذي مغزى وآمن سيبرانياً، يقدم المؤشر العالمي للأمن السيبراني صورة واضحة عن موقعها الحالي وخارطة طريق للتقدم. ومع ذلك، يجب أن تكون الدول مستعدة للانخراط في عمليات مستمرة لتعزيز الأمن السيبراني وتحسين جودة وفعالية أنشطتها. وسيواصل المؤشر رصد جهود الدول وتقدمها بينما تسعى لمواجهة التحديات المستقبلية وتوفير اتصال ذي مغزى للجميع[3].

ثالثاً: موقع العراق في المؤشر

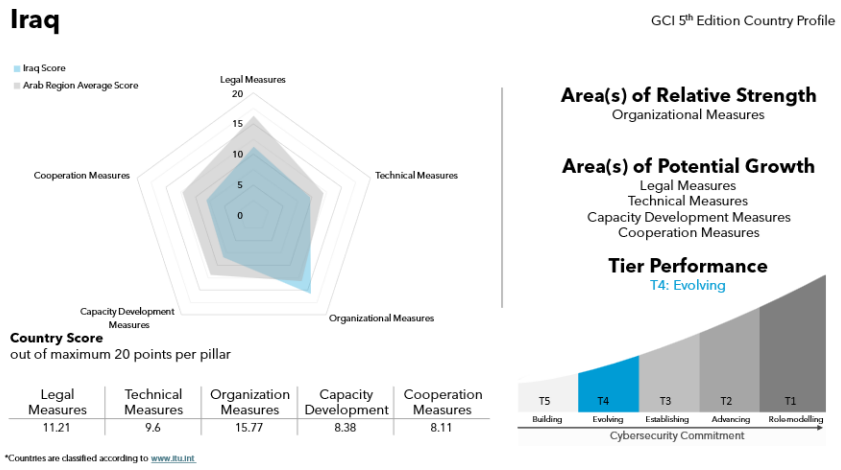
يُعتبر العراق من بين الدول التي تواجه تحديات متزايدة في مجال الفضاء السيبراني، سيما في الجانب الأمني. فمع التحول السريع للمجتمعات من الفضاء الواقعي إلى الفضاء السيبراني، وجد العراق نفسه يدخل هذا الفضاء الواسع وسريع التغيّر دون المرور بمرحلة انتقالية تمكّنه من التكيّف والاستعداد الكافي. وعند النظر إلى **مؤشر الأمن السيبراني العالمي**، الذي يستند إلى خمس ركائز أساسية لقياس مستوى الأمن

[3] مصدر سابق

السيبراني في كل دولة من خلال تحليل 80 مؤشراً فرعياً، نجد أن هذه الركائز تشمل ما يلي[4]:

١. **الركيزة القانونية:** التدابير المتعلقة بوجود الأُطر القانونية والمؤسسات المختصة بالتعامل مع الأمن السيبراني والجرائم السيبرانية.
٢. **الركيزة التقنية:** التدابير القائمة على وجود مؤسسات فنية متخصصة تُعنى بالجوانب التقنية للأمن السيبراني.
٣. **الركيزة التنظيمية:** التدابير المرتبطة بوجود سياسات واستراتيجيات تنسيقية تهدف إلى تطوير الأمن السيبراني على المستوى الوطني.
٤. **بناء القدرات:** التدابير المتعلقة بتوفير برامج البحث والتطوير، والتعليم، والتدريب، والمختصين المعتمدين، والمؤسسات العامة التي تسهم في تعزيز القدرات السيبرانية.
٥. **التعاون:** التدابير التي تُعنى بوجود شراكات، وأُطر تعاونية، وشبكات لتبادل المعلومات على الصعيديّن المحلي والدولي.

[4] مصدر سابق -



رسم يوضح موقع العراق في المؤشر الامن السيبراني للعام 2025

https://www.itu.int/epublications/publication/global-cybersecurity-index-2024

عند البحث عن موقع العراق في مؤشر الأعوام السابقة نجد أن موقع العراق في مؤشر الأمن السيبراني لعام 2018 كان (107) عالمياً و(13) عربياً، لكنه تراجع بمقدار (22) نقطة في مؤشر عام 2020 ليصبح في المرتبة (129) عالمياً من أصل (184) دولة، و(17) عربياً بدرجة بلغت (71.20)، كما هو مُبيَّن في الجدول أدناه لعام 2021.

موقع العراق وفقاً لركائز مؤشر الأمن السيبراني للعام 2021

النتيجة الكلية	الإجراءات القانونية	الإجراءات التقنية	الإجراءات التنظيمية	بناء القدرات	إجراءات التعاون
20,71	0,00	6,56	7,75	2,14	4,6

Global Cybersecurity Index 2020, International Telecommunication Union Development Sector, ITU Publications, 2021, P74.

لكن عند مقارنة موقع العراق في مؤشر عام 2024، نلاحظ أن العراق شهد تقدماً كبيراً نتيجةً لجهوده في تطوير الركائز الخمس الأساسية لبناء الأمن السيبراني. فقد حقق قفزة بمقدار (7) مراكز مقارنةً بالعام 2023، إلى جانب تحسّن في الدرجة بمقدار (+4.2) نقطة، وهو أعلى من المتوسط العالمي الذي بلغ (+2.3) نقطة. كما تجاوز العراق دولاً مثل المكسيك وتركيا ومصر، ليحقق مؤشراً بلغ (92.50)، وهو ما يُعد "أكبر تقدم عربي" في هذا المجال. ليحتل بذلك المرتبة (31) عالمياً و(11) عربياً. وقد تمثّلت نقاط القوة التي أظهرها العراق وفقاً لمؤشر الأمن السيبراني في الآتي **:**[5].

1 -**محور التشريعات :**تحسّن بنسبة 15% وذلك بعد إصدار عدد من التشريعات والأوامر الإدارية المتعلقة بالأمن السيبراني.

2- **البنية التحتية :**إنشاء المركز الوطني للأمن السيبراني.

3- **بناء القدرات :**تدريب أكثر من 1000 متخصص في مجال الأمن السيبراني.

موقع العراق وفقًا للركائز مؤشر الأمن السيبراني للعام 2024

النتيجة الكلية	الإجراءات القانونية	الإجراءات التقنية	الإجراءات التنظيمية	بناء القدرات	إجراءات التعاون
53.07	11,21	9,06	15,77	8,38	8,11

Global Cybersecurity Index 2024, International Telecommunication Union Development Sector, ITU Publications, 2024.

[5] مصدر سابق ـ

وعند البحث عن أسباب هذا التحسّن، نجد أن الجهود الحكومية التي اتخذها العراق في مجال الأمن السيبراني شملت ما يلي:

١. وضع استراتيجية شاملة للأمن السيبراني.
٢. إصدار مجموعة من القوانين والتعليمات والأوامر الإدارية التي تُنظِّم الأمن السيبراني في البلاد، مثل قانون التوقيع الإلكتروني ، واقرار وثيقة متابعة السياسات والمعايير لأمن المعلومات، ومشاركة البيانات من قبل مجلس الوزراء[6].
٣. إنشاء العديد من المديريات والشُعَب والأقسام في مختلف مؤسسات الدولة الأمنية، منها وزارة الدفاع، وزارة الداخلية، الأمن الوطني، المخابرات، وجهاز مكافحة الإرهاب، وغيرها.
٤. تعيين مستشار لرئيس مجلس الوزراء مختص في الأمن السيبراني.
٥. تأسيس العديد من المراكز المعنية بالأمن السيبراني.
٦. تطوير عمل فريق الاستجابة للحوادث السيبرانية، وهو فريق وطني مشترك مختص بمجال الأمن السيبراني والاستجابة للحوادث وحماية البنية التحتية للإنترنت، ونشر الوعي في مجال حماية الخصوصية والحماية الذاتية للأفراد والمؤسسات على الإنترنت. يعمل هذا الفريق تحت إشراف مستشارية الأمن الوطني العراقي، ويتحمّل مسؤولية تأمين وحماية الشبكات ومراكز البيانات الوطنية والمواقع الرسمية التي تعمل في الفضاء السيبراني العراقي، ويقوم بتنسيق الجهود الوطنية ودعم المؤسسات في القطاعيّن العام والخاص لحماية نفسها وخدماتها في الفضاء السيبراني[7].

[6] - CER.Thttps://cert.gov.iq/pdf/2.pdf.
[7] - مصدر سابق

٧. عقد العديد من المؤتمرات والورش المعنية بالأمن السيبراني.
٨. تأسيس عدد من الكليات والأقسام العلمية المختصة بالأمن السيبراني في الجامعات العراقية، فضلاً عن فتح أقسام للأمن السيبراني في 30 معهداً مهنياً.
٩. تعزيز الشراكات الدولية في مجال الأمن السيبراني.

10-توسيع البنية التحتية المُتعلِقة بالأمن السيبراني.

ولكن مع ذلك، لا يزال العراق بحاجة إلى بذل المزيد من الجهود لبناء أمن سيبراني رصين، فضلاً عن تحسين موقعه في المؤشر العالمي.

ومن أجل تحقيق ذلك، لابد من العمل على اعتماد مجموعة من الإجراءات، منها:

١. تشريع القوانين المتعلقة بالأمن السيبراني: لا يزال قانون جرائم المعلوماتية، المطروح في البرلمان منذ عام 2011، دون تصويت نهائي عليه، رغم اجتيازه القراءة الأولى. ويُعزى هذا التأخير إلى الخلافات بين القوى السياسية، والنخب الإعلامية والفكرية، ومؤسسات المجتمع المدني بشأن تأثير القانون على حرية التعبير وحرية الإعلام والحريات السياسية عموماً، إضافةً إلى المخاوف من استخدامه كأداة رقمية لقمع المعارضين وحرمانهم من الاستفادة من الفضاء السيبراني، الذي يُعد وسيلة منخفضة الكُلفة وعالية التأثير للتعبير والتواصل، سيما في ظل عدم اكتمال البنية

القضائية الكفيلة بمنع إساءة استخدام هذا القانون. كما ساهمت الضغوط الخارجية المرتبطة بحقوق الإنسان والحريات الرقمية في إعاقة تمريره حتى الآن.

٢. عدد ورش العمل والندوات حول الأمن السيبراني لا يزال محدود جداً مقارنةً بدول الجوار مثل السعودية والإمارات.

٣. لا تزال الميزانيات الْمخصصة للأمن السيبراني قليلة بالمقارنة مع دول الجوار مثل إيران، السعودية، والكويت.

٤. لا توجد بنية تحتية مادية وبشرية متكاملة في مجال الأمن السيبراني، كما لا توجد هيئة وطنية مسؤولة بشكل مباشر عن الأمن السيبراني في العراق.

٥. نقص في الدورات التدريبية لموظفي الدولة كافة حول الأمن السيبراني.

٦. لا يلعب العراق دوراً مهماً وفاعلاً في المنتديات الدولية المعنية بالأمن السيبراني.

٧. شهدت تكلفة الجرائم السيبرانية ارتفاعاً كبيراً على مستوى العالم، حيث وصلت تقريباً إلى 10 تريليون دولار أمريكي سنوياً. وفي منطقة الشرق الأوسط، تشير تقارير من شركتيّ IBM و Verimatrixإلى أن متوسط تكلفة خرق بيانات واحد ارتفع إلى 8.75 مليون دولار أمريكي في عام 2024، مقارنةً بـ 8.07 مليون دولار في عام 2023، وهو ما يُعد تقريباً ضعف المتوسط العالمي الذي يبلغ 4.45 مليون دولار[8]، وفي ظل التحوّل الرقمي والسيبراني المستمر في العراق يومياً، يواجه البلد تحدياً متزايداً يتمثل في ارتفاع التكلفة الاقتصادية للجرائم السيبرانية، التي قد تكون مقاربة لمستوى دول الشرق الأوسط.

---

[8] – Cost of a Data Breach Report 2024. https://www.ibm.com/reports/data-breach

رابعاً: التوصيات لتعزيز الأمن السيبراني في العراق:

يحتاج العراق إلى بناء منظومة فاعلة وشاملة في مجال الأمن السيبراني، لمواكبة التحديات الأمنية المتزايدة والخطيرة التي يشهدها الفضاء السيبراني. ويتطلب ذلك اتخاذ مجموعة من الإجراءات الأساسية، من أبرزها:

1-سنّ التشريعات اللازمة لتنظيم الفضاء السيبراني:

وضع إطار قانوني شامل يتضمن إصدار القوانين والتعليمات الفنية التي تضمن فاعلية أداء الأجهزة الأمنية السيبرانية، مع توفير الدعم القانوني للمؤسسة القضائية في التعامل مع الجرائم والتهديدات السيبرانية ، فضلاً عن فصل قانون الأمن السيبراني عن قانون جرائم المعلوماتية.

2- **تطوير البنى التحتية المادية والبشرية:**

الاستثمار في بناء القدرات التقنية والكوادر البشرية المؤهلة للتعامل مع التحديات السيبرانية، من خلال التدريب والتأهيل المستمر.

3-**تأسيس هيئة وطنية للأمن السيبراني:**

إنشاء جهة مركزية مختصة بإدارة ملف الأمن السيبراني على المستوى الوطني، تتولى التنسيق بين الجهات المدنية والعسكرية ذات العلاقة، لضمان توحيد الجهود ورفع مستوى الحماية السيبرانية.

4-**توسيع التعليم الأكاديمي في مجال الأمن السيبراني:**

العمل على إنشاء كليات وأقسام متخصصة في الأمن السيبراني ضمن الجامعات العراقية المدنية والعسكرية، تمنح درجات البكالوريوس والدراسات العليا، سيما وأنه -حتى الآن - تم فتح برامج ماجستير فقط في جامعات بغداد، الموصل، والجامعة التكنولوجية.

5-**بناء مؤسسات أمنية سيبرانية متخصصة:**

تأسيس كيانات أمنية سيبرانية مثل الشرطة السيبرانية، الأمن الوطني السيبراني، المخابرات السيبرانية، الجيش السيبراني، وغيرها، لمواجهة التهديدات السيبرانية على الصعيديّن الداخلي والخارجي.

6-**تعزيز الوعي الإعلامي والثقافي:**

إطلاق حملات توعية تثقيفية تُسلِّط الضوء على خطورة التهديدات السيبرانية، وتعمل على تعزيز ثقافة الأمن السيبراني لدى مختلف فئات المجتمع.

7-**إنشاء منظومة قانونية وقضائية متخصصة:**

تطوير تشريعات وآليات قضائية فعّالة لمعالجة قضايا الجرائم السيبرانية والارهاب السيبراني والعنف السيبراني والتحقيق فيها وملاحقة مرتكبيها.

8-**الانخراط في التعاون الدولي:**

المشاركة الفاعلة في الاتفاقيات والمؤتمرات الدولية المعنية بالأمن السيبراني، والاستفادة من الخبرات والتجارب العالمية في هذا المجال.

9-**تعزيز برامج التدريب والتأهيل المتخصص:**

توسيع نطاق التدريب في مهارات الأمن السيبراني ليشمل جميع مؤسسات

الدولة، سيما الأجهزة الأمنية كوزارة الداخلية، وزارة الدفاع، الأمن الوطني، المخابرات، الحشد الشعبي، وجهاز مكافحة الإرهاب..الخ.

10-**توسيع مفهوم الأمن السيبراني ليشمل مختلف مجالات الحياة:**

العمل على تطوير فهم شامل للأمن السيبراني بوصفه عنصراً أساسياً في حماية ليس فقط البنى التحتية الرقمية، بل أيضاً الأنشطة الاقتصادية، والسياسية، والثقافية، والطبية، والدينية، وذلك لضمان تحصين المجتمع والدولة في جميع الأبعاد والمستويات ضد التهديدات الرقمية المعاصرة.

***