دراسات

البناء الاستراتيجي للأمن السيبراني في العراق

دراسة في السياسات الحكومية والتحديات التنفيذية

أنور المؤمن

تصـــدر عن مركـز رواق بـــغداد للسياســـات العـــامة
Published by Rewaq Baghdad Center for Public Policy

1 حزيران 2025

مِداد مشروعٌ بحثي يعنى بتقديم اوراق وافكار دقيقة عبر سلاسل، وحلقات متكاملة، تحاول ان تغطي الطيف الواسع من المشكلات التي تواجه قطاعات الدولة العراقية بكل اركانها، ويعتمد بشكل اساس على اوراق السياسات العامة، والسيمنار، والحوارات المعمقة، بين مختلف الاطراف، من صناع القرار في الحكومة التنفيذية، الى التشريعين في مجلس النواب، فضلا عن الباحثين والخبراء في الجامعات ومؤسسات البحث العراقية، وهو احد مشاريع مركز رواق بغداد للسياسات العامة، و يعد هذا المشروع امتداداً للجهد الذي بذل على مدى خمس سنوات من عمر المركز الذي تأسس في العام 2019، اذ قدم خلال تلك السنوات عشرات الدراسات والمشاريع البحثية والأوراق التي نشرت في الموقع الإليكتروني لمركز رواق بغداد.

رئيس المركز عباس العنبوري

مدير المشروع انور المؤمن

تصميم اية الحكيم

يمكن تحميل هذه الورقة مجاناً من الموقع الإليكتروني www.rewaqnaghdad.org

رقم الهاتف: 07845592793

صفحة الفيس بوك مركز رواق بغداد للسياسات العامّة

صفحة الإنستغرام RewaqBaghdad

قناة اليوتيوب Rewaq Baghdad

البناء الاستراتيجي للأمن السيبراني في العراق

دراسة في السياسات الحكومية والتحديات التنفيذية

أنور المؤمن

باحث في مركز رواق بغداد للسياسات العامة، مدير مشروع مداد البحثي

المقدمة

بادئ ذي بدأ شهد العراق بعد عام 2003، تحولات عميقة على مختلف الأصعدة: السياسية، والاجتماعية، والاقتصادية، والثقافية، إلى جانب تغييرات جذرية في مجالات التقنية والاتصالات والإنترنت. ويمكن القول إن العراق بدأ يشكل مجالًا رابعًا جديدًا يُضاف إلى المجالات التقليدية الثلاثة (البر والبحر والجو)، وهو المجال السيبراني، نتيجة الاعتماد المتزايد على تقنيات المعلومات والاتصالات في القطاعات الحكومية والخاصة. مع هذا التحول الرقمي، برزت الحاجة الملحة إلى تطوير استراتيجيات أمن سيبراني فعالة لحماية البيانات الوطنية والبنى التحتية الحيوية من التهديدات المتزايدة والمعقدة. وقد أدرك صانع القرار العراقي أهمية الأمن السيبراني كجزء لا يتجزأ من الأمن القومي، مما دفع إلى تضمينه في استراتيجية الأمن القومي عام 2007، وعام 2025، ثم إصدار استراتيجية وطنية متخصصة للأمن السيبراني عام 2017. رغم ذلك، فإن التوجه الحكومي نحو التحول الرقمي وبناء أُطر الأمن السيبراني بدأ يتضح بشكل جدي منذ عام 2018، حيث بدأت البرامج الوزارية تتضمن خططًا أمنية سيبرانية. إلا أن تنفيذ هذه الاستراتيجيات واجه تحديات كبيرة على مختلف المستويات التنفيذية والتشريعية والتقنية، ما أثر سلبًا على قدرة العراق في مواجهة التهديدات السيبرانية وضمان أمنه السيبراني. يحاول البحث الإجابة عن سؤال أساسي الا هو: (كيف أثرت استراتيجيات الأمن القومي في بعدها السيبراني على صياغة وتطوير الخطط والسياسات الحكومية في العراق بعد عام 2007، وما هي التحديات التي واجهت البناء الاستراتيجي للأمن السيبراني في تحقيق أهدافه؟

البناء الاستراتيجي للأمن السيبراني في العراق.

يمكن القول ان البناء الاستراتيجي للأمن السيبراني يبدأ من الاستراتيجية الشاملة للأمن القومي للدولة، التي يمكن ان تؤسس الى بناء الهياكل والمؤسسات المعنية بالأمن السيبراني فضلا عن ذلك فأن الاستراتيجيات القومية الشاملة تبنى عليها الاستراتيجيات التكتيكية او الخطط التنفيذية التفصيلية[1] وهي هذا الإطار فأن العراق ولغاية أعداد هذه البحث، اقرت الحكومة العراقية، ثلاث استراتيجيات شاملة للأمن القومي بعد عام 2003، فضلا عن استراتيجية تفصيلية للآمن السيبراني عام 2017[2].

[1] في هذا الصدد يميز الباحثون بين نوعين من الاستراتيجيات، الأولى هي الاستراتيجية العظمى او الكبرى او استراتيجية الامن القومي الشاملة، وهي الاستراتيجية التي ترسم الأهداف الحيوية للدولة والتحديات والفرص وعلمية المطابقة والتوازن بين الأهداف والموارد، والنوع الثاني هي الاستراتيجية التنفيذية او خطة العمل، وهذه الاستراتيجية تتضمن الخطة التنفيذية وبشكل تفصيلي للوصول الى الأهداف والغايات المنشودة، للمزيد ينظر: عبد القادر محمد فهمي، المدخل الى دراسة الاستراتيجية، دار السنهوري، بغداد، بلا، ص 31 - 33.

[2] تم الاعتماد على دراسة الاستراتيجيات للمن القومي في هذا البحث على استراتيجيتان: الأولى للعام 2007، لعام 2015، ولم يتسنى للباحث الحصول على الاستراتيجية الأولى للأمن القومي 2005، رغم تأكيد صفاء الشيخ نائب مستشار الامن القومي السابق إقرار العراق لثلاثة استراتيجيات للأمن القومي، للمزيد ينظر، صفاء الشيخ، بين مجلس الامن الوطني ومستشارية الامن القومي من يصنع الامن في العراق، مجلة الرواق، مركز رواق بغداد للسياسات العامة، العدد 9، نيسان 2023، ص 196.

أولا: استراتيجية الامن القومي للعام 2007.

للوهلة الأولى عند الاطلاع على وثيقة الامن القومي العراقي لعام 2007، يؤشر الباحث عدم وورد مصطلح الأمن السيبراني بشكل صريح، لكن الإجراءات والوسائل والاهداف الاستراتيجية الواردة تقع في صميم الأمن السيبراني، اذ ان مفاهيم من قبيل: (حماية شبكات الاتصالات، وأنظمة المعلومات، والدفاع ضد الهجمات المعلوماتية، وتأمين الحكومة الإلكترونية) تدخل ضمن إطار الأمن السيبراني، وقد وردت في الأهداف الاستراتيجية في هذه الوثيقة ما يرتبط بالأمن السيبراني من قبيل:[3]

1. تأسيس شبكة اتصالات آمنة وموثوقة: تشير الاستراتيجية إلى ضرورة استكمال بناء شبكة اتصالات آمنة في عموم العراق.
2. انشاء أنظمة معلومات وإدارة معلومات: تؤكد الاستراتيجية على أهمية إنشاء أنظمة معلومات دقيقة وموثوقة لإسناد المصالح الوطنية، مع الإشارة إلى ضرورة حماية هذه الأنظمة من الهجمات المضادة.
3. تأمين عمليات معلوماتية هجومية ودفاعية: تذكر الاستراتيجية أن الحكومة يتوجب عليها القيام بعمليات معلوماتية للتأثير على أنظمة المعلومات المعادية والدفاع عن أنظمتها تجاه الهجمات المضادة.
4. منع نشر المعلومات المضللة: تشير الاستراتيجية جهود الحكومة العراقية لمنع نشر وتداول المعلومات الخاطئة والدعاية.
5. تأسيس الحكومة الإلكترونية: تشير الاستراتيجية إلى مبادرة الحكومة الإلكترونية، التي تعتمد بشكل أساسي على الإنترنت والبنية التحتية الرقمية، ما يستدعي وجود تدابير أمن سيبراني قوية لحماية بيانات المواطنين والمعاملات الحكومية الإلكترونية من الاختراقات والهجمات.

فضلا عن ذلك تضمنت وثيقة الامن القومي الوسائل لتحقيق تلك الأهداف وفي مقدمتها بناء هياكل لخدمة الانترنت في العراق، وتنظيم استخدامه فضلا عن ضوابط استخدام المجال الاليكتروني، ويمكن تحديد مجموعة الوسائل الخاصة بالأمن السيبراني على النحو التالي:[4]

1. تبني - وبأسرع وقت ممكن - أكثر أنظمة تقنية لمعلومات كفاءة لغرض استخدامها في القطاعين العام والخاص ومن خلال هذه الوسيلة تأمل الحكومة العراقية اكمال ربط العراق ومواطنيه بالمجتمع المدني.
2. تتطلب الديمقراطية والإدارة الرشيدة إيصال معلومات دقيقة وكاملة في الوقت المناسب لمواطنين والمنظمات الخاصة ودوائر الحكومة، وهو أيضاً مهم لاستعادة الأمن والازدهار في العراق.

[3] وثيقة استراتيجية الامن القومي (2007 ـ 2010)، مستشارية الامن القومي العراقي، بغداد، بلا، ص 23.
[4] المصدر نفسه، ص 33

3. ستقوم الحكومة العراقية الفيدرالية والدوائر التابعة لها والمؤسسات الأمنية بإنشاء أنظمة معلومات وأنظمة أدارة معلومات لزيادة الكفاءة الفعالية في تحقيق المهام.
4. ادارة عمليات معلوماتية للتأثير على الجمهور المتلقي مكمل لسعي الحكومة للتأثير على المجاميع المؤيدة والمضادة. يعتبر المجال المعلوماتي في الإستراتيجية الحديثة وفن الحرب موازيا للمجالات الدبلوماسية والاقتصادية والعسكرية، ولذلك فأن حكومة العراق القوات الأمنية ستقوم بعمليات معلوماتية للتأثير على أنظمة المعلومات المعادية وفي نفس، الوقت تدافع عن أنظمة معلوماتها تجاه الهجمات المضادة، ستبذل الحكومة لعراقية جهوداً خاصة لمنع نشر وتداول المعلومات الخاطئة والأعمال الدعائية التي كانت رائجة في زمن النظام السابق.
5. انشاء برنامج الحكومة الالكترونية لإسناد المصالح الوطنية قررت حكومة العراق التقدم للأمام في عملية ربط المواطنين بالحكومة وشعب العراق بالمجتمع الدولي، وتعتبر تقنية المعلومات أحد أهم الأمور المساعدة في مجال هذه الجهود. سيركز العراق بأقصى حد ممكن على التقنية اللاسلكية لتقليص الحاجة إلى استنزاف الوقت وإعادة إنشاء الشبكات الأرضية المكلفة. إن البرنامج الرئيسي تنفيذ هذا الجهد هو مبادرة الحكومة الإلكترونية. تهدف الحكومة الالكترونية لربط المواطنين بالدوائر الحكومية المسؤولة عن توفير الخدمات الأساسية لغرض إنجاز العمل بين الحكومة والمواطنين، أن الغرض من نشاء الحكومة الإلكترونية هو للاستجابة السريعة لاحتياجات المواطنين بأقل وقت ممكن وتجاوز الأعمال الروتينية وبالاستفادة القصوى من منظومة الإنترنت.
6. إصدار قانون يكفل حرية الصحافة والتعبير بكل الوسائل بما لا يخل بالنظام العام والآداب وعليه يتوجب إصدار قانون ينظم هذه العلاقة دون المساس بجوهر الحريات العامة التي ضمنها الدستور والمقارنة بالدول العصرية المتحضرة التي قطعت أشواطا جيدة في إرساء إعلام وصحافة ودور نشر مسموعة ومقروءة ومرئية بمختلف الوسائل والتقنيات.
7. وضع سياسة إعلامية وطنية تعزز المصالح الوطنية وتتصدى للإعلام المحرض على العنف والإرهاب هو هدف استراتيجي يتطلب رسم سياسة إعلامية، واختيار الأشخاص المتمرسين وفي كل المستويات، واعتماد آلية تنظم وتنسق عمل الهيئات المسئولة عن الإعلام العراقي والسعي للانضمام الى الاتفاقيات الدولية التي تعني بالإعلام.

ثانيا :استراتيجية الامن القومي لعام 2015.

تعد هذه هي الاستراتيجية النافذة للأمن القومي في العراق لغاية إعادة هذا البحث،[5] وقد تضمنت مصطلح ومفاهيم الامن السيبراني بشكل دقيق ضمن التحديات والاهداف فضلا عن خاتمة الاستراتيجية، ففي باب

الأهداف الاستراتيجية للأمن القومي العراقي ورد هدف (امن المعلومات والاتصالات السيبراني)، حيث تضمن هذا الهدف ما يأتي:[6]

1. ضمان امن المعلومات والاتصالات
2. تطوير قطاع المعلومات والاتصالات وبنيتها التحتية بما يخدم تطور ورفاهية المجتمع.
3. الحيلولة دون الاستخدام السلبي لتقنيات الاعلام والتواصل الاجتماعي والشبكة العنكبوتية ضد المجتمع والدولة مع ضمان الحريات الأساسية المنصوص عليها في الدستور.

اما في باب المخاطر والتهديدات التي تواجه الامن القومي في العراق، فقد اعتبرت هذه الوثيقة، ان الامن السيبراني: (يمثل المستوى الثاني من المخاطر والتهديدات التي تواجه الامن القومي العراقي وتحتاج الى خطط عمل على الأمد المتوسط..) وجاء في توصيف التهديدات السيبراني التي تواجه العراق بالنص: (... ان منظومات وشبكات الحاسوب والمعلومات لازالت في مراحل النمو في العراق ولم تصل بناها الى مرحلة يمثل التهديد عليها خطرا بالغً على الامن الوطني، ومع ذلك فان نموها السريع يوجب الاخذ بنظر الاعتبار تهديدات الفضاء الإلكتروني المتنامية...)، وتناولت الوثيقة اليات والوسائل تحقيق الأهداف في مجال الامن السيبراني وهي على النحو التالي[7]:

1. تنفيذ سياسة مشاركة وامن المعلومات الوطنية التي تم وضعها
2. انشاء مركز معلومات وطني او العمل على تطوير مركز معلومات البطاقة الوطنية الذي يجري انشاءه الى مركز معلومات وطني وانشاء مركز وطني للمعلومات الجغرافية.
3. تشكيل مؤسسة تتولى اعداد وتنفيذ سياسة واستراتيجية وطنية لتحقيق الامن السيبراني تتضمن تشخيص ومعالجة التهديدات والجرائم السيبرانية وضمان التنسيق مع الجهات المعنية دون المساس بالحقوق الفردية للمواطن. وتشريع القوانين اللازمة لذلك.
4. تطوير مناهج التدريس والتدريب

---

[5] تعد استراتيجية الامن القومي للعام 2015، الأهم بين الاستراتيجيات الثلاث وذلك للأسباب التالية: أولا: جاءت ديباجة هذه الاستراتيجية محملة بالتهديدات الموجهة للأمن القومي، الذي تعرض الى انتكاسة كبيرة في حزيران 2014، عندما احتل تنظيم داعش ثلاث محافظات عراقية وسيطر على مساحة تقدر بثلث مساحة العراق والامر الذي أدى الى قائمة طويلة من التهديدات تمثلت بعد الكبير للنازحين وتدمير البنى التحتية، وتدمير للأثار، وتهريب للثروات، فضلا عن الخسائر المالية والبشرية الهائلة، ثانيا: اشارت هذه الاستراتيجية الى ان المشاكل التي ورثها النظام الجديد في العراق بعد عام 2003، من المرحلة السابقة، واعتبرها تحديات متمثلة بمرحلة الحصار الاقتصادي على العراق (1990 - 2003)، وما خلفته من اثار فضلا عن الاثار التي لحقت بالمجتمع العراقي من جراء الحروب التي شنها النظام السابق على دول المنطقة، وما ترتب على ذلك من تبعات خارجية تمثلت بمشكلات حدودية وديون وتعويضات وغيرها، ثالثا: أن هذه الاستراتيجية لازالت قيد التطبيق، وتعد اول استراتيجية تقر من قبل مجلس الوزراء في عام 2016، وليس مجلس الأمن الوطني، كما أنها كانت تتمتع بقوة إلزامية أكثر من الاستراتيجيات التي سبقتها، ووقد تم اصدار امر ديواني بتشكيل لجنة في مستشارية الامن القومي لمتابعة مدى تطبيق الاستراتيجية. للمزيد ينظر: صفاء الشيخ، مصدر سبق ذكره، ص 198.

[6] وثيقة استراتيجية الامن الوطني العراقي 2015، مستشارية الامن القومي العراقي، بغداد، بلا، ص 12.

[7] المصدر نفسه، ص 30.

5. المشاركة الفاعلة في الاتفاقيات والنشاطات الدولية.
6. وضع وتنفيذ سياسة وطنية للتعامل مع وسائل الاعلام والتواصل الاجتماعي وغيرها، لتوجيه الطاقة النفسية للإنسان العراقي باتجاه إيجابي ينمي قدراته ويساهم في بناء الوطن ونفس الوقت التصدي للجهود المعادية والمستمرة الرامية الى زرع الاحباط والياس والسلبية والتحريض على العنف والتفرقة الطائفية والاثنية.

وانتهت الاستراتيجية في خلاصتها بوجوب وضع سياسة واستراتيجية وطنية للأمن السيبراني وتشريع القوانين والانظمة اللازمة لحماية المعلومات والاتصالات والخصوصية الفردية وبأسرع وقت ممكن بغية اللحاق بالعالم المتطور من خلال بناء قدرات وطنية والدور الهام للقطاع الخاص في هذا الصدد ...).[8]

ثالثا: استراتيجية الامن السيبراني عام 2017.

يمكن القول ان وثيقة استراتيجية الامن السيبراني العراقي لعام 2017، فقد نقلت مستوى البناء الاستراتيجي الى مرحلة جديدة، من حيث الخطوات العملية والتنفيذية والمديات الزمنية، فضلا عن مستويات مسؤولية التنفيذ التنفيذية والتشريعي والقضائية، فضلا عن تحديدها لأشكال ومصادر التهديد السيبراني، والفرص التي يوفرها بناء امن سيبراني، والوسائل التنفيذية لتحقيق الامن السيبراني طبقا لمدد زمنية محددة، إضافة الى التأكيد على دور الجانب الثقافي والمعرفي المجتمعي للأمن السيبراني، والاعتماد على الذات فضلا عن التعاون الدولي في هذا الصدد.

1. **التهديدات التي تواجه الامن السيبراني في العراق وفقا لاستراتيجية الامن السيبراني 2017:** ابتدأت هذه الوثيقة بتحديد مجموعة من الاشكال للتهديدات التي تواجه الامن السيبراني في العراق وهي قبيل[9]: العمليات التخريبية التي اصابت بعض المواقع الحكومية، وتزايد صناعة الجريمة السيبرانية، الممارسات الاحتيالية، وقوع الاستغلال عبر الإنترنت من شريحة الشباب من السكان، إساءة استخدام وسائل العالم ومواقع التواصل الاجتماعية لشن حملات خبيثة ضد الدولة، الصراع والعنف المستمر من خلال الإنترنت، التخريب الاقتصادي من خلال حرمان المواطنين من الوصول الى الخدمات الإليكترونية الحكومية وغير الحكومية، التجسس الإلكتروني المنسق، التدخل الخبيث في أنظمة الكمبيوتر والأجهزة الرقمية الأخرى، القرصنة الإلكترونية، سرقة الأصول الفكرية، الإرهاب الإلكتروني، الجرائم المالية عبر الإنترنت، غسيل الأموال، سرقة الهوية، التزوير، الابتزاز، البرمجيات الخبيثة، تزييف والتصيد، البريد الإلكتروني غير المرغوب، الخداع، برامج التجسس، وسرقة الملكية الفكرية، أحصنة طروادة والفيروسات، التلاعب بالأجهزة، والحرمان من الخدمة، خرق الوصول، سرقة كلمة المرور، نظام التسلل تشويه الموقع، استغلال متصفح الويب الخاص والعام، الرسائل الفورية وإساءة استخدام وسائل الاعلام والتواصل الاجتماعية.

---

[8] المصدر نفسه، ص 36.

[9] استراتيجية الامن السيبراني العراقي، الموقع الإليكتروني الاتحاد الدولي للاتصالات، متاح على الرابط، https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/00056_06_iraqi-cybersecurity-strategy.pdf، تاريخ الدخول والمشاهدة 2025/5/13، ص 3.

2. **الأهداف الاستراتيجية للأمن السيبراني في العراق وفقا لاستراتيجية الامن السيبراني 2017:** ان الأهداف الاستراتيجية المراد تحقيقها في مجال الأمن السيبراني الواردة في هذه الوثيقة الاستراتيجية فهي: (... حماية للبنى التحتية المعلوماتية الوطنية في مختلف الميادين وتحديد المجالات التي يجب العمل عليها في إطار تنفيذي متناسق للارتقاء بمستوى العراق السيبراني نحو بيئة سيبرانية امنة..) كما ان الوثيقة تسلط الضوء على الطرق التي سيتم به تقييم وتطوير وتنفيذ الإنذار المبكر والكشف والتفاعل وإدارة الأزمات لتوفير الاستعداد الاستباقي للرد على التهديدات الموجهة إلى البنى التحتية المعلوماتية الحرجة في العراق والتعامل معها[10].
3. **مصادر التهديد السيبراني وفقا لاستراتيجية الامن السيبراني 2017:** حددت هذه الاستراتيجية مصادر التهديد للأمن السيبراني فهي:[11] الدول الأجنبي، الهاكرز، النقابات الجنائية المنظمة، الإرهابيين والجماعات المتطرفة، الشركات
4. **المراحل الزمني لتنفيذ الاستراتيجية الامن السيبراني 2017:** حددت هذه الاستراتيجية ثلاث مراحل زمنية لتنفيذ هذه الاستراتيجية وهي على النحو التالي[12]:

المرحلة الأولى: معالجة المخاوف الفورية لمدة عام واحد، وتتضمن الإجراءات التالية:

- العمل على ايجاد التدابير والإجراءات لسد الفجوة الأمنية السيبرانية ومعالجة أوجه الضعف الأساسية فيها.
- إنشاء منصة مركزية آلية عمل الأمن السيبراني.
- زيادة الوعي بالأمن السيبراني وآثاره على الامن القومي العراقي.
- الاعتماد على فريق الاستجابة للحوادث السيبرانية العراقي في هذه المرحلة.
- العمل على طرح مسودات للقوانين المتعلقة بالفضاء السيبراني.
- العمل على طرح اسم الدولة العراقية في مجال الامن السيبراني عالميا.
- العمل على التواصل في مجال التعاون الدولي.

المرحلة الثانية: بناء البنية التحتية لمدة 3 سنوات، وتتضمن الإجراءات التالية:

- إعداد ما يلزم من العمليات والمعايير والترتيبات المؤسسية.
- بناء القدرات بين الباحثين ومهنيين أمن المعلومات.
- العمل على استحداث اختصاص جامعي يختص بالأمن السيبراني
- إضافة تخصص يعنى بالجنائيات الرقمية وطرق التحقيق والاثبات في القضايا المتعلقة بالجرائم المعلوماتية
- إضافة المناهج والتخصصات التي تعنى بالجرائم المعلوماتية لطالب كليات الحقوق والقضاة.

[10] المصدر نفسه، ص 3
[11] المصدر نفسه، ص 6.
[12] المصدر نفسه، ص 11،

المرحلة الثالثة: تطوير الاعتماد على الذات لمدة 5 سنوات فأكثر، وتتضمن:

- تطوير الاعتماد على الذات من حيث التكنولوجيا وكذلك المهنيين.
- رفد المؤسسات الحكومية بخريجي اختصاص الامن السيبراني.
- مراقبة آليات الامتثال للخطط والمعاير القياسية الموضوعة لألمن السيبراني العراقي.
- تقييم الآليات وتحسينها.
- خلق ثقافة الامن السيبراني.

5. **مستويات تنفيذ الاستراتيجية:** توزعت مستويات تنفيذ هذه الاستراتيجية بين المستوى التنفيذي والتشريعي، وعلى النحو التالي[13]:

المستوى التنفيذي: الحكومي فيتضمن مجموعة من الإجراءات:

- العمل على التنسيق لتكوين مبادرة الامن السيبراني الوطني.
- تعزيز التعاون الفعال بين القطاع العام والقطاع الخاص.
- انشاء التبادل والمشاركة الرسمية للمعلومات والتشجيع على المشاركة الغير الرسمية للمعلومات للسرعة في تناقل المعلومات.
- العمل على تفعيل الحكومة الإلكترونية بشكل يضمن راحة المواطن
- بناء وتطوير إطار تكنلوجي وطني للأمن السيبراني والذي يحدد متطلبات السيطرة على المن السيبراني العراقي.
- العمل على بناء او انشاء برنامج وطني لتقييم إصدار شهادات للمنتجات ونظم الامن السيبراني.
- العمل على بناء وتطوير وتعزيز ثقافة الأمن السيبراني الوطني.
- العمل على انشاء وتوحيد وتنسيق برامج التوعية والتثقيف في مجال الأمن السيبراني.
- العمل على إنشاء وتطوير آلية فعالة لنشر المعلومات عن الأمن السيبراني على المستوى الوطني.
- تحديد الحد الأدنى من المتطلبات والمؤهلات للعاملين في مجال أمن المعلومات.

[13] المصدر نفسه، ص 8.

المستوى الإطار التشريعي والقانوني فيتضمن مجموعة من الإجراءات:

- مراجعة وتحسين القوانين السيبرانية العراقية الحالية (ان وجدت) لغرض معالجة الطبيعة الديناميكية للتهديدات التي تواجه الامن السيبراني العراقي.
- طرح وانشاء قوانين سيبرانية جديدة لغرض تعزيز الوضع القانوني السيبراني العراقي كقانون امن الاتصالات والمعلومات، قانون الخصوصية والخ.
- التأكد من أن جميع التشريعات المحلية المعمول بها تكمل وتنسجم مع القوانين والمعاهدات والاتفاقيات الدولية.
- انشاء برامج بناء القدرات التدريجي للجهات القانونية التنفيذية الوطنية.

المبحث الثاني: السياسات الحكومية العراقية في المجال السيبراني

يمكن القول ان التحول الإليكتروني في العراق قد شهد تطورا ابتداء منذ عام 2017، حيث تم إطلاق اول مشروع اليكتروني وهو مشروع البطاقة الوطنية العراقية الاليكترونية، اذ تم تشريع قانون البطاقة الوطنية في عام 2016، ومنذ عام 2017 ولغاية عام 2024، اذا أصدرت وزارة الداخلية العراقية 40.152.177،[14] وفي عام 2021، تم اطلاق مشروع الحكومة الإليكترونية (بوابة اور)، وكان التشغيل التجريبي في تضمن تقديم 60 خدمة اليكترونية للمواطنين، ثم تم اعتمادها رسميًا في 2022 بـ 90 خدمة، وبدأت اغلب قطاعات الدولة بالتحول نحو الاتمتة الاليكترونية في المجالات الصحية كنظام الضمان الصحي، والمجالات السياسية كأجراء الانتخابات الاليكترونية، فضلا عن المجالات المالية والمصرفية، حيث وصل مبلغ المدفوعات الرقمية إلى 7.6 تريليون دينار عراقي في عام 2024، ووصل عدد بطاقات الذكية المصرفية (وفقا لإحصائيات البنك المركزي العراقي) الى 20 مليون بطاقة في عام 2024[15].

ويمكن القول ان هذا التحول نحو المجال السيبراني، لم يكن مستندا الى استراتيجيات الامن السيبراني، فحسب، اذ ان الامن السيبراني مثل اهتمام حكوميا على مستوى البرامج الوزارية للحكومات العراقية منذ عام 2018، حيث تبنت تلك البرامج ما ورد في الاستراتيجيات الامن القومي في المجال السيبراني من حيث بناء التحول الاليكتروني واهمية الامن السيبراني لهذا التحول فضلا عن انشاء هياكل متخصصة من اجل تحقيق الامن السيبراني في العراق.

---

[14] الداخلية: أكثر من 40 مليون عراقيّ حصلوا على البطاقة الوطنية الموحدة، وكالة بغداد اليوم الإخبارية، متاح على الرابط، https://baghdadtoday.news/257371-%D8%A7%D9%84%D8%AF%D8%A7%D8%AE%D9%84%D9%8A%D8%A9-%D8%A3%D9%83%D8%AB%D8%B1- تاريخ الدخول والمشاهدة، 2025/5/13.

[15] مؤشرات اقتصادية للفصل الرابع لعام 2024، الموقع الإليكتروني للبنك المركزي العراقي، متاح على الرابط، https://cbi.iq/news/view/2815 ، تاريخ الدخول والمشاهدة 2025/5/13.

أولا :البرنامج الوزاري للحكومة العراقية عام 2018.

تضمن هذا البرنامج في المحور الأول منه الموسوم بـ (استكمال بناء أسس الدولة الاتحادية الواحدة ونظامها الجمهوري النيابي الديمقراطي) وقد تضمنت الفقرة الثالثة منه (التحول الكامل نحو تطوير أنظمة الحوكمة بشكل جذري...) ونصت على: (... يجب ان تكون الحوكمة الجيدة بديلاً عن الادارات البيروقراطية المتخلفة السابقة، واحلال النظم الذكية والحكومات الالكترونية بديلاً عن النظم الورقية، لتقديم ممارسة رائدة تحظى بالاهتمام الاول للمسؤولين لتمكين البلاد من تحقيق تقدم حقيقي ومحاربة الفساد، لما توفره النظم الورقية والبيروقراطية من مجالات فساد في التدخل والوساطات غير المشروعة والرشاوى والعراقيل، التي تضع الجميع تحت ضغط الممارسات الخاطئة ونقص الشفافية وضعف المعلوماتية وشخصنة المؤسسات، مع التركيز على استخدام الانظمة الذكية وانظمة التعقب والتعريف الالكترونية لتنظيم المرور والسيطرة على الارهاب والاجرام والاقتصاد، والتخلص من الحواجز والسيطرات لإعادة الحركة والحياة الطبيعية الى المدن والبلاد...)[16].

وتضمن هذا المحور مجموعة من الإجراءات التي تعهدت الحكومة في هذا البرنامج من تنفيذها في المجال السيبراني وهي:

1. تطوير الخدمات الالكترونية وتوحيد المعلومات المشتركة بين هذه الخدمات والمعلومات
2. التشريعات الخاصة بعمل الحكومة الالكترونية
3. تأسيس الشبكة الحكومية المؤمنة
4. تأسيس مركز البيانات الوطني
5. تأسيس مشروع التوقيع الالكتروني
6. تأسيس نظام النافذة الواحدة للخدمات الالكترونية
7. انشاء البوابة الوطنية للخدمات الحكومية
8. انشاء نظام إدارة الموارد البشرية والرواتب المركزي

إضافة الى ذلك أكد البرنامج الوزاري على ضرورة تشريع قانون امن المعلومات، اذ نص على (... تفعيل القوانين المتعلقة بمكافحة الإرهاب ونشر الكراهية وتشريع قانون أمن المعلومات، ورصد كل الحركات والنشاطات المشبوهة والتي تهدف الى الاخلال بأمن المواطن والتصدي لها، من خلال عمليات تنفيذية وسيبرانية وإعلامية...)[17].

[16] البرنامج الحكومي 2018 ـ 2022، رئاسة مجلس الوزراء، بغداد، 2019، ص 17.
[17] المصدر نفسه، ص 19.

ثانيا: البرنامج الوزاري للحكومة العراقية عام 2022

كان لقطاع الامن السيبراني اهتمام في البرنامج الوزاري للحكومة العراقية عام 2022 اذ تضمن بعض الإجراءات للتحول الرقمي الحكومي فضلا عن الامن السيبراني وهي[18]: انشاء مركز البيانات الرقمي، تنفيذ المرحلة الثانية من مشروع البطاقة الموحدة عام 2016، وألبدا بأصدر البطاقة الموحدة الإليكترونية للعراقيين المقيمين خارج العراق، تنفيذ مشروع الجواز الاليكتروني، تنفيذ مشروع الفيزا والإقامة الاليكترونية، تنفيذ مشروع الأتمتة الإليكترونية لرصد المخالفات ومراقبة الطرق بواسطة الكاميرات وأجهزة قياس السرعة، ربط الأدلة الجنائية مع توابعها في المحافظات بمنظومة اتصال مؤمنة لتبادل البيانات، ربط قواعد بيانات الأدلة الجنائية مع قواعد بيانات البطاقة الموحدة، مشروع التحول الاليكتروني وبناء نظام مركزي لإصدار فواتير الكهرباء وتجهيز المنظمات الاليكترونية لذلك، اتمتة إجراءات الجمارك، مشروع النظام الضريبي الإلكتروني الشامل، تطوير نظام البطاقة التموينية الاليكترونية، تطبيق نظام النافذة الواحدة في تسجيل الشركات، اتمتة دوائر التسجيل العقاري، اتمتة دوائر التنفيذ، اتمتة دوائر الكتاب العدول، استكمال مشروع صد الهجمات السيبرانية.

هياكل الامن السيبراني في العراق

يمكن القول ان التوجه الحكومي نحو التحول الرقمي بناء على ما ورد في الاستراتيجيات او في البرامج الوزارية، كان يتطلب انشاء هياكل لحماية الامن السيبراني، خصوصا ان هذا التحول قد شهد كثافة في الاستخدام سيما في مجالات نتعد مهمة وحساسة كالمجلات الأمنية (مشاريع وزارة الداخلية كالبطاقة الوطنية، والجواز الاليكتروني)، فضلا عن المجالات السياسية كأجراء الانتخابات الإليكترونية في العراق، وبناء عليه أنشأت الحكومة العراقية مجموعة من الهياكل والمؤسسات بهدف تحقيق الامن السيبراني سواء للبنية التحتية الحكومية الإليكترونية وتأمين الحماية السيبرانية لها، او بالنسبة للمواطنين من حيث حمايتهم من الجرائم الإليكترونية ومظاهر التهديدات السيبرانية الأخرى الواردة في استراتيجية عام 2017. وهذه الهياكل هي:

أولا: مركز الامن السيبراني في وزارة الداخلية: أنشأ هذا المركز وفقا للاستراتيجية الوطنية للأمن السيبراني عام 2017، في وزارة الداخلية العراقية في 4 كانون الأول 2022، وهو مركز أمني معلوماتي يعنى بمجالات الأمن السيبراني ويرتبط بمكتب وزير الداخلية، يهدف الى حماية البنية التحتية المعلوماتية لدوائر وزارة الداخلية من التهديدات السيبرانية والحفاظ على الأمن الوطني وسلامة بيانات ومعلومات المؤسسات والمواطنين والافراد العاملين في وزارة الداخلية[19].

[18] مسودة البرنامج الحكومي 2023 ـ 2025 الإجراءات التنفيذية للوزارات، الأمانة العامة لمجلس الوزراء، بغداد، 2022، ص 13 ـ 43.
[19] وزارة الداخلية العراقية، مركز الامن السيبراني، متاح على الرابط https://cert.gov.iq/cert /، تاريخ الدخول والمشاهدة، 2025/5/13.

ثانيا: مديرية الامن السيبراني التابع لوزارة الداخلية: أنشئت هذه المديرية في شباط 2025 ضمن وزارة الداخلية، وتقوم هذه المديرية بالمهام التالية[20]:

1. وضع السياسات والاستراتيجيات الخاصة بالأمن السيبراني ومتابعة تنفيذها.
2. ادارة حوادث وتهديدات الامن السيبراني.
3. الكشف عن الثغرات الامنية في التطبيقات والمواقع والانظمة.
4. الكشف عن نقاط الضعف في البنى التحتية للشبكات السلكية واللاسلكية.
5. تحليل مواقع الانترنت ومواقع التواصل الاجتماعي.
6. تثقيف ونشر الوعي الامني بين منسوبي قوى الامن الداخلي وباقي شرائح المجتمع.
7. مراقبة وتحليل مراكز البيانات والمحطات الطرفية الخاصة.
8. الاستجابة والحد من عمليات اساءة استخدام تكنولوجيا المعلومات والاتصالات.

ثالثا: مديرية الأمن السيبراني في وزارة الدفاع العراقية: أنشأت في عام 2022، بهدف حماية الفضاء السيبراني للوزارة كتأمين الاتصالات العسكرية والبيانات والبنية التحتية لوزارة الدفاع الوطني[21].

رابعا :جهاز الامن الوطني: يعمل هذه الجهاز كوكالة امنية رئيسية لجمع المعلومات وتحليل التهديدات والمشاركة النشطة ضد مختلف التهديدات السيبرانية، ويقدم هذا الجهاز خدمات مباشرة للامنا لسيراني في حال تعرض المواطنين الى تهديد سيبراني وجرائم اليكترونية من خلال وضع رقم استجابة طارئ (131)،[22] فضلا عن ذلك اسس جهاز الامن الوطني في 7 تشرين الأول 2024، منصة اليكترونية بهدف حماية البيانات الشخصية، باسم "أمان" وتعنى بفحص الهواتف والملفات والروابط قبل استخدامها والتأكد من خلوها من أي برامج خبيثة[23].

خامسا: مركز البيانات الوطني في الأمانة العامة لمجلس الوزراء: تم افتتاحه في 20 اب 2023، ويعد مركز البيانات الوطني بنية تحتية للتحول الرقمي في العراق، حيث يشرف على البوابة الحكومية الموحدة للخدمات الإلكترونية (اور) وحيث يعد امن هذه البيانات من أولويات الامن القومي العراقي، اذ يدير هذا المركز بيانات حكومية وخاصة بالمواطنين من حيث البينات الشخصية والتجارية والصحية والأمنية وغيرها. يوفر المركز بيئات خادم افتراضية آمنة وخدمات الحوسبة السحابية للمؤسسات الحكومية. كما أنشأ خدمة إلكترونية

[20] وزارة الداخلية العراقية، مديرية الامن السيبراني، متاح على الرابط، https://moi.gov.iq/?page=6295 ، تاريخ الدخول والمشاهدة، 2025/5/13.

[21] وزارة الدفاع العراقية، المفتشية العسكرية العامة تجري تفتيشا لمديرية الأمن السيبراني، متاح على الرابط، https://mod.mil.iq/?article=4360 ، تاريخ الدخول والمشاهدة، 2025/5/13.

[22] جهاز الامن الوطني العراقي، متاح على الرابط، https://www.inss.gov.iq/index.html، تاريخ الدخول والمشاهدة 2025/5/13.

[23] المنصة الإليكترونية امان، متاح على الرابط، https://aman.gov.iq/ ، تاريخ الدخول والمشاهدة، 2025/5/13.

في أيار 2024 للمواطنين للإبلاغ عن الثغرات الأمنية في المواقع والخدمات الحكومية. من اجل تشجيع المواطنين في تعزيز الأمن السيبراني للحكومة[24].

سادسا: فريق الاستجابة لحوادث الأمن السيبراني: فريق أمني تقني مختص بمجال الأمن السيبراني، والاستجابة للحوادث السيبرانية، وحماية البنية التحتية للأنترنت، ونشر الوعي في مجال حماية الخصوصية والحماية الذاتية للأفراد والمؤسسات على الانترنت، أنشأ من قبل مستشارية الامن الوطني مع إطلاق الاستراتيجية للأمن السيبراني عام 2017 وللفريق مهام محددة وهي:[25]

1. جمع المعلومات عن التهديدات والمخاطر السيبرانية المحلية والإقليمية والدولية.
2. الاستجابة للتنبيهات الصادرة من المراكز الإقليمية والدولية وشركات القطاع الخاص والخبراء في مجال الأمن السيبراني.
3. الاستجابة الفورية للحوادث السيبرانية من خلال تقييم الضرر ومستوى الخطورة واحتواء الهجمة ومعالجة الخروقات الأمنية.
4. دعم ومساندة الفرق الأمنية المحلية في جميع المؤسسات والدوائر وتقييم إجراءاتها بشكل دوري والتنسيق لإجراءات فحوص أمنية شاملة للتأكد من تطبيق معايير الأمن السيبراني.
5. التقويم التكنلوجي والمتابعة الدورية للنظام الأمني للمعلومات المطبقة حالياً في القطاعين العام والخاص لتقويم الإجراءات الأمنية والاحترازية المتبعة.
6. دعم مديري الأنظمة والبيانات في الوزارات والمؤسسات الحكومية بهدف تحصين شبكاتها وحمايتها من الاختراق والمعالجة عند حدوث طارئ.
7. الكشف المبكر عن الهجمات الإلكترونية ومعالجتها ووضع الحلول المناسبة لتفادي حصول اي خسائر للبيانات جراء تلك الهجمات.

سابعا: جهاز المخابرات الوطني: يعد هذا الجهاز الأمني من الأجهزة المهمة والاساسية في حماية الامن السيبراني للعراق، لما له من سلطات وقدراته في جمع المعلومات الاستخبارية والكشف عن التهديدات والاستجابة لها فيما يتعلق بالأمن السيبراني والتهديدات التي تواجه العراق، وفي هذا المجال فأن نشاط وعمل جهاز المخابرات من اكثر الأنشطة والاعمال سرية من بين هياكل الامن القومي العراقي، واذا كان جهاز المخابرات، يهتم بالجهد الأمني والاستخباري تجاه التهديدات الخارجية، فمن المرجح ونتيجة للتعقيد والتشابك في مجال الامن السيبراني ان تكون له نشاطات في هذا الاطار على المستوى الداخلي والشخصي فيما يتعلق بأمن الافراد في العراق.

[24] الامانة العامة لمجلس الوزراء، دائرة مركز البيانات الوطني، متاح على الرابط، https://ndc.egov.iq/، تاريخ الدخول والمشاهدة، 2025/5/13.

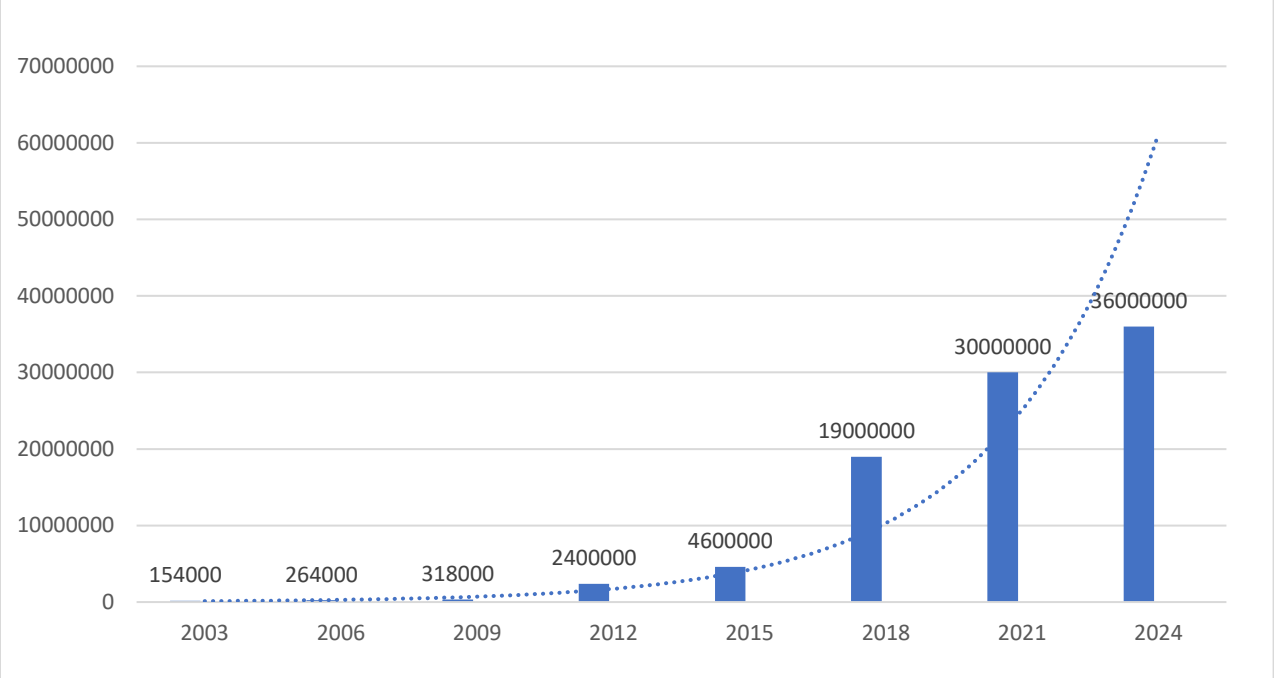
[25] فريق الاستجابة لحوادث الامن السيبراني، متاح على الرابط، https://cert.gov.iq/cert/ ، تاريخ الدخول والمشاهدة، 2025/5/13.

التحديات التي تواجه الامن السيبراني في العراق.

بالرغم وجود استراتيجيات واهتمام حكومي متزايد بقطاع الأمن السيبراني في العراق، إلا أن هذا القطاع يواجه تحديات كبيرة أبرزها ضعف البنية التحتية التقنية، وغياب التشريعات القانونية الفعّالة، ونقص الكوادر البشرية المتخصصة. كما يعاني العراق من قلة التنسيق المؤسسي، ومشكلات في البنية التحتية لقطاع الانترنت، ونقص الوعي السيبراني لدى الأفراد والمؤسسات، مما يجعله عرضة لهجمات إلكترونية متكررة وتهديدات متزايدة على أمنه الوطني، ومن وجهة نظر الباحث ان أولى التحديات التي يواجه هذا القطاع هو الشحة والمحدودية في نشر البيانات والوثائق الرسمية المتعلقة بالأمن السيبراني، سواء بالنسبة لعدد الجرائم والهجمات السيبرانية، فضلا عن عدم وجود دليل او وثائق او بيانات رسمية فيما يتعلق بالأمن السيبراني، إضافة الى ذلك يعاني هذا القطاع من غياب القوانين والتشريعات الخاصة بالأمن السيبراني، اذ لا يوجد في العراق . حتى وقت اعداد هذا البحث . أي تشريع محدد في مجال الامن السيبراني، سواء على مستوى الجرائم السيبرانية، او على مستوى حماية البيانات والخصوصية الاليكترونية، فضلا عن عدم وجود الجهة العليا للأمن السيبراني في العراق، وبالرغم من ان استراتيجية الامن السيبرانية عام 2017، تناولت تفصيلات تنفيذية عديدة الا ان هذه الاستراتيجية جهة عليا ذات بناء قانونية ودستوري لتحديد الجهات المسؤولة عن تنفيذها ووضع المعايير الدولية والأطر التنظيمية لها، وتقديم التقارير الدورية لها، غير ان هذه التحديات اذا ما تم حلها تبقى هنالك تحديات اكثر خطوة وتهديدا للأمن السيبراني في العراق وهي كقطاع الانترنت.

الانترنت والامن السيبراني في العراق.

يمكن القول ان العراق قد متواليات هندسية في زيادة اعداد مستخدمي الانترنت منذ عام 2003، اذ ارتفعت اعداد المستخدمين بشكل قفزات سريعة وصولا الى عام 2024، حتى وصل الى ما يقارب 80% من إجمالي السكان البالغ عددهم 45 مليون نسمة (كما هو مبين في الجدول رقم 1).



اعداد مستخدمي الانترنت في العراق منذ عام 2003 ولغاية 2024 الجدول من اعداد الباحث، بالاعتماد على بيانات الموسوعة الحرة ويكيبيديا.

وبالرغم من وجود الاستراتيجيات على مستوى الامن القومي العراقي، فضلا عن الاستراتيجية المتخصصة بالأمن السيبراني، الا ان هذا القطاع لا يزال يعاني من تحديات وردت في الاستراتيجيات الا انها لم تعالج بشكل سليم ولا تزال تشكل ثغرات خطيرة في بناء امن سيبراني استراتيجي في العراق، اذ ان قطاع الإنترنت في العراق غير مُنظَّم حاليًا، ويحتاج لتطوير البنية التحية على مستوى الأسس القانونية والتقنية والتنظيمية وبناء القدرات اللازمة لتوفير الأمن السيبراني لمستخدمي الانترنت في العراق، ومن التحديات التي تواجه قطاع الانترنت في العراق وتؤدي الى ثغرات في الامن السيبراني منها:

1. الفوضى وسوء الإدارة لهذا القطاع، فمثلا لم يتم تشريع قانون ينظم عمل قطاع الاتصالات وتكنولوجيا المعلومات لغاية اعداد هذا البحث، وهو الامر الذي أوجد حالة من تداخل الصلاحيات بين عمل وزارة الاتصالات وهيئة الاعلام والاتصالات، كون ان جزء من عمل الهيئة معني بهذا القطاع، اذ يبلغ عدد مشتركي خطوط خدمة الانترنت للهاتف النقال للشركات العاملة

(زين، اسياسيل، كورك) (20.3) مليون مشترك،[26] فضلا عن ان هيئة الاعلام والاتصالات لم يشرع لها قانون حتى الان، ولا تزال تعمل وفق نص أمر سلطة الائتلاف المؤقتة رقم 65 لسنة 2004.

2. عمليات تهريب سعات الانترنت، وهذه تعد من أبرز المشكلات التي تواجه قطاع الانترنت في العراق والتي تكلف الدولة مبالغ كبيرة جدا، تصل إلى (80) مليون دولار شهريا، وتنقسم عمليات التهريب الى نوعين[27]:

- النوع الأول: عن طريق تمرير سعات إنترنت من خارج العراق دون دخولها إلى الشبكة الرسمية التابعة للدولة، أو بوابات النفاذ الحدودية.
- النوع الثاني: فإنه يجري عن طريق إحداث ثقب في الكابل الضوئي للإنترنت، والربط بطريقة محترفة مع الأسلاك الشعيرية.

3. اعتماد قطاع الإنترنت الثابت في العراق على الاتصال اللاسلكي (Wireless)، في إيصال الخدمة للمستخدمين، اذ تشير الاحصاءات لعام 2023 (الجهاز المركزي للإحصاء والسيطرة النوعية) الى عدد ابراج الانترنت للشركات المزودة 31,578 في عموم المحافظات العراقية باستثناء إقليم كردستان، وهذه رقم كبير مقارنة بعدد مستخدمي مشروع (FTTH) وهو (216.8) الف مشترك، وهذا يعني ان القطاع الانترنت لا يزال يعتمد بنسبة مرتفعة جدا على تقنية (Wireless)، والحق فأن تقنية الألياف الضوئية تتفوق بشكل هائل على البث اللاسلكي اذ ان الأخيرة تواجه مشكلات ابرزها: بطء نقل البيانات، وتأخر الاستجابة، بالأخص عند كثرة استخدام أجهزة البث في منطقة محدودة مما يؤدي للتداخل والتشويش فضلا عن التداخل الإشعاعي الذي يؤدي ازدحام الأبراج اللاسلكية البالغ عددها (31,578 برجًا)[28] لغاية عام 2019، مما يُسهّل على المهاجمين تنفيذ هجمات اعتراض البيانات (Eavesdropping) أو حقن حزم بيانات ضارة[29].

ويمكن القول ان الغالبية العظمى من الجرائم والهجمات الإلكترونية التي تعرض لها مستخدمي الانترنت في العراق تُرتكب سواء عبر المواقع الاليكترونية او عبر تطبيقات التواصل الاجتماعي، كانت تستهدف المواطنين بنسبة أكثر من المؤسسات الحكومية او الشركات، وتشمل أكثر الهجمات الإلكترونية شيوعًا: الاحتيال، الإلكتروني، وسرقة الهوية، واستغلال الأطفال في المواد الإباحية، والملاحقة الإلكترونية، والابتزاز الإلكتروني،

---

[26] وزارة التخطيط، الجهاز المركزي للحصاء، مسح استخدام التكنلوجيا والاتصالات لعام 2022، متاح على الرابط، https://cosit.gov.iq/ar/ تاريخ الدخول والمشاهدة، 2025/5/11.

[27] خسائر مالية فادحة.. كيف تجري عمليات تهريب الإنترنت بالعراق؟، صحيفة الاستقلال الاليكترونية، متاح على الرابط، https://www.alestiklal.net/ar/article/dep-news-1588691720 ، تاريخ الدخول والمشاهدة 2025/5/13.

[28] وزارة التخطيط، الجهاز المركزي للإحصاء، مسح أبراج الانترنت، للعام 2019، متاح على الرابط التالي، https://cosit.gov.iq/ar/ ، تاريخ الدخول والمشاهدة 2025/5/13.

[29] أنواع الهجمات السيبرانية وتأثيراتها وطرق الحماية منها، موقع نافذتي، متاح على الرابط، https://nafidaty.com/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%D8% AA/ ، تاريخ الدخول والمشاهدة، 2025/5/13.

وانتهاك حقوق النشر، وقرصنة الأقمار الصناعية، والإرهاب الإلكتروني[30]. وعلى المستوى الرسمي فقد حدثت هجمات اليكترونية بين عامي ٢٠١٦-٢٠١٧، تمثلت في اختراقات المواقع الاليكترونية لكلا من: موقع رئيس الوزراء العراقي، موقع مستشار الامن القومي، موقع مجلس النواب العراقي، موقع وزارة الداخلية، اختراق موقع الاستمارة الإلكترونية للتعيين على ملاك وزارة الصحة، وزارة الاتصالات، وزارة الشباب والرياضة، لموقع الرسمي للمفوضية العليا المستقلة للانتخابات.

الاستنتاجات

1. أظهر صانع القرار الاستراتيجي العراقي وعيًا متزايدًا بأهمية الأمن السيبراني، حيث تم إدراجه ضمن استراتيجيات الأمن القومي منذ عام 2007، وتبلور ذلك بإقرار استراتيجية وطنية متخصصة عام 2017.
2. رغم وجود أطر استراتيجية واضحة، إلا أن البنية التشريعية والتنظيمية ظلت متأخرة عن مواكبة التهديدات السيبرانية المتنامية، مع غياب قوانين وتشريعات سيبرانية
3. واجه تنفيذ الاستراتيجيات تحديات كبيرة، من بينها ضعف البنية التحتية للإنترنت، ونقص الموارد البشرية المؤهلة، وضعف التنسيق بين المؤسسات الحكومية، فضلا عن بناء هياكل للأمن السيبراني غير رسمية تقوض من قدرة العراق على بناء امن سيبراني استراتيجي.
4. هناك فجوة واضحة بين البناء الاستراتيجي للأمن السيبراني والسياسات الحكومية التنفيذية، إذ لم تتحقق الأهداف المرسومة بالقدر المطلوب بسبب العوائق التشريعية والتنظيمية والفنية.

التوصيات

1. تسريع إصدار التشريعات السيبرانية الشاملة: ضرورة إقرار قوانين متخصصة بالأمن السيبراني، تشمل مكافحة الجرائم الإلكترونية، حماية البيانات، والخصوصية، بما يتماشى مع التطورات التقنية والمعايير الدولية، لسد الفجوة التشريعية الحالية.
2. تعزيز التنسيق المؤسسي بين الجهات الحكومية: إنشاء هيئة وطنية عليا للأمن السيبراني تتولى التنسيق بين الوزارات والمؤسسات، وتوحيد الجهود في مواجهة التهديدات السيبرانية، ووضع سياسات موحدة للتعامل مع الحوادث والاستجابة للطوارئ.
3. تطوير البنية التحتية الرقمية: الاستثمار في تحديث وتوسيع شبكات الإنترنت الوطنية، وتأمينها ضد الهجمات، مع التركيز على حماية البنى التحتية الحيوية (الكهرباء، المياه، الاتصالات، المال)، وتطبيق معايير أمنية صارمة في جميع القطاعات.
4. بناء القدرات البشرية والتدريب: إدراج تخصصات الأمن السيبراني والتحقيق الرقمي في الجامعات العراقية، وتكثيف برامج التدريب والتوعية لموظفي الدولة والقطاع الخاص، ونشر ثقافة الأمن السيبراني بين جميع فئات المجتمع.

[30] سامر سلمان الجبوري، جريمة الاحتيال الاليكتروني دراسة مقارنة، رسالة ماجستير غير منشورة، كلية الحقوق، جامعة النهرين، بغداد، 2017، ص 58.

5. تعزيز التعاون الدولي والإقليمي: الانضمام إلى الاتفاقيات الدولية ذات الصلة، وتفعيل الشراكات مع المنظمات والدول المتقدمة في مجال الأمن السيبراني، للاستفادة من الخبرات وتبادل المعلومات حول التهديدات وأفضل الممارسات.
6. تفعيل برامج التوعية المجتمعية: إطلاق حملات توعية وطنية حول مخاطر الفضاء السيبراني، وطرق الحماية من الاحتيال والهجمات الإلكترونية، مع التركيز على الفئات الأكثر عرضة (الشباب، الأطفال، كبار السن).
7. تشجيع البحث العلمي والابتكار في الأمن السيبراني: دعم المشاريع البحثية في الجامعات والمراكز المتخصصة، وتوفير منح وتمويل للابتكار في حلول وتقنيات الحماية السيبرانية، بما يسهم في بناء اقتصاد رقمي آمن ومستدام.