
# إستراتيجية الأمن السيبراني العراقي

## ٢٠٢٢ ـ ٢٠٢٥

(مسودة نهائية)


فريق الإستجابة للأحداث السبرانية

## المحتويات

## التمهيد

إن الفضاء السيبراني لا يختص حصراً بخدمات الانترنت وتكنولوجيا الاتصالات والمعلومات فحسب، وانما يدخل في عدة مجالات أخرى مختلفة مثل البنى التحتية والخدمات الحكومية والمجتمعية، ولكن بمميزات وخصائص وتحديات مختلفة. يتميز هذا الفضاء بالتعامل مع البيانات والمعلومات بحفضها وتعديلها وتبادلها من خلال أنظمة شبكية خاصة تحكمها وتديرها مفاهيم الأمن السيبراني، حيث أصبح عالميا يمتلك ابعادا وطنية ودولية، وتتجسد في كل مفاصل الدولة الأمنية والاقتصادية والاجتماعية ولكن بصيغة الكترونية.

بالرغم من المزايا التي يقدمها التقدم التكنولوجي عن طريق الخدمات الرقمية الا انه يمكن أن يشكل تهديدا كبيرا يسبب أضراراً واسعة على الأمن الوطني والتنمية الاقتصادية والبنى التحتية الحرجة، وهذه التهديدات بدأت تتصاعد في الآونة الأخيرة وتصبح عابرة للحدود الوطنية، مما يجعل مواجهتها تحديا كبيرا ومعقدا لجميع الدول، ونظرا لحداثة التجربة ولوجود العديد من التهديدات والمخاطر التي يمكن أن نواجهها في هذا العالم، فلابد من بناء الأسس الصحيحة لإطار امني متكامل يوفر الحماية الكافية لقطاع الاتصالات وتكنولوجيا المعلومات ويعزز دوره في تحقيق الأهداف التنموية العراقية، وقد وضعت هذه الإستراتيجية على اساس هذا السياق وأستجابةً لهذا الأدراك.

## فريق الإعداد

إنطلاقاً من أهمية الامن السيبراني ، وجهت رئاسة الوزراء من خلال مجلس الامن الوطني بتشكيل فريق وطني مشترك بعضوية الجهات والمؤسسات ذات العلاقة وهي كل من (مجلس النواب، مجلس القضاء الاعلى، وزارة الدفاع، وزارة الداخلية، وزراة العدل، وزارة الاتصالات، وزارة التعليم العالي والبحث العلمي، وزارة الكهرباء، وزارة النفط، جهاز المخابرات الوطني العراقي، جهاز الأمن الوطني، جهاز مكافحة الارهاب، هيئة الحشد الشعبي، هيئة الاعلام والاتصالات، فريق الاستجابة لحوادث الأمن السيبراني، مستشار مدير مكتب رئيس مجلس الوزراء، الشركات الاهلية) لغرض وضع إستراتيجية العراق في مجال الأمن السيبراني وبالتعاون مع المختصين الدوليين من منظمة أسكوا.

# الفصل الاول

# لمحة عن إستراتيجية الامن السيبراني

## أ- المقدمة

الفضاء السيبراني هو عبارة عن شبكة مترابطة من الهياكل الأساسية للمعلومات الأساسية الحرجة وغير الحرجة، حيث يعمل على تقريب موارد المعلومات والاتصالات المترابطة من خلال استخدام تكنولوجيات المعلومات والاتصالات.

يشمل هذا الفضاء جميع أشكال التدخلات الرقمية، التفاعلات والتواصل الاجتماعي، التخصصات الاجتماعية، أنشطة المعاملات، المحتويات، والاتصالات، والموارد التي يتم نشرها من خلال الشبكات المترابطة جزءاً اساسياً من مقومات المجتمع والاقتصاد ويلعب دورا كبيرا في تنميتهما فضلا عن دوره في تعزيز قطاعي الأمن والدفاع وتطبيق الحكومة الالكترونية، وانتشر استخدامه في القطاع العام والخاص وبين المواطنين، وأصبح الاعتماد عليه بشكل أكبر في قطاعات البنى التحتية الحرجة كالطاقة والموارد المائية والصحة والنقل والاتصالات والخدمات المالية وقطاع الاتصالات وتكنولوجيا المعلومات فضلا عن الانترنت، حيث أصبح يربط كل هذه المكونات مع بعضها البعض ويوفر الفرص التنموية لجميعها.

عرف الأمن السيبراني في التقارير الصادرة عن قطاع تقييس الاتصالات بأنه "مجموع الأدوات والسياسات ومفاهيم وضوابط الأمن والمبادئ التوجيهية ونهج إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات وآليات الضمان والتكنولوجيا التي يمكن استخدامها في حماية البيئة السيبرانية وأصول المؤسسات والمستخدمين ، وتشمل أصول المؤسسات والمستخدمين أجهزة الحوسبة الموصولة بالشبكة والموظفين والبنية التحتية والتطبيقات والخدمات وأنظمة الاتصالات ومجموع المعلومات المنقولة و/أو المحفوظة في البيئة السيبرانية" [١].

ويسعى الأمن السيبراني إلى تحقيق خصائص أمن أصول المؤسسات والمستخدمين والحفاظ عليها وحمايتها من المخاطر الأمنية ذات الصلة في البيئة السيبرانية، وتضم الأهداف العامة للأمن ما يلي: التوفر، السلامة، والسرية.

## ب- أهمية إعداد إستراتيجية الأمن السيبراني

أعتمد الوجود الاقتصادي الرقمي للبلدان على الأداء الفعال لحوكمة البنية التحتية الرقمية. حيث ان العراق ليس معزولاً عن العالم بل هو مترابط مع بلدان أخرى وجهات فاعلة في الفضاء السيبراني من خلال شبكات مترابطة للبنى التحتية للمعلومات. وبالتالي، فإن البلد معرض لمخاطر يمكن التنبؤ بها وأخرى لا يمكن التنبؤ بها. مثلما هناك جهات فاعلة ذات نوايا مشروعة، فهناك أيضا جهات فاعلة أخرى ذات نوايا غير مشروعة وخبيثة داخل الشبكة العالمية.

نظراً لوجود قضايا هيكلية حرجة يمكن استغلالها لأغراض خبيثة ونوايا جنائية ضد البلد من أجل المساس بسرية نظم المعلومات الوطنية والبنية التحتية الحيوية للمعلومات وسلامتها وتوافرها وإمكانية الوصول إليها؛ مما ينعكس سلباً على المواطن وبالتالي على الأمن الوطني بشكل عام.

---

(١) www.itu.int

ان توفير الأمن للبنية التحتية الحيوية للمعلومات وغيرها من العناصر الحرجة في نظام المعلومات في ظل الوضع الراهن هو تحدٍ وطني ضخم. ويحتاج الأمن الوطني إلى إطار متماسك لحوكمة الأمن السيبراني لتوفير نهج شامل إزاء المشهد الأمني الحالي والمستقبلي. فالجهات الفاعلة الحكومية وغير الحكومية التي تتعرض للجرائم السيبرانية ومجهزة تجهيزاً كافياً بأدوات إلكترونية متطورة تتسبب في أضرار ذات بعد لم يسبق له مثيل.

## ج- الرؤية الوطنية للأمن السيبراني

تكون هذه الرؤية شاملة للفضاء السيبراني بأكمله، تلبي أولويات العراق وتطلعاته، وتؤكد على تعزيز حماية الأنظمة التقنية والتشغيلية والبنى التحتية الحساسة والقدرة على الصمود والتصدي للحوادث السيبرانية واحتواء الأضرار والتعافي منها في الوقت المناسب، بالإضافة إلى تعزيز ثقة المؤسسات الوطنية والمستثمرين والأفراد في الفضاء السيبراني العراقي، وكذلك المساهمة في النمو الاقتصادي والاجتماعي للعراق.

## د- اهداف إستراتيجية الأمن السيبراني

تعمل الإستراتيجية على توفير خارطة طريق متماسكة وبحوث علمية وآليات عمل لتنفيذ وتحقيق الرؤية الوطنية بشأن الأمن السيبراني، وتحقق مجموعة اهداف تتمثل بما يلي:

**أولاً**. حوكمة الأمن السيبراني الوطني.

**ثانياً**. رصد التهديدات ورسم المعالجات الإستراتيجية والتكتيكية والاستجابة الطارئة.

**ثالثاً**. إعداد الخطط الإستراتيجية ضمن محاور العمل، وبناء وانشاء مراكز خدمات الحكومة الالكترونية ضمن مواصفات ومعايير أمن سيبراني رصين.

**رابعاً**. بناء القدرات وتهيئة الكوادر المتخصصة بالإضافة إلى زيادة الوعي الوظيفي للعاملين.

**خامساً**. التوعية الاجتماعية وحماية الأسرة والطفل للتعامل مع الخدمات الرقمية المختلفة.

**سادساً**. تنشيط الدور الأكاديمي ومراكز البحث والتطوير.

**سابعاً**. تفعيل شراكات إستراتيجية على المستوي المحلي مع القطاعات الحكومية والخاصة.

**ثامناً**. تشجيع الصناعات المحلية والابتكارات.

**تاسعاً**. فحص وتدقيق الأجهزة والبرامج الالكترونية المنتجة والمستوردة لمطابقة معايير سلامة الأمن السيبراني.

**عاشراً**. تفعيل التعاون على المستوى الوطني والإقليمي والدولي.

## هـ- نطاق تطبيق الإستراتيجية وصلاحية التنفيذ

إن نطاق تطبيق هذه الإستراتيجية يستهدف مؤسسات القطاع العام و الخاص ويشمل كذلك الفرد والمجتمع العراقي، ويكون صلاحية تنفيذها من قبل مركز الأمن السيبراني الذي سيتم تشكيله بواسطة الجهات الأمنية ذات العلاقة للفترة الزمنية الممتدة بين الأعوام ٢٠٢٢-٢-٢٠٢٥ ضمن الخطة المعدة لتغطية متطلبات رفع مستوى الأداء وتذليل التحديات وتقليل المخاطر المتعلقة بالأمن السيبراني على المستوى الوطني والإقليمي والدولي.

من الجدير بالذكر، أن هذه الإستراتيجية سوف يتم مراجعتها وتحديثها وتطويرها وفقا للمستجدات في مجال الأمن السيبراني بالاعتماد على مؤشرات التقييم والمراقبة والتحديات اثناء تطبيق المبادرات والبرامج، ومقترحات الخبراء الوطنين والدوليين بشكل يحافظ على أهدافها ويحقق غاياتها بالاستعانة بأفضل الممارسات والآليات والمعايير.

# الفصل الثاني

# دراســـة أولية عن الأمن الســـيبراني العراقي

## أ- المقدمة

أنطلاقاً من ضرورات الواقع التي تفرض علينا الاهتمام والتعامل مع الفضاء السيبراني، فإن الحضور الوطني في هذا المجال يعرضه إلى بعد جديد من المخاطر، ولذلك يتم تطوير إستراتيجية الأمن السيبراني العراقي. إن المخاطر السيبرانية من خلال هذه الوثيقة هي وجود تهديد داخل الفضاء السيبراني قد يضر بأمن وسلامة نظم المعلومات وهياكل البنى التحتية المعلوماتية الأساسية، علاوة على ذلك، فإن التهديدات يمكن أن تستغل الثغرات الحالية الموجودة وبشكل يؤثر على سلامة وأمن نظام المعلومات أو شبكات المعلومات أو البنى التحتية وغيرها من المرافق الحيوية الحكومية. حيث يتوجب الإسراع في فهم التهديدات السيبرانية ومدى قابلية التأثير.

## ب- البنى التحتية الحرجة

تعرف البنى التحتية الحرجة كما ورد في وثيقة الإستراتيجية الوطنية لأمن البنى التحتية الحرجة (الحساسة) ب" الأصول والمرافق الحيوية التي يمثل تدميرها او تعطيلها لأسباب طبيعية أو من صنع الإنسان بضمنها الإرهاب و المخاطر التي تهدد الأمن الوطني والتنمية وسلامة المواطنين وسبل معيشتهم" [٢]

ترتبط التهديدات الحالية بالأصول الرقمية بأحد من مؤسسات القطاع العام أو الخاص او المواطن وكما يلي:

**أولاً : قطاع الأفراد:** حيث يعد الحلقة الأهم في هذه الإستراتيجية كونه اللبنة الأساس في بناء مجتمع متمدن، واعي، وحمايته بواسطة محاربة الأفكار المتطرفة والإرهاب والهندسة الاجتماعية.

**ثانياً : قطاع الأمن وفرض القانون:** يشمل المؤسسات الأمنية والقضائية وممتلكاتها للأنظمة والمعلومات الالكترونية.

**ثالثاً : قطاع الطاقة:** يتمثل بمجموعة متعددة من البنى التحتية والخدمات وأجهزة السيطرة الالكترونية في مجالات انتاج وتصدير النفط والغاز، ومحطات توليد وتجهيز الطاقة الكهربائية وشبكاتها.

**رابعاً : قطاع المصارف والخدمات المالية:** يتمثل بالبنك المركزي العراقي، البنوك والمصارف الحكومية والاهلية مزودي الخدمات المالية كمكاتب الصرافة والتحويل المالي، أسوق وأفرع تداول الأوراق المالية، وخدمات الدفع الالكتروني، منظومات الحسابات المصرفية، والتسوق عبر الانترنت.

---

**(٢) وثيقة الإستراتيجية الوطنية لأمن البنى التحتية الحرجة**

**خامساً : قطاع البنى التحتية للاتصالات والمعلوماتية:** وتشمل كل ما له ربط بشبكة الاتصالات السلكية واللاسلكية وشبكات كوابل الالياف الضوئية البحرية منها والأرضية، موانع وشبكات البدالات وافرعها، وشبكات الاتصال المحلية والدولية ومزودي الخدمات الالكترونية والانترنت.

**سادساً : قطاع خدمات الحكومة الالكترونية:** منصات ومواقع وتطبيقات الحكومة الالكترونية، الخدمات التي توجهها الحكومة للمواطن كالأنظمة الالكترونية التي تستخدمها الحكومة في مؤسساتها وقواعد البيانات المركزية والاحتياطية، وأنظمة اصدار البطاقات التعريفية كالجوازات والبطاقة الوطنية الموحدة واجازات السوق وتسجيل المركبات ووثائق المؤسسات الصحية والأكاديميات للدراسات الجامعية والمدرسية والمعاهد.

**سابعاً : قطاع الاعلام والصحافة:** المتمثل بشبكات الاعلام الحكومية والمحلية المرئية منها أو المسموعة أو المقروءة، وحمايتها من ترويج الأفكار الكاذبة او المحرضة.

**ثامناً : القطاعات الأخرى:** ومنها قطاع النقل والقطاع الصحي.

## ج- التهديدات مصادرها وانواعها

**تتعدد مصادر التهديدات وهي الآتي:**

**أولاً : تهديدات خارجية:** وهي تهديدات من قبل جماعات أجنبية تعمل من داخل العراق او خارجه، قد تكون تحت رعاية حكومات أو حماية المافيات الدولية.

**ثانياً : الإرهابيين والجماعات المتطرفة والتكفيرية** : وهي أي جهة سرية أو علنية تلبي زعزعة الاستقرار الأمني والاقتصادي والمادي والاجتماعي للعراق.

**ثالثاً : المخربون** : وهم كل من له نية أو فعل أو نشاط يستهدف البنى التحتية الحرجة بدواعي خبيثة أو تخريبية.

**رابعاً : الشركات الداخلية أو الخارجية الغير ملتزمة بالقانون او العقود النافذة:** وهم شركات القطاع الخاص والعام مسجلة في داخل العراق أو دولية ولا تلتزم بأصول التعاقد وشروطه ومواصفاته ولا تلتزم بالقانون النافذ داخل العراق.

**خامساً :سوء الاستخدام أو جهل المستخدم:** وهو المواطن الذي يجهل الاستخدام السليم للموارد والممتلكات الرقمية العامة.

**أما أنواعها فهي:**

**أولاً: تهديدات تستهدف مؤسسة:** ويندرج ضمنها الآتي :

- **العمليات التخريبية:** وهي التي تتعرض لها المواقع الحكومية ومنها ما يكون مواقع مادية للبنى الحرجة.
- **منع الوصول إلى الخدمات الإلكترونية الحكومية وغير الحكومية:** وهي التي ترتبط بها شبكات الاتصال والربط والاستضافة لهذه الخدمات.
- **الهجوم الإلكتروني المنظم:** ويكون من قبل دول أو جماعات أو افراد ضد أي مؤسسة ضمن البني الحرجة.
- **التدخل الخبيث في أنظمة الكمبيوتر والأجهزة الرقمية الأخرى:** ويشمل الأجهزة الالكترونية والأنظمة العاملة في مؤسسات الدولة.
- **الإرهاب الإلكتروني:** وهو الذي يستهدف التدمير الخبيث للمؤسسات وخدماتها.
- **التهرب الضريبي للخدمات الالكترونية والرشوة :** وهو ما تستخدمه الشركات العاملة في العراق سواء كانت مقراتها محلية أو دولية ولا تتعامل بموجب القانون العراقي النافذ وتسبب اضرار اقتصادية.

**ثانياً: تهديدات تستهدف مجموعة:** ويندرج ضمنها الآتي :

- **غسيل وتهريب الأموال:** وهي أي عملية مالية تندرج تحت تعريف غسيل الأموال وتهريب العملة سواء كانت من أطراف فردية او مجموعات.
- **الجرائم المالية:** ومنها الاحتيالات المالية والابتزاز والرشوة وغيرها من التي تمارس على شبكات الاتصال الدولي والمحلي.
- **سرقة الأصول الفكرية:** وهو أي التعامل مع المواد المادية والرقمية ومخالفة حقوق الطبع والنشر والتجارة .
- **خلق الصراع والعنف المستمر من خلال منصات التواصل الاستراتيجي:** والغرض منه تهيئة المجتمعات لتبني مواقف من شأنها زعزعة الاستقرار الداخلي عبر ترويج الأفكار العنيفة والمحرضة على الكراهية وإساءة استخدام وسائل الاعلام ونشر الأخبار الكاذبة.

**ثالثاً: تهديدات تستهدف فرد** : ويندرج ضمنها الآتي :

- **القرصنة الإلكترونية:** هي أي فعل قد يمس الممتلكات الرقمية للفرد أو اجهزته أو ذاته عبر استخدام شبكات الاتصال.
- **الممارسات الاحتيالية وغيرها من الاحتيالات المالية أو الفكرية:** وهي التي تؤذي الفرد العراقي مادياً او فكرياً عبر استخدام أساليب التخفي والتتبع والتجسس وغيرها.
- **الابتزاز والاستغلال:** ومنها التأثيرات والضغوط المادية تجاه الضحية لدفعه للتعامل بشكل منافي للسلوك السليم والمنطقي والخضوع لتنفيذ الأوامر الضارة بذاته او بالمجتمع.

## د- التأهب الوطني

قام العراق في العقد الأخير بمجموعة إجراءات تتعلق بالأمن السيبراني تضمنت تطوير أنظمة الحوكمة الالكترونية بشكل جذري وتسهيل المعاملات للمواطن وحماية الفرد والمجتمع والمؤسسات من الأحداث السيبرانية وتمثلت هذه الإجراءات بما يلي:-

**أولاً** : في عام ٢٠١٢، أقر مجلس الوزراء العراقي وثيقة "السياسات الإستراتيجية الوطنية وخطة عمل الحوكمة الالكترونية العراقية (٢٠١٢ – ٢٠١٥)"، وكذلك وثيقة "إطار التخاطب البيني للحكومة والتصميم المعماري للمؤسسة الوطنية".

**ثانياً** : أطلق العراق في خريف ٢٠١٢ وثيقة "السياسة الوطنية لأمن الاتصالات والمعلومات"، حيث وضح فيها عددا من المفاهيم الأساسية لسياسات أمن الاتصالات والمعلومات وأبرز فيها التحديات، المتطلبات، التعليمات، والإجراءات الوطنية؛ بالإضافة إلى الملاحق الفنية ذات العلاقة.

**ثالثاً** : تم تشكيل اللجنة الفنية لأمن الاتصالات والمعلومات من قبل مجلس الأمن الوطني في عام ٢٠١٥ لغرض إدارة الأمن السيبراني العراقي بمختلف محاوره ومستوياته.

**رابعاً** : تم تأسيس الفريق الوطني للاستجابة للأحداث السيبرانية العراقي CERT في عام ٢٠١٧، الذي تشكل من فريق من المختصين في المجال التقني من مختلف المؤسسات الحكومية ذات العلاقة. ان فريق CERT العراقي يمثل سلطة موثوقة تعزز من قدرة العراق على الاستجابة لحوادث الأمن السيبراني.

**خامساً** : بذل العراق جهودا كبيرة في انشاء قاعدة واسعة من مسودات التشريعات السيبرانية، تم وضعها من قبل مختلف المؤسسات الحكومية ذات العلاقة، واللجنة العليا للحوكمة الالكترونية، والتي تتعلق بالجرائم السيبرانية وحماية

البيانات ذات الطابع الشخصي، على سبيل المثال (قانون الجرائم المعلوماتية ، قانون الاتصالات والمعلوماتية، وقانون حماية الخصوصية ، واقرار قانون التوقيع الالكتروني والمعاملات الالكترونية).

**سادساً:** تم وضع مسودة وثيقة "سياسات ومعايير امن المعلومات ومشاركة البيانات" في عام ٢٠١٩، لغرض تحديد قواعد السلوك اللازمة لتوفير الحد الادنى من ضوابط الأمن السيبراني بناءاً على المعايير العالمية والتوصيات الدولية التي تم اقرارها بموجب قرار الامن الوطني.

**سابعاً:** أقر مجلس الوزراء في ربيع ٢٠٢٠ وثيقة "الإستراتيجية الوطنية لأمن البنى التحتية الحرجة الحساسة"، بتعريف البنى التحتية الحساسة والمخاطر والتهديدات وآليات إدارة المخاطر والمراقبة.

## هـ- التحديات ومواطن الخلل

**اولاً. القوانين النافذة:** أن القوانين الرادعة للأفعال المرتبطة بالجرائم الالكترونية ضمن السلطة القضائية مستندة على قانون العقوبات العراقي – رقم ١١١ لسنة ١٩٦٩. حيث تم تجريم الأفعال الضارة تجاه الأشخاص لعمليات الابتزاز، الاحتيال، الخطف وغيرها. من الواضح أن هذه القوانين قد شرعت منذ فترة طويلة وفي فترة لا تتوفر فيها عناصر الجريمة الالكترونية، إلا أن المشروع العراقي بالتعاون مع السلطة القضائية لم يترك الأمر دون عقاب. وقد حرص السلطة التشريعية على تبويب هذه الجرائم الالكترونية ضمن المواد النافذة مثل جرائم التهديد في المواد ٤٣٠ و٤٣١، جرائم القذف في المادة ٤٣٣، جرائم السب في المادة ٤٣٤، جرائم افشاء السر في المواد ٤٣٧ و ٤٣٨، و جرائم الاحتيال في المادة ٤٥٦. حيث لابد من إيجاد قوانين رادعة تتماشى مع تقدم التكنولوجيا واختلاف الدليل المادي كونه أصبح الكتروني في هذه الأيام. كما لا يخفى، أن من أصعب المهمات التي تلقى على عاتق السلطة القضائية هو التعامل مع الدليل الالكتروني الذي قد يفقد فعاليته مع تقادم القضية او مع تأخر المجني عليه في الإبلاغ. حيث لابد من وجود آلية توعية للمواطن بأهمية الدليل الالكتروني ومدى فعاليته إذا ما تم الحصول عليه في وقت مبكر.

**ثانياً.مركزية الإدارة لأمن المعلومات والبيانات والفضاء السيبراني:** أن عدم وجود مركزية في التعامل مع القضايا السيبرانية قد خلق فراغاً تنظيمياً في عملية الرصد والمتابعة وتوفير الموارد، إذ بات ضرورياً إنشاء تشكيل وطني يتولى التنسيق مع الجهات المتعددة المصلحة تحت مظلة وطنية واحدة لإعداد الاستراتيجيات والممارسات الضرورية لخلق أمن وفضاء سيبراني متزن ومحمي.

**ثالثاً.الكوادر المختصة:** إن توافر الكوادر المختصة والمهتمة بالعلم الحديث للأمن السيبراني بالإضافة إلى توافر فرص الهجرة لهذه الخبرات، قد أدى إلى قلة بالغة الأثر في إمكانيات المؤسسات على إدارة وتعامل كوادرها بالقضايا المتعلقة بالأمن السيبراني. هذا بالإضافة إلى قلة التخصيصات المالية والخطط الإستراتيجية في مجال تكنولوجيا المعلومات أدى إلى ندرة وجود مناهج اكاديمية ودورات تدريبية مختصة بهذا المجال توجه نحو المهتمين والموهوبين.

**رابعاً.البنى التحتية:** أدت عمليات اعمار العراق ما بعد ٢٠٠٣ إلى التوجه نحو الخدمات الأساسية وعدم التفاعل مع المتطلبات الحديثة لمواكبة التقدم التكنولوجي. حيث أصبح العراق اليوم في مرحلة حرجة لإيجاد وبناء مؤسسات اكاديمية وانشاء بنايات بمواصفات محددة لإستضافة وتشغيل الخدمات والتطبيقات للحكومة الالكترونية و خدمات عامة والسيطرة على تمرير حزم الانترنت للمواطنين وبأسعار تضمن توافره وتوفيره.

**خامساً.مستوى الوعي العام:** إن الفضاء الالكتروني للخدمات والتطبيقات ذو مساحة واسعة من اهتمام المجتمع العراقي، وكما فيه الكثير من الإيجابيات فهو يحمل الاخطار كذلك. لذا يتوجب زيادة توعية المجتمع والفرد تجاه الأفكار والمخاطر التي يمكنها الوصول اليه والتأثير على مستواه المنطقي واستغلال ممتلكاته الرقمية والشخصية لحمايته فهو النواة الأساسية في بناء المجتمع وتطور حضاراته. حيث تتوافر على منصات التواصل الاستراتيجي الكثير من المواد المتطرفة والإرهابية والأشخاص المتصيدين لقليلي الوعي عبر ابتزازهم واستغلال عدم تواصلهم مع الجهات المعنية في السيطرة وفرض القانون.

**سادساً.التفاعل الدولي:** يعد العراق ذو طابع سياسي معتدل يعمل على خلق صداقات والالتزام بخطوات إستراتيجية للتفاعل مع المجتمع الدولي. الا أنه ما زال لا يملك الاتفاقيات الثنائية مع الأطراف الإقليمية والدولية والعقود الإستراتيجية مع القطاع الخاص الدولي لتفعيل عمل حماية الأمن السيبراني.

## و- التأثير والفرص

إن تطبيق الأمن السيبراني في مجال الفضاء الإلكتروني العراقي لابد أن يساعد البلد على الاستعداد والاستجابة لهذه التهديدات الأمنية والمساعدة على معالجة ضعف البلد في المجال الرقمي، فضلا عن تعزيز قدرتنا على توفير تدابير مضادة بالاشتراك مع جهات فاعلة شرعية وغير حكومية أخرى. حيث يعد هذا الأساس المنطقي الاستراتيجي لوضع الأسس الوطنية للأمن السيبراني والسياق السليم لتعريف إستراتيجية الأمن السيبراني العراقي من أجل الاستعداد للأمن القومي.

أن مساعي الحكومة العراقية في السنوات القليلة الماضية لإطلاق خدمات الحكومة الالكترونية يجب أن يتوازن وإيجاد آليات للمحافظة على المعلومات، حيث أن مزايا الخدمات الالكترونية الوطنية التي توجه نحو المواطن وفي داخل مؤسسات الدولة لها المردود الاقتصادي والتقني الكبير في تسريع عمليات إنجاز المعاملات وتحقيق الرفاهية للمواطن تجاه حقوقه التي

كفلها الدستور العراقي له. وله الأثر من جانب أخر في تسريع دوران عجلة التطور للاقتصاد العراقي الذي أدخل الأتمتة الالكترونية في بناء البنية التحتية الحرجة وخصوصاً منها النفط والطاقة.

ان السيطرةعلى المرافق السيبرانية وضمان امنها له مردودات اقتصادية تساهم في النتاج القومي تتمثل بتقليل الاضرار الاقتصادية من خلال عمليات عديدة منها غسيل الأموال والإرهاب وتهريب الوقود والتهرب الضريبي للخدمات الالكترونية وتجارة المنافذ الحدودية البرية والبحرية. بالإضافة إلى احتضان المجتمع الدولي مستقبلا للعراق كبلد مسيطر على موارده وحدوده المادية منها والالكترونية وذو ثقة تستحق أن يكون ضمن خطط النقل الالكتروني والربط على الشبكات الدولية للخدمات الالكترونية. كما إن التقليل من مخاطر التهديدات وآثارها عند حصولها قد يفتح باب الاستثمار والإقبال للشركات العالمية للعمل في بيئة العراق الإلكترونية في قطاعات صناعة الطاقة وتكنولوجيا المعلومات.

# الفصل الثالث

# خريطة طريق التنفيذ

## أ– المقدمة

اعتمدت خريطة الطريق على تقسيم مراحل التنفيذ الى ثلاث مراحل رئيسية فمنها التنظيم والتخطيط ومنها النهج الإستراتيجي واخيراً التقييم والمتابعة. علما أن الأدوار والمسؤوليات قد تم تفصيلها في وثيقة سياسات ومعايير أمن المعلومات ومشاركة البيانات.

## ب– المرحلة الأولى: التنظيم والتخطيط

ويتضمن ما يلي :

### اولاً. دراسة واقع الحال ومسح الجهوزية

تقديم دراسة من واقع الحال للأمن السيبراني في العراق من خلال عمل استبيان وقياس المؤشرات الوطنية لمسح جهوزية المؤسسات في القطاع الحكومي والخاص وتحديد مواطن الضعف للموجودات الرقمية عن طريق تعريفها وحصرها وتصنيفها الى عدة مستويات منها حرجة، او ضرورية، او تكميلية.

### ثانياً. تحليل الدراسة

إعداد آلية لتحليل نتائج الأستبيان ولوضع اليات تنفيذية دقيقة يمكن الاستفادة منها في خطة التنفيذ الفعلية، كما يتم إعداد ملف الإستراتيجية التنفيذي والذي يتضمن دراسات الجدوى بما يتعلق بالأمن السيبراني، هيكل التنفيذ الأعمال والمدة الزمنية، والكلف التخمينية والدراسة المالية، وتحديد آليات التمويل المادي والطاقات البشرية.

### ثالثاً. إعداد الهيكل التنظيمي والحوكمة الفعالة

نظراً للظروف و الحاجة الماسة إلى إيجاد إدارة مركزية عليا تعتني بتطبيق الإستراتيجية وتحرص على متابعة التنفيذ وتذليل الصعوبات والعقبات لتوفير الموارد المالية والكوادر البشرية لإنجاح إتمام العمل بها، لا بد من إنشاء تشكيل يتولى تفعيل وتقسيم وإقرار المسؤوليات والواجبات وتحديثها بما تتطلبه أولويات النجاح لتنفيذ هذه الإستراتيجية.

### رابعاً. إعداد وتهيئة الهيكل التنفيذي

يعد التشكيل الوطني هو صاحب الادارة في الهرم التنفيذي والذي يتكون من عدة لجان وفرق ومؤسسات معنية من القطاعات الحكومية والخاصة، وتتولى العمليات الضرورية بما يخص خطة التنفيذ وتدريب وتأهيل الكوادر المعنية لتطبيق الخطوات المطلوبة وتحت معايير وإرشادات متخصصة.

### خامساً. إعداد وتحديث السياسات والتعليمات

تكلف اللجنة المشكلة الإعداد وثيقة سياسات ومعايير أمن المعلومات ومشاركة البيانات بالتعاون مع الفريق الوطني لاستجابة للأحداث السيبرانية، او من ينوب عنهما مستقبلا بمهمة إعداد مجموعة من الأطر والممارسات الخاصة بسلامة الأمن السيبراني وما يتطلب من ملاحق لتوضيح سقف المعايير الفنية ووضع الارشادات الإدارية المطلوبة. حيث تعتمد آلية إعداد المعايير على المتطلبات العالمية التي تختص بالأمن السيبراني ومنها ISO NIST، وCobit 5.بالاستناد على المعايير العالمية، يتم إعداد التقرير الوطني للمعايير والارشادات ويتم تحديثه بشكل دوري للوصول إلى أفضل الممارسات في الأمن السيبراني من خلال استخلاص التجارب الدولية والضروريات التقنية لتفادي المستجدات التكنولوجية في تطبيق هذه المعايير وعكسها بشكل يتناسب ووضع العراق في استحداث الأنظمة الالكترونية وحسب تطبيقها في القطاعات المختلفة.

### سادساً.الترويج والاستعداد

من خلال هذه المرحلة يكون التعاون مع أصحاب الجهات ذات المصلحة والعلاقة كلُ حسب تخصصه، يتم تنفيذ برنامج الترويج الإعلامي والطباعة والنشر الإستراتيجية للأمن السيبراني وملحقاتها من سياسات وإرشادات وتعليمات وغيرها من الملاحة الداعمة ويتضمن بالإضافة الى المواد الدعائية، عقد ورش عمل ومؤتمرات للمختصين والشركاء الوطنين في القطاع الحكومي والخاص لمناقشة الإستراتيجية وتبادل الخبرات.

## ج– المرحلة الثانية: النهج الإستراتيجي

ويتضمن ما يلي :

### اولاً. الاستجابة الطارئة

تتضمن خطة المعالجة الفورية، حيث يتولى الفريق الوطني للاستجابة للأحداث السيبرانية والجهات الأخرى ذات العلاقة كل حسب تخصصه، تنفيذ التدابير والإجراءات لسد الفجوة الأمنية السيبرانية في البنى التحتية الحرجة ومعالجة أوجه الضعف الأساسية فيها.

### ثانياً. البرامج الإستراتيجية

تتألف من عدة محاور وتنقسم إلى ما يلي:

- **المحور التشريعي**: الذي يهتم بوجود مؤسسات تشريعية ومعطيات قانونية تختص بالتعامل مع الأمن السيبراني من خلال تحسين القوانين الحالية الخاصة به وتشريع قوانين سيبرانية جديدة لغرض تعزيز الوضع القانوني للأمن السيبراني العراقي وفرض العقوبات الرادعة على عدم الامتثال أو خرق القانون.

إن الهدف الأساسي من هذا المحور هو أن يكون هناك تشريعاً كافياً للتنسيق والممارسات على المستويات الداخلية والإقليمية والدولية وتبسيط الإجراءات القانونية تجاه الجرائم الإلكترونية والسيبرانية لغرض الإسراع في الاستجابة الفورية لدرء المخاطر. من أهم هذه القوانين التي يتولى متابعتها التشكيل الوطني بالتعاون مع المختصين في الجهات القانونية والتشريعية والأكاديمية في كليات الحقوق والقانون متابعة تطبيق قانون الجرائم المعلوماتية ومدى فعالية قانون التوقيع الالكتروني والمعاملات الالكترونية وقانون الاتصالات والمعلوماتية وقانون حماية الخصوصية وغيرها من البرامج التي تتضمن بشكل عام :

- ❖ **برنامج تحديث التشريعات:** مراجعة وتحديث القوانين الرقمية العراقية الحالية (ان وجدت) لغرض معالجة الطبيعة الديناميكية للتهديدات التي تواجه الأمن السيبراني العراقي.
- ❖ **برنامج اصدار القوانين الرقمية:** تشريع قوانين رقمية جديدة لغرض تعزيز الوضع القانوني الرقمي العراقي وحماية وردع التهديدات ضد البنية التحتية الحرجة.
- ❖ **برنامج التشريعات الدولية:** التأكد من أن جميع التشريعات المحلية المعمول بها تتكامل وتنسجم مع القوانين والمعاهدات والاتفاقيات الدولية.

- **المحور الفني:** تعد التكنولوجيا العنصر الأساسي للدفاع ضد التهديدات السيبرانية (بما في ذلك استخدام فرق الطوارئ أو الاستجابة للحوادث، أطر تنفيذ المعايير العالمية، التقنية والأليات والقدرات التي تم اعتمادها لمعالجة الرسائل الاقتحامية وحماية الأطفال عبر الإنترنت وما إلى ذلك)، حيث يتابع هذا المحور من التنقية، بناء وتثبيت معايير الحد الأدنى للأمن، خطط الاعتماد المقبولة لتطبيقات وأنظمة البرمجيات، وما يتوجب لتنفيذ هذه الجهود من خلال توحيد الجهود الوطنية لمراقبة الحوادث والتحذير منها والاستجابة لها.

يتضمن هذا المحور متابعة المصادقة وتطبيق وثيقة سياسة أمن المعلومات ومشاركة البيانات وتحديث الملاحق الفنية بما يتوافق ولضرورة حماية الأمن السيبراني، كما يتضمن بناء وانشاء وتطوير المؤسسات التكنولوجية الإستراتيجية ومنها:

- ❖ **برنامج حماية البنى التحتية الحرجة:** وهو برنامج يعد بالتوافق مع متطلبات مسودة الإستراتيجية الوطنية لأمن البنى التحتية الحرجة، حيث يغطي الجانب التقني والمتطلبات الرقمية لرفد عملية الحماية وتقليل أثار المخاطر.
- ❖ **برنامج الأمن والدفاع السيبراني:** يعنى بالعمليات والممارسات الاستباقية التي تضمن تأمين وحماية المؤسسات ضد أي نوع من أنواع الهجمات السيبرانية.

- ❖ **مركز البيانات الوطني**: انشاء مركز بمواصفات عالمية لاستيعاب المنظومات والأجهزة الالكترونية التي تتولى إطلاق خدمات الحكومة الالكترونية .
- ❖ **مراكز الفضاء والدليل الرقمي**: لمتابعة وتحليل الدليل الالكتروني بالتعاون بين الأجهزة الأمنية والمؤسسة القضائية.
- ❖ **مركز الشفرة الوطني**: لصناعة خوارزميات التشفير تحت إدارة وطنية لإيجاد أدوات وطنية لمواجهة التهديدات التقنية وحماية المعلومات والبيانات.
- ❖ **مركز المراقبة والتحليل السيبراني SOC**: لرصد وتحليل واستجابة الأحداث السيبرانية.
- ❖ **مركز المعلومات الجغرافي**: لإيجاد آلية تعاون بين مراكز المعلومات الجغرافية في الأجهزة الأمنية المختصة.

- **المحور التنظيمي**: يختص بآليات التنفيذ السليم لأي مبادرة وطنية من شأنها التأثير على سلامة أمن المعلومات والبيانات والأمن السيبراني بشكل عام ، ومن خلاله يتم متابعة الغايات والأهداف الإستراتيجية التي تحددها الدولة، إلى جانب الخطة الشاملة في التنفيذ ، كما يتم قياس مدى تفاعل القطاعات الأخرى فيما بينها ومدى فعالية التنسيق بين المؤسسات التنظيمية المعنية في تطوير الأمن السيبراني.

يتولى التشكيل الوطني تقييم أداء الهياكل التنظيمية على أساس وجود المؤسسات والاستراتيجيات التي تنطوي على تطوير الأمن السيبراني على المستوى الوطني والدولي.

من أهم البرامج عبر هذا المحور هو **برنامج أمن الحوكمة والحكومة الإلكترونية** الذي يوفر رؤية لمخاطر العمل في المؤسسات الحكومية استنادا إلى التهديدات الإلكترونية، والتي تساعد في عمليات مراقبة الامتثال وتحسين الوضع الأمني السيبراني العام للمؤسسات، كما يعد النواة الأساسية لممارسة الشفافية والنزاهة المتعلقة بالأمن السيبراني عبر استخدام وتطوير المفاهيم الأساسية وتحديث المتطلبات الإدارية والفنية بشكل مستمر لتقييم التهديدات الإلكترونية وإدارتها ومعالجتها بشكل أفضل.

- **محور بناء القدرات**: يعد محور بناء القدرات (بما في ذلك حملات التوعية العامة، وإطار الدراسة الأكاديمية واعتماد المتخصصين في الأمن السيبراني، ودورات التدريب المهني في مجال الأمن السيبراني، البرامج التعليمية أو المناهج الأكاديمية، وما إلى ذلك) جزءا لا يتجزأ من الركائز الثلاث الأولى (القانونية والتقنية والتنظيمية)، حيث يتم متابعة العديد من الآثار الاجتماعية والاقتصادية والسياسية عن طريق القدرات البشرية وما لها من تأثير سريع لرفع مستوى الوعي والمعرفة والدراية عبر القطاعات، وإعداد وتطوير المهنيين المؤهلين في المؤسسات الحكومية، و من اهم هذه البرامج ما هو متعلق بالاستجابة الفورية، بناء القدرات، والتوعية، وهي الآتي :

- ❖ **برنامج البحث العملي والتطوير الذاتي**: يعد مركز البحث والتطوير اللبنة الأساسية لأنطلاق العديد من البرامج وتحليل مخرجاتها، وهذا يتطلب توفير قدرات مختصة لتوفير التقييم والتقويم الأساسي في التوجهات الإستراتيجية

في الأمن السيبراني الوطني، حيث يتولى التشكيل الوطني التنسيق مع وزارة التعليم العالي والبحث العلمي عبر الجامعات، المؤسسات الأكاديمية، مراكز البحث والتطوير، مراكز الدراسات والمعاهد المختصة في تعزيز اليات البحث والتطوير والاستشارات العلمية.

- ❖ **برنامج إعداد فرق الاستجابة المحلية في المؤسسات CCERT**: ويكون هذا البرنامج جزء داعم للفريق الوطني للاستجابة للأحداث السيبرانية داخل المؤسسات المختلفة لغرض التواصل الفعال تجاه الأحداث السيبرانية و تطبيق سياسة و معايير أمن المعلومات و مشاركة البيانات ويكون لكل مؤسسة مدير أمن معلومات (CISO) يختص بأمنها ويقوم بالتنسيق مع فريق ال(CERT) الرئيسي.
- ❖ **برنامج التدريب والتطوير المهني للهواة والمحترفين في الأمن السيبراني**: يساهم هذا البرنامج في إعداد القادرين على استخدام الأدوات المحترفة ذات الضرورة في عمليات التصدي والتحليل والهجوم بما يخص الأمن السيبراني ليكونوا داعمين، وتحت رعاية الفريق الوطني للاستجابة للأحداث السيبرانية.
- ❖ **برنامج تدريب الجهات التنفيذية لمتابعة ومعالجة الجرائم السيبرانية** تتولى الجهات التنفيذية في أجهزة امن الدولة والجهات المختصة تطوير كوادرها بما يختص بعمليات الأمن السيبراني ومعرفة استخدام أدوات التحقيق الجنائي الرقمي وكيفية الأستجابة للأحداث والتعامل معها.
- ❖ **برنامج التوعية الوظيفي للممتلكات الرقمية العامة** وهو جزء من آليات تطبيق سياسة ومعايير أمن المعلومات ومشاركة البيانات ، وتدريب كوادر موظفي القطاع الحكومي والخاص تجاه أهمية الممتلكات الرقمية والممارسات السليمة للتعامل معها والحفاظ عليها.
- ❖ **برنامج التوعية الاجتماعي حول الأمن السيبراني**: من الضروري استهداف فئات عمرية مختلفة من المجتمع لغرض التوعية تجاه الممتلكات الشخصية الالكترونية وآليات التعامل السليم تجاه البوابات الرقمية للحكومة الالكترونية والتعامل مع الجهات المختصة في قضايا الاحتيال والابتزاز والانتحال.

- **محور التعاون الدولي:** يضم الاتفاقات الثنائية والمتعددة الأطراف، ومشاركة المنظمات الدولية كالمنتديات والجمعيات، والشراكات بين القطاعين العام والخاص، والشراكات بين الوكالات، وأفضل الممارسات.

لا يخفى عن الذكر ما يمكن أن يتيح التعاون الدولي في تطوير قدرات أقوى للأمن السيبراني وما قد يساعد على ردع تهديدات متكررة ومستمرة على شبكات الإنترنت عن طريق التمكين من إجراء التحقيق وفرض القانون والعدالة، ويحوي هذا المحور على عدة برامج هي الآتي:-

- **برنامج المشاركة الفعالة:** تشجيع المشاركة الفعالة مع معظم هيئات الأمن السيبراني الدولية والإقليمية ذات الصلة، والفرق والوكالات المتعددة الجنسيات.
- **برنامج النشاطات الدولية:** تعزيز المشاركة الفعالة في جميع الفعاليات والمؤتمرات والمنتديات الدولية المتعلقة بالأمن السيبراني. كذلك تعزيز الموقع الاستراتيجي للعراق ضمن التقييم العالمي في مجال الأمن السيبراني من خلال استضافة مؤتمرات دولية دورية في مجال الأمن السيبراني.
- **برنامج الشراكات الدولية:** العمل على تكوين شراكة واتفاقيات بين الفريق الوطني للاستجابة للأحداث السيبرانية وفرق الاستجابة الالكترونية الدولية الأخرى لأجل تطوير الفريق وتوسعة أفقه.
- **برنامج التعاون مع مصنعي التكنولوجيا:** تفعيل شراكات إستراتيجية مع مصنعي التكنولوجيا للأجهزة والبرمجيات والخدمات في العالم.

## د- المرحلة الثالثة : التقييم واصدار التوصيات

### اولاً. التقييم والمتابعة عبر المؤشر الوطني

إعداد المؤشر الوطني الموازي للمؤشر العالمي ((Global Cybersecurity index (GCI المقدم من قبل الاتحاد الدولي للاتصالات (ITU)، والذي يعرف بمؤشر الأمن السيبراني الوطني ((National Cybersecurity Index (NCI لإيجاد آليات فحص وقراءة مؤشرات السلامة الرقمية في مختلف القطاعات، حيث يحتوي التقرير على مؤشرات مختلفة منها دولية تعنى بقياس نسب الوعي والإجراءات المتخذة تجاه التوصيات الدولية بما يخص الأمن السيبراني على مختلف تخصصاتها القانونية، التقنية، التنظيمية، بناء القدرات، والتعاون الدولي. ومنها أيضا مؤشرات وطنية، والتي تقسم إلى المؤشرات الداخلية وما يرتبط بها من وعي وظيفي تجاه الملكية الرقمية العامة والتهديدات ذات العلاقة، والمؤشرات الاجتماعية التي تستهدف قياس تأثير مخرجات الجهود الحكومية تجاه زيادة الوعي للفرد داخل المجتمع بما يتعلق بالمعلومات الشخصية الرقمية والخدمات التي تقدمها الحكومة الالكترونية وما يليه من تأثير على مستويات الأجرام الرقمي ومنها الابتزاز الإلكتروني، والاختراقات التقنية، والاحتمالات المالية وغيرها.

### ثانياً. إعداد تقرير التنفيذ

يتم إعداد تقرير دوري يختص بمتابعة وتنفيذ مخرجات القياس للمؤشرات الوطنية، وإعداد خلاصة حول ما تم تحقيقه، وما هي أفضل الممارسات في التطبيق، والمتطلبات المستقبلية للمحافظة على سير الخطة.

## ثالثاً. تطبيق سياسات التغيير والتطوير

من ضمن إطار المرحلة الرابعة، إعداد وتحديث السياسات والتعليمات، حيث يتم إعداد سياسة التغيير والتطوير والمحافظة على سير العمل في هذه المرحلة ما قبل الأخيرة، والذي يتطلب من التشكيل الوطني مراجعة نتائج التقييم الدوري وإعداد خلاصة متطلبات للتغيير في خطة التنفيذ للمحافظة على تحقيق أهداف الإستراتيجية.

## رابعاً. الإستراتيجية المستقبلية

يتولى التشكيل الوطني عن طريق استخلاص الدروس والعبر والتحديات المستحدثة في إعداد تقرير الاغلاق للإستراتيجية الذي يتضمن عدد من التوصيات وأفضل الممارسات التي حقق نجاحات في الواقع الأمني السيبراني.

# إستراتيجية الأمن السيبراني العراقي


فريق الإستجابة للأحداث السبرانية