استراتيجية الامن السيبراني العراقي

مستشارية الامن الوطني
امانة سر اللجنة الفنية العليا لأمن الاتصالات والمعلومات

المحتويات

(١) لمحة عامة عن الاستراتيجية الوطنية السيبرانية

١,١ مقدمة:

- الاستراتيجية الوطنية للأمن السيبراني هي استراتيجية الاستعداد الوطني لتوفير تدابير متماسكة وإجراءات استراتيجية لضمان أمن وحماية الوجود العراقي في الفضاء السيبراني، وحماية البنية التحتية الحيوية للمعلومات، وبناء ورعاية مجتمع إنترنت موثوق به.
- عادة، تتألف استراتيجية الامن السيبراني الوطنية من عدة استراتيجيات قصيرة ومتوسطة وطويلة الامد تغطي جميع الأولويات الوطنية، وتعالج التعرض الوطني للمخاطر السيبرانية. هنالك تهديدات سيبرانية رئيسية في جميع أنحاء العالم التي تضر بالمصلحة الوطنية. مثل؛
  - الجريمة الإلكترونية
  - الإرهاب الإليكتروني
  - الصراع السيبراني
  - التجسس السيبراني
  - إساءة معاملة الأطفال واستغلالهم عبر الإنترنت.

- لهذه التهديدات قدرة كبيرة على الإضرار بسلامة الأمة، وتعطل عمليات البنية التحتية الحيوية للمعلومات، وتقويضها والعمليات الحكومية، والأمن القومي.
- تقوم استراتيجية الامن السيبراني الوطني بتحديد وتنسق وتوجه البلد في تنفذ الساسة الوطنية للأمن السيبراني واخذ تدابير متماسكة وإجراءات مضادة ضد التهديدات السيبرانية من أجل تامين وحماية ودفاع الفضاء الإلكتروني الوطني.
- الاستراتيجية تقدم مبادرات مختلفة في المجالات المركزة عليها والآليات الوطنية لوضع وتنفيذ الحكومة الفعالة, الإطار التشريعي والتنظيمي, إطار تكنولوجيا الأمن السيبراني, ثقافة الأمن السيبراني وبناء القدرات, البحث والتطوير نحو الاعتماد على الذات, الامتثال والتنفيذ للقوانين والسياسات الموضوعة, الجاهزية لحوادث الامن السيبراني و التعاون الدولي.

١,٢ الرؤية الوطنية لألمن السيبراني:

وقد حددت الاستراتيجية الوطنية للأمن السيبراني غرضا واضحا واتجاها ثابتا , فما هي رؤية الأمن السيبراني في العراق؟ مجتمع آمن ومضمون ونابض بالحياة ومرن وموثوق به يوفر فرصا لمواطنيه ويحمي الأصول والمصالح الوطنية ويعزز التفاعلات السلمية والمشاركة الاستباقية في الفضاء السيبراني من أجل الرخاء الوطني.

١,٣ . هدف الاستراتيجية الوطنية للأمن السيبراني:

والهدف من هذه الاستراتيجية هو توفير خارطة طريق متماسكة ومبادرات وآليات لتنفيذ و لتحقيق الرؤية الوطنية بشأن الأمن السيبراني.

١,٤ الفضاء السيبراني في سياق الرخاء الوطني والفرص:

- يوفر الفضاء السيبراني منصات وفرصا ممتازة لتأمين وتنمية اقتصاد البلاد.
- إن كل مواطن مرتبط بالفضاء الإلكتروني عبر الإنترنت يتأثر بشكل لا يمكن تصوره ويسمح له باتخاذ الإجراءات.
- في السنوات القليلة المقبلة، سيصبح العراق اقتصادا نطاقا و عريض حيث سيكون لكل فرد ومواطن حرية الوصول إلى الإنترنت دون عوائق.
- سيصبح الفضاء السيبراني هو الاتجاه السائد لتحقيق التكامل الوطني وتمكين الاقتصاد الرقمي. وهو فضاء مدعوم بالمعرفة مع قدرة هائلة على سد الفجوات في التنقل والتجارة والابتكارات والتعليم والحد من الفقر والتمكين الاقتصادي.

- ما هو الفضاء السيبراني؟

والفضاء السيبراني عبارة عن شبكة مترابطة من الهياكل الأساسية للمعلومات الأساسية الحرجة وغير الحرجة، والذي يعمل على تقريب موارد المعلومات والاتصالات المترابطة من خلال استخدام تكنولوجيات المعلومات والاتصالات. وهو يشمل جميع أشكال

التدخلات الرقمية , التفاعلات والتواصل الاجتماعي ,التخصصات الاجتماعية , أنشطة المعاملات, المحتويات, والاتصالات، والموارد التي يتم نشرها من خلال الشبكات المترابطة.

- لماذا يجب ان يعتبر الفضاء الإلكتروني مهما للحكومة الوطنية؟

وقد ثبت أن لدينا ثلاث (٣) مجالات ومنافذ تستخدم في شتى المجالات وهي الأرض والبحر والجو، لذلك على العراق ان يعتبر مجال الفضاء السيبراني هو مجاله الرابع (٤) لما له من تأثير فعال وواضح في قيادة المهام الوطنية الحرجة مثل التنمية الاقتصادية والتجارة والمعاملات، والتفاعلات الاجتماعية، والطبية والصحية، والعمليات الحكومية، والأمن القومي والدفاع.

١,٥ تأثير المخاطر السيبرانية على الأمن القومي والاقتصاد

- يعتمد الوجود الاقتصادي الرقمي للبلد على الأداء الفعال للبنية التحتية الرقمية. وفي الفضاء السيبراني، فإن البلد ليس معزولا ولكنه مترابط مع بلدان أخرى وجهات فاعلة في الفضاء السيبراني من خلال شبكات مترابطة للبنى التحتية للمعلومات. وبالتالي، فإن البلد معرض لمخاطر يمكن التنبؤ بها و اخرى لا يمكن التنبؤ بها.
- تماما كما لدينا جهات فاعلة ذات نوايا مشروعة، فهناك أيضا جهات فاعلة أخرى ذات نوايا غير مشروعة وخبيثة. داخل الشبكة العالمية للشبكات، توجد عيوب 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 ومما ينعكس سلبا على المواطن وبالتالي على الامن الوطني.
- توجد مواطن ضعف في الفضاء السيبراني يمكن استخدامها لاستغلال المصالح الاقتصادية الوطنية وتشكل تهديدا للأمن القومي. على سبيل المثال،
  - 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 الاعلام 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
  - غسل الأموال،

كلها هذه الأمور لا تنسجم مع سياسة الرفاهية لأي دولة ولها الأثر الاقتصادي الذي يكون كفيل بتدمير أي دولة.

١,٦ الأمن السيبراني في سياق استراتيجية الأمن القومي:

توفير الأمن للبنية التحتية الحيوية للمعلومات وغيرها من العناصر الحرجة في نظام المعلومات في ظل الوضع الراهن هو تحد وطني ضخم. ويحتاج الأمن الوطني إلى إطار متماسك للأمن السيبراني لتوفير نهج شامل إزاء المشهد الأمني الحالي والمستقبلي، لأن أمن الدولة والتضاريس والاقتصاد يسير بخطى سريعة ويتجهان نحو تضاريس متحركة ومتنقلة رقميا. فالجهات الفاعلة الحكومية وغير الحكومية المتورطة في الجرائم السيبرانية مجهزة تجهيزا كافيا بأدوات إلكترونية متطورة تتسبب في أضرار ذات بعد لم يسبق له مثيل. ومن شأن إدراج الأمن السيبراني في مجال الفضاء الإلكتروني 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. وهذا هو الأساس المنطقي الاستراتيجي لوضع السياسة الوطنية للأمن السيبراني والسياق الذي يتم فيه تعريف استراتيجية الأمن السيبراني العراقي من أجل الاستعداد للأمن القومي.

(٢) فهم التعرض الوطني للمخاطر السيبرانية

٢,١ مقدمة

تماشيا مع المبدأ الواقع الذي يفرض علينا الاهتمام والدخول في المجال السيبراني العالمي ، فإن الحضور الوطني في مجال الفضاء السيبراني يعرضه إلى بعد جديد من المخاطر. ولذلك، يتم تطوير استراتيجية الأمن السيبراني العراقي من فحص التعرض لمخاطر الأمن في البلد بأسره.

ما هي المخاطر السيبرانية؟

المخاطر السيبرانية هي احتمال وجود تهديد وهشاشة داخل الفضاء الإلكتروني للبلد يضر بأمن وسلامة نظم المعلومات وهياكل البنى التحتية المعلوماتية الأساسية. وعلاوة على ذلك، فإن التهديدات يمكن ان تستغل الثغرات الحالية الموجودة وبشكل يؤثر على سلامة وأمن نظام المعلومات أو شبكات المعلومات أو البنى التحتية للشبكات.

وللخطر السيبراني الوطني مكونان رئيسيان:

- التهديدات السيبرانية
- مدى كوننا معرضين للهجمات السيبرانية (الثغرات الموجود)

٢,٢ تأثيرات التهديد الإلكتروني:

- ❖ احد التهديدات السيبرانية هو احتمال وجود محاولات لأتلاف أو تعطيل عمليات شبكة الكمبيوتر ونظام المعلومات الضعيفة التحصين.
- ❖ طبيعة وابعاد تأثير التهديد السيبراني تكون متنوعة، وهي تنطوي على مصدر التهديد الذي يقوم قبل الهجوم باستغلال ظروف وقوع حادث او خرق أمنى معين. عادة، مصدر التهديد يبدأ من خلال الرغبة في الاختراق والوصول إلى المعلومات الهامة أو الضوابط الأمنية بهدف الاستفادة من الخرق، على سبيل المثال لتحقيق مكاسب مالية.
- ❖ يتم تصعيد التهديد السيبراني إلى هجوم إلكتروني من قبل جهة التهديد حيث يبذل جهد لاستغلال ضعف أنظمة الكمبيوتر وشبكات المعلومات والاتصالات والعمليات او الخدمات التي تعتمد على الإنترنت من أجل النوايا الإجرامية والاغراض الخبيثة.
- ❖ وعادة ما ينطوي الهجوم الإلكتروني على استخدام برمجيات ضارة لتغيير الرموز البرمجة الرقمية والمنطق الرياضي أو البيانات، مما يؤدي إلى عواقب التخريبية التي يمكن أن تضر بسرية وسلامة وتوافر البيانات وبالتالي تؤدي إلى التلاعب في نظم المعلومات والبنية التحتية للشبكة.
- ❖ قد تؤدي الهجمات السيبرانية إلى العواقب التالية:

• سرقة الهوية، • تزوير، • الابتزاز، • البرمجيات الخبيثة، • تزييف، • والتصيد، • البريد الالكتروني غير المرغوب، • خداع، • برامج التجسس، • وسرقة الملكية الفكرية.	• أحصنة طروادة والفيروسات • التلاعب بالأجهزة، • والحرمان من الخدمة • خرق الوصول، • سرقة كلمة المرور، • نظام التسلل، • تشويه الموقع، • يستغل متصفح الويب الخاص والعام، • الرسائل الفورية وإساءة استخدام وسائل الاعلام والتواصل الاجتماعية،

❖ **مصادر التهديد السيبراني**
- الدول الأجنبية
- النقابات الجنائية المنظمة
- الإرهابيين و الجماعات المتطرفة
- الهاكرز
- الشركات

❖ وكما مبين في السياسات الأمن السيبراني الدولي فان هنالك خمسة (٥) تهديدات سيبرانية رئيسية (المذكورة اعلاه) تعتبر على أنها مخالفة لاستراتيجية الأمن الوطني لأي دولة. ولهذه التهديدات قدرة كبيرة على إحداث أضرار جسيمة لسلامة اقتصاد البلد.
❖ تتمثل الأيديولوجية الأساسية لهذه الاستراتيجية الوطنية للأمن السيبراني في تقديم الأطر والآليات الاستراتيجية ذات الصلة لمعالجة هذه التهديدات السيبرانية وتأمين الأمة في مجابهة الهجمات السيبرانية.

٢,٣ ضرورة تقييم مواطن الضعف الوطنية

❖ الثغرات هو الضعف الهيكلي لنظم المعلومات في البلاد والبنية التحتية الحيوية للمعلومات التي تتراوح بين العيوب التقنية، والتدابير الغير مدروسة، والإهمال البشري.
❖ تتطلب الاستراتيجية الوطنية للأمن السيبراني إجراء تقييم على مستوى الدولة كاملا من أجل تحديد نقاط الضعف في نظم المعلومات الحكومية، والمواقع الشبكية، والشبكات، وعمليات معالجة البيانات، وكذلك مواطن الضعف الموجودة في البنية الأساسية للمعلومات الحيوية للبلد.
❖ ويساعد تقييم الضعف الوطني الحكومي على تقدير مستوى عدم استعدادها، والحاجة إلى حماية البنى التحتية المعلوماتية والبنية الأساسية للاتصالات.
❖ **الهدف من الاستراتيجية** هو بناء آليات لأخذ الإجراءات المضادة التي من شأنها أن تيسر قدرة البلد على معالجة الثغرات الهائلة في مواطن الضعف بين نظم المعلومات، والبنية التحتية الحيوية للمعلومات، وحماية وجودنا المستقبلي في الفضاء السيبراني.
❖ هناك جهود تهدف إلى معالجة بعض هذه التحديات على المستويات الوزارية من خلال فريق الاستجابة للحوادث الاليكترونية العراقي. ومع ذلك، فإن استراتيجية الامن السيبراني العراقي تعمل على وضع الحجر الأساس لتنسيق النظام البيئي السيبراني في البلاد مع إطار موحد للأمن السيبراني.

٢,٤ قياس الآثار والفرص

❖ هناك العديد من المزايا المرتبطة بتنفيذ الاستراتيجية الوطنية للأمن السيبراني. إن بناء ورعاية الثقة في استخدام نظم المعلومات الوطنية وتكنولوجيا المعلومات والاتصالات الحساسة أمر حاسم بالنسبة للرفاه الاجتماعي والاقتصادي للمواطنين، ولذلك فمن المهم تأمين أمتنا في الفضاء السيبراني وبالتالي غرس مستوى عال من الثقة بين المستخدمين و الثقة في الاقتصاد الرقمي اللأمة.
❖ حاليا بدا بلدنا بالاعتماد على أداء تكنولوجيا المعلومات والاتصالات وتشغيل البنى التحتية للمعلومات الحيوية. وتعتمد تعاملاتنا في النقل والاتصالات والتجارة الإلكترونية والخدمات المالية على سرية المعلومات التي تتدفق من خلال هذه البنى التحتية وتكاملها وتوافرها.
❖ تعمل استراتيجية الأمن السيبراني على اظهار بنية أمنية وطنية جديدة وشاملة من خلال دمج الأمن المادي والسيبراني كتدابير مضادة ضد التهديد الخارجي، مما يعزز قدرة البلد على التأهب.
❖ هنالك عدة فرص ومجالات سوف تتاح في حال تواجد البلد في المجال السيبراني وكما يلي:
- الاقتصاد الرقمي المرن، وتحفيز الابتكارات، والمشاركة الفعالة، والتنمية، وتدفق الاستثمار الأجنبي المباشر.
- فرصة لاستغلال الفضاء السيبراني للنهوض بالقدرات العسكرية للبلاد في مجال التهديد الخارجي والصراع والعنف والإرهاب.
- استعداد العراق للدفاع عن مواطنيه، والحفاظ على عمليات البنية التحتية للمعلومات الهامة في وقت الهجمات الإلكترونية التي لا يمكن التنبؤ بها، ويضمن استمرارية العمليات الحرجة وسط الخصوم.

(٣) استراتيجية التأهب الوطني

٣,١ توجه السياسة الوطنية للأمن السيبراني

- تحدد الاستراتيجية الوطنية للأمن السيبراني استعداد البلد لحماية وإعداد الأمة بأسرها مقدما من أجل حماية البنى التحتية الرقمية والقدرة التنافسية الاقتصادية العالمية في الفضاء السيبراني. ويعالج أيضا الرغبة في تمكين الأمة من بناء قدرات شاملة من الناحية الهيكلية والإجرائية على المستويين الاستراتيجي والتكتيكي في التخفيف من المخاطر السيبرانية.
- يتوقف عامل النجاح الحاسم الذي تقوم به الاستراتيجية على التعبئة الشاملة والمشاركة والتنسيق للمكونات الحاسمة لضمان وجودنا في الفضاء السيبراني وحماية البنى التحتية للمعلومات الحيوية.
- يتفق اتجاه سياسة الحكومة بشأن الأمن السيبراني مع الاتجاه الإقليمي والعالمي بشأن تأمين الفضاء السيبراني.
- إن التركيز الأهم لاستراتيجية الأمن السيبراني هو التصدي لتعرضنا للمخاطر السيبرانية، وحماية البنية التحتية للمعلومات الأساسية الوطنية، واستغلال فرص الفضاء الإلكتروني لأغراض الأمن القومي والأهداف الاقتصادية، والعمل على دعم مجتمع سيبراني موثوق به.

٣,٢. ضرورة الاستراتيجية الوطنية للأمن السيبراني

- إن الطبيعة المتعددة الأبعاد للتهديدات الأمنية الآخذة في التطور هي من تحرك استراتيجية الأمن الوطني السيبراني الحالية إلى ما هو أبعد من النطاق التقليدي.
- بحسب طبيعة التهديدات الأمنية الحالية مثل الجريمة السيبرانية والعنف والصراع والإرهاب على نحو متزايد والطبيعة التي لا حدود لها للفضاء السيبراني فأن هذا سوف يشكل تهديدا لاعتمادنا المستقبلي على الفضاء السيبراني.
- تعمل الحكومة حاليا على الاستجابة باتجاه الحد من تأثير التهديدات السيبرانية وتصاعدها بطريقة تضمن وجود الأمة وتضمن الثقة في امننا و اقتصادنا.

٣,٣. أهداف الاستراتيجية الوطنية للأمن السيبراني

- تهدف الاستراتيجية إلى وضع خارطة طريق وطنية مع آليات منسقة مختلفة؛ إطار تنفيذي؛ والإجراءات التي تضمن تحقيق الرؤية الوطنية والأهداف المتعلقة بالأمن السيبراني.
- ولذلك، فإن الاستراتيجية ضرورية لتحقيق الأهداف المحددة التالية:
  - تشريعات شاملة لمكافحة الجريمة السيبرانية والتدابير المضادة للتهديد السيبراني التي يمكن اعتمادها على الصعيد الوطني، الإقليمية والعالمية ذات الصلة في سياق تأمين الفضاء السيبراني للبلاد.
  - توفير التدابير التي تحمي البنية التحتية الحيوية للمعلومات، فضلا عن الحد من مواطن الضعف والثغرات الوطنية من خلال إطار ضمان الأمن السيبراني.
  - وضع الية فعالة للاستجابة لحالات الطوارئ في الحاسوب.
  - العمل على تحسين قدرة وتطوير فريق الاستجابة لحالات الطوارئ في الحاسوب العراقي (CERT).
  - إن الآليات الوطنية لبناء القدرات والتوعية العامة وتمكين المهارات ضرورية للمساعدة في تعزيز قدرتنا على الاستجابة السريعة والفعالة للهجمات السيبرانية.
  - وضع آلية موثوقة لإشراك أصحاب المصلح المتعددين و الوطنيين والدوليين من أجل التصدي بشكل جماعي للتهديدات السيبرانية.
  - لردع وحماية الحكومة من جميع أشكال الهجمات السيبرانية.
  - تنسيق مبادرة الأمن السيبراني على جميع مستويات الحكومة في البلاد.

- بناء القدرات الوطنية ضد التهديدات الإلكترونية بالتعاون المنسق من خلال الشراكة بين القطاعين العام والخاص وإشراك أصحاب المصلح المتعددون.
- تعزيز الرؤية الوطنية للأمن السيبراني من خلال التوعية والشراكة من خلال تقاسم المسؤوليات وكذلك العمل على ايجاد مجتمع موثوق به من أصحاب المصلحة.
- تعزيز التنسيق والتعاون بين أصحاب المصلحة الإقليميين والعالميين بشأن الأمن السيبراني.

❖ تعمل الاستراتيجية على تعريف الأسس اللازمة لإطار عمل وطني منسق ومتوافق على الصعيد العالمي للعمل والتعاون في حماية الهياكل الأساسية الوطنية للمعلومات الحيوية من التهديدات السيبرانية.

٣,٤ نطاق الاستراتيجية الوطنية للأمن السيبراني

ويغطي نطاق الاستراتيجية الوطنية للأمن السيبراني مجالات الأولويات الوطنية فضلا عن الإطار العام للشراكة والتعاون الدولي بشأن الأمن السيبراني. وتعمل الاستراتيجية على تغطية المجالات التالية:

- الحكومة الفعالة
- الإطار التشريعي والتنظيمي
- إطار تكنولوجيا الأمن السيبراني
- ثقافة الأمن السيبراني وبناء القدرات
- البحث والتطوير نحو الاعتماد على الذات
- الامتثال والتنفيذ
- الجاهزية لحوادث الامن السيبراني
- التعاون الدولي

(٤) خارطة الطريق لاستراتيجية الامن السيبراني

- تعمل استراتيجية الامن السيبراني على تكوين استراتيجية منسقة وتستجيب بشكل ديناميكي نحو التهديدات التي تواجه الامن القومي. ومن مظاهر التهديد الأمني الوطني الناشئة هذا هو التعرض الوطني للمخاطر أثر الوجود الغير منسق في الفضاء السيبراني. وفي سياق التحديات الأمنية الفورية والمستقبلية، تهدف الاستراتيجية الوطنية للأمن السيبراني في العراق إلى إدارة التهديدات الأمنية في الفضاء الإلكتروني بما يتماشى مع أهدف الأمن القومي العام والمصلحة العامة.

- حيث ان الرؤية الوطنية للأمن السيبراني تتجه نحو مجتمع آمن ومضمون ونابض بالحياة ومرن وموثوق به يوفر فرصا لمواطنيه ويحمي المصالح الوطنية ويعزز التفاعلات السلمية والمشاركة الاستباقية في الفضاء السيبراني من أجل الرخاء الوطني. كذلك تهدف الرؤية الى تعزيز القدرات الوطنية في مجال الأمن السيبراني في العراق على نحو متناسق ومستدام ومتكامل من أجل التصدي والتخفيف من المخاطر السيبرانية في الفضاء السيبراني والتقليل من حدته.

- تهدف استراتيجية الامن السيبراني الوطنية الى حماية للبنى التحتية المعلوماتية الوطنية في مختلف الميادين ولأجل ذلك يجب تحديد المجالات التي يجب العمل عليها في إطار تنفيذي متناسق للارتقاء بمستوى العراق السيبراني نحو بيئة سيبرانية امنة. كما انها سوف 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.

- حيث باشر فريق الاستجابة الاليكتروني العراقي (CERT)مهامه بهذا الصدد وعمل على ايجاد التدابير والإجراءات لسد الفجوة الامنية السيبرانية ومعالجة أوجه الضعف الأساسية فيها. كذلك قام فريق الاستجابة الاليكتروني العراقي(CERT) بتشكيل عدة فرق تعمل على حدة وبشكل منسق حيث تم تقسيم وتصنيف المجالات التي يجب العمل عليها بشكل الذي يضمن إنتاجية الاستراتيجية الأمنية السيبرانية العراقية وفي إطار زمني محدد الى (٨) اقسام وحسب المعيار العالمي لأتحاد منضمة الاتصالات العالمية(ITU) وكذلك بما يضمن الارتقاء بمستوى العراق السيبراني العالمي وكما مبين ادناه:

٤,١ الحكومة الفعالة

- 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 الالكترونية بشكل يضمن راحة المواطن.

٤,٢ الإطار التشريعي والتنظيمي

- 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.
- انشاء برامج بناء القدرات التدريجي للجهات القانونية التنفيذية الوطنية.
- التأكد من أن جميع التشريعات المحلية المعمول بها تكمل وتنسجم مع القوانين والمعاهدات والاتفاقيات الدولية.

٤,٣ إطار تكنولوجيا الأمن السيبراني

- بناء وتطوير إطار تكنلوجي وطني للأمن السيبراني والذي يحدد متطلبات السيطرة على الامن السيبراني العراقي.
- العمل على بناء او انشاء برنامج وطني لتقييم / إصدار شهادات للمنتجات ونظم الامن السيبراني.

٤,٤ ثقافة الأمن السيبراني وبناء القدرات

- العمل على بناء وتطوير وتعزيز ثقافة الأمن السيبراني الوطني.
- العمل على انشاء و توحيد 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.

٤,٥ البحث والتطوير نحو الاعتماد على الذات

- العمل على تنسيق وتحديد أولويات البحث والتطوير في مجال الأمن السيبراني.
- العمل على توسعة وتعزيز مجتمع الأبحاث في مجال الأمن السيبراني.
- العمل على تعزيز، تطوير وتسويق الملكية الفكرية والتكنولوجية والابتكارات من خلال البحوث المركزة والمتخصصة والتطويرية.
- العمل على تغذية ودعم السوق المحلي و الصناعات في مجال الامن السيبراني.
- العمل على استحداث اختصاص جامعي يختص بالأمن السيبراني (**bachelor degree in cyber security**). ويكون وفق معايير خاصة.
- إضافة تخصص يعنى بالجنائيات الرقمية (**Digital Forensic**) وطرق التحقيق والاثبات في القضايا المتعلقة بالجرائم المعلوماتية.
- إضافة المناهج والتخصصات التي تعنى بالجرائم المعلوماتية لطلاب كليات الحقوق والقضاة.

٤,٦ الامتثال والتنفيذ

- توحيد أنظمة الأمن السيبراني عبر جميع مفاصل الدولة العراقية.
- العمل على تقوية وتعزيز الرصد والتنفيذ للمعايير في مجال الامن السيبراني.
- وضع إطار معياري لتقييم مخاطر الامن السيبراني.

٤,٧ الجاهزية لحوادث الامن السيبراني

- العمل على تعزيز وتقوية فريق الاستجابة للحوادث السيبرانية العراقي(CERT).
- العمل على وضع آليات فعالة للإبلاغ عن الحوادث السيبرانية.
- العمل على حث وتشجيع جميع الجهات والعاملين في مجال الامن السيبراني لمتابعة ورصد الفعاليات المتعلقة بالأمن السيبراني.
- العمل على وضع معيار إطاري موحد لإدارة استمرارية الأعمال.
- نشر تنبيهات انيه حول الثغرات، الضعف والتحذيرات فيما يتعلق بالأمن السيبراني.
- تشجيع جميع الجهات المتعلقة بالأمن السسيبراني على تنفيذ برامج دورية لفحص وتقييم مدى احتمالية التعرض للهجمات السيبرانية.

٤,٨ التعاون الدولي

- تشجيع المشاركة الفعالة في جميع هيئات الأمن السيبراني الدولية ذات الصلة، والأفرقة والوكالات المتعددة الجنسيات.
- تعزيز المشاركة الفعالة في جميع الفعاليات والمؤتمرات والمنتديات الدولية المتعلقة بالأمن السيبراني.
- تعزيز الموقع الاستراتيجي للعراق في مجال الأمن السيبراني من خلال استضافة مؤتمرات دولية دورية في مجال الامن السيبراني.
- التواصل مع منضمة الاتصالات العالمية (ITU) والعمل على تحديث الملف المتعلق بالوعي الأمني السيبراني العراقي
- العمل على تكوين شراكة واتفاقيات بين فريق الاستجابة الالكتروني العراقي(CERT) وفرق الاستجابة الاليكترونية الدولية الأخرى لأجل تطوير الفريق وتوسعة أفقه.

(٥) السقف الزمن التنفيذي

المرحلة الأولى (١ سنة)

معالجة المخاوف الفورية

- العمل على ايجاد التدابير والإجراءات لسد الفجوة الامنية السيبرانية ومعالجة أوجه الضعف الأساسية فيها.
- إنشاء منصة مركزية لآلية 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 (٣ سنوات)

بناء البنية التحتية

- إعداد ما يلزم من العمليات والمعايير والترتيبات المؤسسية.
- بناء القدرات بين الباحثين ومهنيي أمن المعلومات.
- العمل على استحداث اختصاص جامعي يختص بالأمن السيبراني (**bachelor degree in cyber security**).
- إضافة تخصص يعنى بالجنائيات الرقمية (**Digital Forensic**) وطرق التحقيق والاثبات في القضايا المتعلقة بالجرائم المعلوماتية.
- إضافة المناهج والتخصصات التي تعنى بالجرائم المعلوماتية لطلاب كليات الحقوق والقضاة.

المرحلة الثالثة (٥ سنوات وما بعدها)

تطوير الاعتماد على الذات

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