المركز العربي للبحوث القانونية والقضائية

المعهد العالي للقضاء -ليبيا

ورشة عمل

"الأمن السيبراني ودور القضاء في مكافحة الجرائم الالكترونية (أفاق وتحديات)"

المنعقدة بتاريخ ٢٠٢٤/٨/٢٦

بالمعهد العالي للقضاء

طرابلس - ليبيا

الموضوع

الاطار الاستراتيجي للامن السيبراني واهم المؤشرات العالمية

اعداد القاضي / حاتم جعفر

الرئيس بمحاكم الاستئناف – جمهورية مصر العربية

الاطار الاستراتيجي للامن السيبراني واهم المؤشرات العالمية

مقدمة

زاد الوعي عالمياً بأهمية الامن الامن السيبراني في السنوات الأخيرة نتيجة للتطور الهائل في طريقة استخدام التكنولوجيا ونوعية ذلك الاستخدام، الامر الذي أدى الى حتمية اللجوء لتلك الوسائل مما ساعد واسس لظهور مصطلح التحول الرقمي وزيادة نسبة الاعتمادية على تلك الوسائل .

ظهرت بشكل واضح الضرورة الملحة للتوسع في هذا التحول الرقمي مع ظهور وانتشار جائحة كرونا في العالم والذي حول الامر من اختيار ورفاهية الى أسلوب حياة وحتمية لا غني عنها ولا بديل لها وهو ما دفع عجلة التطور الرقمي نحو الانتشار مما استتبعه ضرورة تأمين تلك المعاملات الناتجة عن عملية التحول الرقمي في إطار متناسق ومتناغم مع باقي جهود الدولة مما أدى اقليمياً لظهور الاستراتيجيات الخاصة بالامن السيبراني .

كما أدى مفهوم العولمة وما تبعه من مكاشفة بين افراد المجتمع الدولي الى ظهور اليات لقياس مدى تقدم الدول وتطورها وهو ما ظهر في شكل خطط خمسية او عشرية أو اكثر وكذا مؤشرات لقياس الأداء كما انتشر عالميا وجود جهات متخصصة بدراسة ومتابعة وتقييم هذه المؤشرات بصورة مستقلة في الاغلب الاعم وبقدر كبير من الشفافية خاصة اذا كانت تلك المؤشرات تعتمد على حقائق ونتائج اكثر من اعتمادها على الآراء ومن هنا ظهرت مؤشرات عالمية معترف بها في مجال الامن السيبراني تحديداً وهو ما يجعلنا نتناول بالدراسة اهم هذه الأطر والاتجاهات الخاصة بالامن السيبراني ثم اهم مؤاشرات تقييمها على المستوى الدولي، الامر الذي يجعلنا نتناول بالشرح تمهيداً لذلك بعض المفاهيم ومنها :-

١- مفهوم الاستراتيجية . "Strategy".
٢- استراتيجية الامن السيبراني. Cybersecurity Strategy.
٣- مكونات استراتيجية الامن السيبراني Components of Cybersecurity Strategy.
٤- تقييم المخاطر والتعافي من الكوارث . Risk Assessment and Disaster Recovery.

ثم نتاول اهم الأطر والاتجاهات العالمية والمحلية وهي

١- دليل الاتحاد الدولي للاتصالات ITU لوضع استراتيجية وطنية للامن السيبراني .
٢- اطار عمل الوكالة الأوروبية لامن الشبكات والمعلومات ENISA .
٣- اطار عمل المعهد الوطني الأمريكي للمعايير والتكنولوجيا NIST.

بعدها يمكننا التعرض لأهم وأشهر مؤشرات قياس الأداء والتقييم الدولي للأمن السيبراني ومنها ما يتبع جهات أممية عالمية واشهرها مؤشر الأمن السيبراني العالمي Global Cybersecurity Index (GCI) الذي يصدره الاتحاد الدولي للاتصالات وكذا مؤشر National Cyber Security Index (NCSI) والذي تصدره احدى الجهات الاكاديمية في دولة استونيا إضافة لعدد من المؤشرات العالمية الأخرى ولكننا سنقصر العرض على هذين المؤشرين فقط.

١- مفهوم الاستراتيجية :

الاستراتيجية (Strategy): تعود جذور هذا المصطلح إلى الكلمة اليونانية "ستراتوس" (Stratos) التي تعني الجيش، و"آجين" (Agein) التي تعني القيادة، أي أنّ معنى الاستراتيجية هو قيادة الجيش، غير أنّه على عكس التكتيك الذي يكون محلي ومحدود من ناحية الوقت والمكان (كسب معركة)، فإنّ الاستراتيجية لديها هدف أوسع وطويل الأجل (كسب الحرب).

هناك عدة تعريفات مختلفة لمفهوم الاستراتيجية وتتنوع هذه التعريفات بحسب النطاق الزمني والتخصص الدقيق، فهي تعد خطة طويلة الأمد للوصول إلى هدف ما، وتُعد مهارةً لازمةً لتحقيق النجاح في الحرب، أو السياسة، أو الأعمال، أو الصناعة، أو الرياضة، وغيرها وقد عرفها الفريد تشاندلر أبو الاستراتيجية بانها" تحديد الأهداف والغايات الأساسية للمؤسسة واعتماد مسارات العمل وتخصيص الموارد اللازمة لتلك الأهداف " والاصل في الاستراتيجية او علم التخطيط بصفة عامة انها في الاساس مصطلح عسكري ويقصد به الخطة الحربية، أو هي فن التخطيط للعمليات العسكرية قبل نشوب الحروب، وفي نفس الوقت فن إدارة تلك العمليات عقب نشوب الحروب [١] كما تعرف الاستراتيجية أنها عبارة عن مجموعة من الطرق، الأساليب والمناهج التي تنظم مجريات العمل، والتي على أثرها يتم الوصول للهدف المنشود وفي الوقت المحدد، كل ذلك في ظل الإمكانيات المتاحة من الطاقة البشرية والمالية أيضاً [٢]

ويمكن القول بأن الاستراتيجية عبارة عن مجموعة من الإجراءات المنظمة القادرة على حصر واستغلال الموارد للوصول الى نتيجةأو تحديد هدف معين .

٢- استراتيجية الامن السيبراني .

استراتيجية الأمن السيبراني هي مجموعة من الأهداف والخطط والإجراءات التي تهدف إلى حماية الفضاء السيبراني وتحسين الأمن السيبراني على المستوى الوطني خلال مدة معينة، وذلك في نطاق زماني ومكاني محددين بعد حصر وتحديد الأصول الرقمية المهددة والاخطار المحتملة، أو كما عرفها دليل الاتحاد الدولي للاتصالات بأنها " مجموعة من الأدوات والسياسات والمبادئ التوجيهية والإجراءات والتدريب وأفضل الممارسات وآليات الضمان والتقنيات التي يمكن استخدامها في حماية توفر وسلامة وسرية الأصول في البنى التحتية الموصولة التابعة للحكومة والمنظمات الخاصة والمواطنين، بما في ذلك أجهزة الحوسبة الموصولة والموظفين والبنية التحتية والتطبيقات والخدمات وأنظمة الاتصالات والبيانات في البيئة السيبرانية".

ومن هذا المنطلق تشمل استراتيجية الأمن السيبراني على الأقل:

١- تعزيز حماية أنظمة التقنيات التشغيلية على كافة الأصعدة ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات وما تحويه من بيانات.
٢- إعداد إطار نظامي شامل لحماية الفضاء السيبراني.
٣- تطوير الكوادر الوطنية في مجال الأمن السيبراني.
٤- تطوير قيادات سيبرانية فعّالة.
٥- دعم التعاون للحماية السيبرانية.
٦- تطوير الإطار التنظيمي للأمن السيبراني لمقدمي الخدمة في قطاع الاتصالات وتقنية المعلومات.
٧- تطبيق وتشغيل أدوات وتقنيات الرصد على مستوى القطاع لدعم إطار حوكمة الأمن السيبراني
٨- تحديد ووضع معايير الرصد والإبلاغ عن أمن المعلومات والأمن السيبراني.
٩- إنشاء سياسات ومعايير وإجراءات الأمن السيبراني.

---

١ تعريف الاستراتيجية موسوعة ويكيبيديا
٢ سوزي الريس مقال عن تعريف الاستراتيجية موقع المقال

١٠- تحديد وتعريف ضوابط الأمن السيبراني وتوثيق الموافقة عليها وإجراء تنفيذها بطريقة منظمة.

١١- تطوير وتحديث الأنظمة والسياسات والإجراءات الأمنية بشكل دوري ومنتظم.

٣- مكونات استراتيجية الامن السيبراني

استراتيجية الأمن السيبراني تتكون من ثلاثة عناصر رئيسية وهي الأشخاص والإجراءات والتقنيات. وتعتبر هذه العناصر متكاملة وتعمل معا لتحقيق الأمن السيبراني.[٣] وفيما يلي شرح لكل عنصر:

الأشخاص: يشير هذا العنصر إلى الأفراد الذين يعملون في مجال الأمن السيبراني، ويشمل ذلك المدراء والموظفين والمستخدمين. ويتطلب هذا العنصر توفير التدريب والتعليم المستمر للأفراد لتحسين مهاراتهم وزيادة وعيهم بأمن المعلومات والأمن السيبراني، يجب تعزيز الوعي الأمني لدى الموظفين والمستخدمين وتوفير التدريب اللازم لهم لتحسين مهاراتهم في التعامل مع التهديدات السيبرانية.

الإجراءات: يشير هذا العنصر إلى السياسات والإجراءات التي تتبعها المؤسسات لحماية الأصول الرقمية والمعلومات الحساسة. وتشمل هذه الإجراءات تحديد وتعريف ضوابط الأمن السيبراني وتوثيق الموافقة عليها وإجراء تنفيذها بطريقة منظمة، وإنشاء سياسات ومعايير وإجراءات الأمن السيبراني والتي يجب تحديثها وتطويرها ومتابعتها بشكل مستمر.

التقنيات: يشير هذا العنصر إلى الأدوات والتقنيات التي تستخدم لحماية الأصول الرقمية والمعلومات الحساسة. وتشمل هذه التقنيات تطبيق وتشغيل أدوات وتقنيات الرصد على مستوى القطاع لدعم إطار حوكمة الأمن السيبراني، وتحديد ووضع معايير الرصد والإبلاغ عن أمن المعلومات والأمن السيبراني، وتطوير وتحديث الأنظمة والسياسات والإجراءات الأمنية بشكل دوري ومنتظم.

٤- التقنيات المستخدمة في تنفيذ استراتيجية الأمن السيبراني

توجد العديد من التقنيات الحديثة التي تستخدم في استراتيجية الأمن السيبراني، ومن بين هذه التقنيات:-

- تقنيات الذكاء الاصطناعي والتعلم الآلي: حيث يتم استخدام هذه التقنيات لتحليل البيانات والكشف عن الأنماط الغير عادية والتهديدات السيبرانية والتعرف على الهجمات المحتملة.

- تقنيات الحماية من البرامج الضارة: حيث يتم استخدام برامج مكافحة الفيروسات والبرامج الضارة وجدران الحماية لحماية الأنظمة والبيانات من الهجمات السيبرانية.

- تقنيات الحماية من الاختراق: حيث يتم استخدام تقنيات الحماية من الاختراق مثل الجدران النارية والتحقق من الهوية والتحقق من الوصول لمنع الوصول غير المصرح به إلى الأنظمة والبيانات.

- تقنيات الحماية من الهجمات السيبرانية المتقدمة: حيث يتم استخدام تقنيات مثل تحليل السلوك والكشف عن التهديدات المتقدمة والتحليل الاستخباري للحماية من الهجمات السيبرانية المتقدمة.

- تقنيات الحماية من الهجمات السيبرانية الجديدة: حيث يتم استخدام تقنيات مثل الكشف عن الهجمات السيبرانية الجديدة والتحليل الاستخباري للحماية من الهجمات السيبرانية الجديدة.

---

[٣] المركز الوطني الارشادي للامن السيبراني

٥- تقييم المخاطر والتعافي من الكوارث .

في مجال الأمن السيبراني، يعني تقييم المخاطر والتعافي من الكوارث تحديد الأخطار المحتملة التي تواجه المؤسسات والأفراد في عالم الإنترنت وتحديد الإجراءات الوقائية والاستجابة اللازمة للتصدي لهذه المخاطر والتعافي من الأضرار التي يمكن أن تحدث في حال وقوع الكوارث السيبرانية.

ويتضمن تقييم المخاطر في الأمن السيبراني تحليل عوامل الخطر المحتملة وتحديد مدى تأثيرها واحتمالية حدوثها، وكذلك تحديد التدابير الوقائية والإجراءات اللازمة للتصدي للمخاطر المحتملة مثل تحديث البيانات، الاختراقات، الفيروسات، البرمجيات الخبيثة، وغيرها من الهجمات السيبرانية.

أما التعافي من الكوارث السيبرانية، فهو عملية استعادة الأنظمة والبيانات المتضررة وتدمير البرمجيات الخبيثة[٤] وتحديث الأنظمة الأمنية والخطط الاستراتيجية والتكتيكية للتصدي للهجمات السيبرانية المستقبلية.

وتشمل عملية التعافي في الأمن السيبراني أيضاً التأكد من وجود خطط للوقاية من الهجمات السيبرانية المستقبلية وتطوير الأنظمة والتقنيات المقاومة للمخاطر السيبرانية وتدريب الموظفين على كيفية التعامل مع الهجمات السيبرانية وتطوير الوعي الأمني لدى الأفراد والمؤسسات. وتشمل أيضاً إجراءات التخزين الآمن للبيانات والاحتفاظ بنسخ احتياطية لها واختبار الأنظمة الأمنية بشكل دوري للتأكد من كفاءتها وجاهزيتها للتصدي للهجمات السيبرانية. وتعتبر هذه الإجراءات جزءاً أساسياً من استراتيجية الأمن السيبراني الشاملة والتي يتم تنفيذها لحماية المؤسسات والأفراد من الهجمات السيبرانية المستمرة.

[٤] مسح الحكومة الإلكترونية ٢٠٢٢ مستقبل الحكومة الرقمية

الفصل الأول

الاتجاهات الحديثة لإدارة استراتيجيات الأمن السيبراني

المبحث الأول:-
دليل الاتحاد الدولي للاتصالات لوضع استراتيجية وطنية للامن السيبراني.
المبحث الثاني:-
اطار الأمن السيبراني للمعهد الوطني للمعايير والتكنولوجيا "NIST"
المبحث الثالث :-
اطار عمل الوكالة الأوروبية للأمن السيبراني "ENISA"

الفصل الثاني

أهم المؤشرات العالمية لقياس أداء الدول في الأمن السيبراني

المبحث الأول :
المؤشر العالمي للأمن السيبراني Global Cybersecurity Index (GCI)
المبحث الثاني :
المؤشر الوطني للأمن السيبراني National Cyber Security Index (NCSI)

المبحث الأول

دليل الاتحاد الدولي للاتصالات لوضع استراتيجية وطنية للامن السيبراني.

الاتحاد الدولي للاتصالات (ITU) هو وكالة تابعة للأمم المتحدة المتخصصة في مجال تكنولوجيا المعلومات والاتصالات (ICT)، وتأسس في عام ١٨٦٥ لتسهيل التوصيلية العالمية وتحسين الاتصالات الدولية. ويعد الاتحاد الدولي للاتصالات المنظمة الرئيسية المسؤولة عن تطوير المعايير الدولية لتكنولوجيا المعلومات والاتصالات، وتعزيز التوصيلية العالمية وتحسين الوصول إلى تكنولوجيا المعلومات والاتصالات في جميع أنحاء العالم. ويعمل الاتحاد الدولي للاتصالات على تحسين الوصول إلى الاتصالات في البلدان النامية وتعزيز التوصيلية الهادفة في أقل البلدان نمواً. ويوفر الاتحاد الدولي للاتصالات العديد من البرامج والمبادرات لتعزيز التوصيلية العالمية وتحسين الوصول إلى تكنولوجيا المعلومات والاتصالات في جميع أنحاء العالم. ويعتبر الاتحاد الدولي للاتصالات مؤسسة رائدة في مجال تكنولوجيا المعلومات والاتصالات ويعمل على تعزيز التوصيلية العالمية وتحسين الوصول إلى تكنولوجيا المعلومات والاتصالات في جميع أنحاء العالم.

وفي اطار سعي الاتحاد الدولي للاتصالات لتأكيد القيام بدوره في وضع وتطوير المعايير الدولية الخاصة بمجتمع الاتصالات وتكنولوجيا المعلومات اطلق الاتحاد دليلاً لوضع الاستراتيجية الوطنية للأمن السيبراني وتم تعديلها أكثر من مرة وفي الإصدار الأخير لهذا الدليل قام الاتحاد ببيان وتحديد الأطراف الفاعلة في منظومات الامن السيبراني للدول والغرض من وضعه وقد شارك في وضع هذا الدليل اثنى عشر شريكاً دولياً كان من ابرزهم الوكالة الاوروبية لأمن الشبكات والمعلومات "ENISA" إضافة لعدد من المنظمات الحكومية الدولية والمنظمات الدولية والقطاع الخاص والمجتمع المدني.

وقد تحدد في مستهل الدليل **الغرض** الأساسي هذا الدليل "وهو توجيه القادة الوطنيين وواضعي السياسات لدى وضع استراتيجية وطنية للأمن السيبراني ولدى التفكير استراتيجياً بشأنه وذلك بهدف وضع إطار مفيد ومرن وسهل الاستخدام لتحديد سياق رؤية البلد الاجتماعية والاقتصادية والموقف الأمني الراهن ولمساعدة واضعي السياسات في رسم استراتيجية تأخذ في الاعتبار الوضع الخاص للبلد والقيم الثقافية والاجمتاعية وللتشجيع على تحقيق الأمن والصمود وتطوير مجتمعات موصولة معززة بتكنولوجيا المعلومات والاتصالات".

كما يتحدد **نطاق** الدليل حسبما توضح فيه ليشمل مختلف جوانب تحديات الامن السيبراني المتمثلة في الحوكمة والسياسة والجوانب التشغيلية والتقنية والقانونية وصولاً للمبادئ الشاملة والممارسات الجيدة حتى يتم صياغة الاستراتيجية مع الاخذ في الاعتبار الواقع وهو الإجراءات "العملية" التي تتخذها الدول في مختلف مراحل الاستراتيجية وبين محتوى النص الفعلي للاستراتيجية .

تم تحديد **الجمهور المستهدف** من الدليل بأنهم أولاً القادة الوطنيين وواضعي السياسات لتطوير استراتيجية وطنية للأمن السيبراني ثم مجموعة أصحاب المصلحة الآخرين ومنهم الحكوميون والمنظمات التنظيمية ومقدمي خدمات تكنولوجيا المعلومات والاتصالات والمؤسسات الأكاديمية ومؤسسات البحوث.

ووفقاً لهذا الدليل تم **تعريف الأمن السيبراني** ولأغراض الدليل بأنه " مجموعة الأدوات والسياسات والمبادئ التوجيهية ونُهج إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات وآليات الضمان والتقنيات التي يمكن استخدامها في حماية توفر وسلامة وسرية الأصول في البنى التحتية الموصولة التابعة للحكومة والمنظمات الخاصة والمواطنين، وتشمل هذه الأصول أجهزة الحوسبة الموصولة والموظفين والبنية التحتية والتطبيقات والخدمات وأنظمة الاتصالات والبيانات في البيئة السيبرانية"

حدد الدليل **فوائد الاستراتيجية** وعملية وضع-ها لتكون بمثابة

١- تعبير عن الرؤية والأهداف والمبادئ والأولويات الرفيعة المستوى التي ترشد البلد في تناول مسألة الأمن السيبراني .
٢- نظرة عامة تشمل أصحاب المصلحة المكلفين بتحسين الأمن السيبراني للبلد وأدوارهم ومسؤولياتهم.
٣- وصف للخطوات والبرامج والمبادرات التي يضطلع بها البلد لحماية البنية التحتية السيبرانية لديه، ومن ثم لتعزيز أمنه وقدرته على الصمود .

كما يمكن استخلاص عدة فوائد أخرى من اجمالي الدليل وهي :-

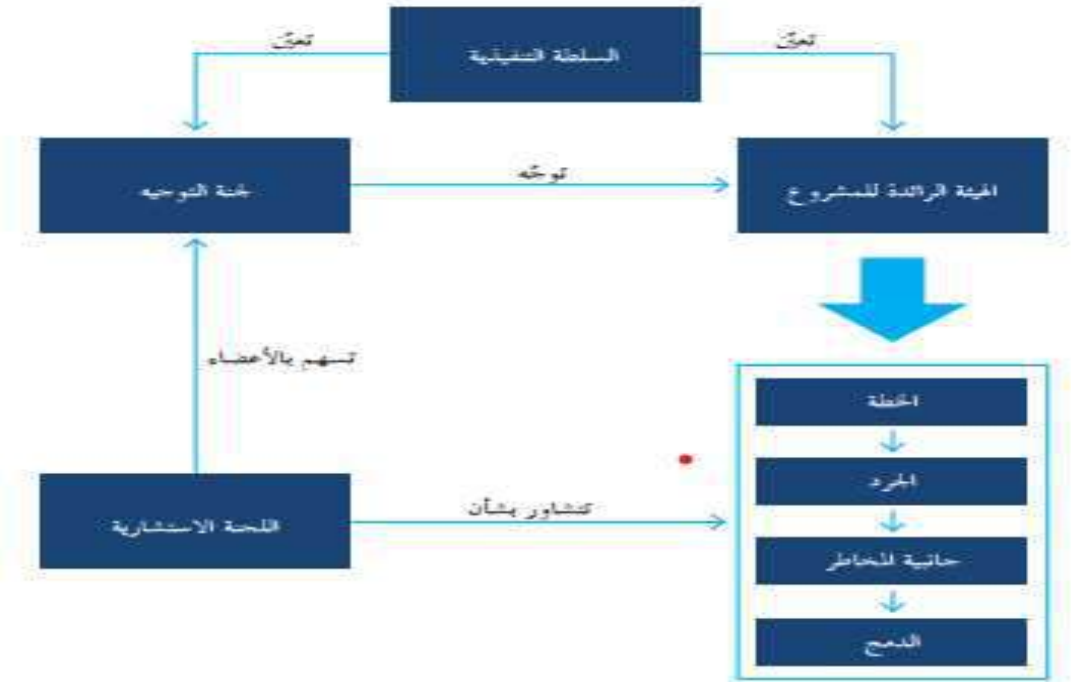
١- توفير بيئة أمنية سيبرانية أفضل للتجارة والاستثمار.
٢- حماية الحجم الاقتصادي الوطني وزيادة التنافسية في سوق الأعمال العالمية.
٣- حماية المعلومات والخصوصية الشخصية.
٤- تعزيز قدرة المؤسسات الوطنية لمواجهة التهديدات السيبرانية.
٥- التعاون مع شركاء دوليين لتبادل المعلومات والخبرات التقنية في مواجهة التهديدات السيبرانية.

دورة حياة الاستراتيجية الوطنية للأمن السيبراني "مراحل وضعها"

قسم الدليل مراحل وضع الاستراتيجية الى خمسة مراحل هي :-

١- المرحلة الأولى : - الاستهلال .

يتم في هذه المرحلة تحديد الهيئة الرائدة للمشروع ويجب ان تكون محايدة ومستقلة عن التنفيذ، ثم إنشاء لجنة توجيهية لمساعدة الهيئة الرائدة وبعد ذلك يتم تحديد أصحاب المصلحة وهم المعنيون بالمشاركة في وضع الاستراتيجية بصورة شاملة من جميع أصحاب الخبرات سواء من الحكومة او القطاع الخاص أو المجتمع المدني والخبراء ومشغلي البنى التحتية الحرجة وغيرهم، وعقب ذلك يتم التخطيط لوضع الاستراتيجية بعد اعداد الخطة اللازمة وموافقة السلطة التنفيذية عليها اعمالاً لإجراءات الحوكمة الوطنية بعد ان يتم تحديد الموارد والتمويل وخلافه طوال مدة الخطة .



٢- المرحلة الثانية :- الجرد والتحليل.

يتم في هذه المرحلة جمع البيانات والمعلومات المتعلقة بالأمن السيبراني في الدولة، وتقييم المشهد الوطني للأمن السيبراني، بالإضافة إلى تقدير المشهد الحالي والمستقبلي لصوغ استراتيجية وطنية للأمن السيبراني .وتشمل هذه المرحلة تحديد ماهية التهديدات وتقييم المخاطر التي تهدد الأمن السيبراني في البلد، بالإضافة إلى تقدير قدرات النظام الأمني السابق على التصدي لتلك التهديدات كذلك، وتتضمن هذة المرحلة تحديد ماهية الموارد والاستثمارات المطلوبة لتقوية ورفع كفاءة النظام الأمني السابق. وفي نهاية هذه المرحلة يتعامل فريق عمل استراتيجية الأمن السيبراني مع المعلومات التي تم جمعها وتحليلها لتقديم تقرير يقدم لمحة عامة عن الموقف الوطني الاستراتيجي للأمن السيبراني والمخاطر التي يجب التصدي لها.

٣- المرحلة الثالثة :- الإنتاج.

يتم في هذه المرحلة صياغة مشروع للاستراتيجية الوطنية للأمن السيبراني، وذلك بعد تحديد التهديدات والمخاطر التي يواجهها النظام الأمني السابق في المرحلة الثانية. وتشمل هذه المرحلة تشاور مع مجموعة واسعة من أصحاب المصلحة، بما في ذلك المؤسسات الحكومية والخاصة والأكاديمية وغيرها، لضمان تضافر جهود جميع أصحاب المصلحة في صياغة استراتيجية شاملة. بعد ذلك، يتم التماس الموافقة الرسمية على مشروع استراتيجية الأمن السيبراني من قبل جهات حكومية رفيعة المستوى كذلك، يتضمن هذه المرحلة نشر الاستراتيجية بشكل رسمي للجمهور وفي النهاية يتم إعداد خطة عمل تفصيلية تحدد المبادرات التي يتعين تنفيذها لتحقيق أهداف الاستراتيجية الوطنية للأمن السيبراني.

وتشمل هذه الخطة تحديد الموارد البشرية والمالية التي يتعين تخصيصها لتنفيذ المبادرات، بالإضافة إلى تحديد المواعيد الزمنية ومعايير لقياس التقدم في التنفيذ. وتهدف هذه المرحلة إلى صياغة استراتيجية شاملة وفعالة للأمن السيبراني وضمان تحقيق أهدافها بشكل فعال.

٤- المرحلة الرابعة :- التنفيذ .

هي مرحلة التنفيذ وهي أهم عنصر في دورة حياة الاستراتيجية الوطنية للأمن السيبراني، تتضمن هذه المرحلة وضع خطة عمل توجه مختلف الأنشطة المتوخاة، وتخصيص الموارد البشرية والمالية لتنفيذ المبادرات، بالإضافة إلى تحديد المواعيد الزمنية ومعاييرقياس مستوى التقدم في التنفيذ. يجب أن يكون هناك نهج منظم للتنفيذ، مدعوم بموارد كافية من أجل نجاح الاستراتيجية. كما يتطلب التنفيذ المشاركة والتنسيق من جانب طائفة من مختلف أصحاب المصلحة في شتى الدوائر، بما في ذلك القطاع الخاص والمجتمع المدني، بالإضافة إلى ذلك يجب أن تتم مراقبة وتقييم التنفيذ بشكل دوري.

وذلك بهدف تحديد أية مشاكل قد تظهر خلال عملية التنفيذ واتخاذ الإجراءات اللازمة لحلها. كما يتعين على فرق العمل المسؤولة عن التنفيذ أن تكون قادرة على التكيف مع التغيرات المستجدة في بيئة الأمن السيبراني، وتحديث خططها بشكل دوري لضمان استمرارية نجاح الاستراتيجية وفقاً لهذا التطور.

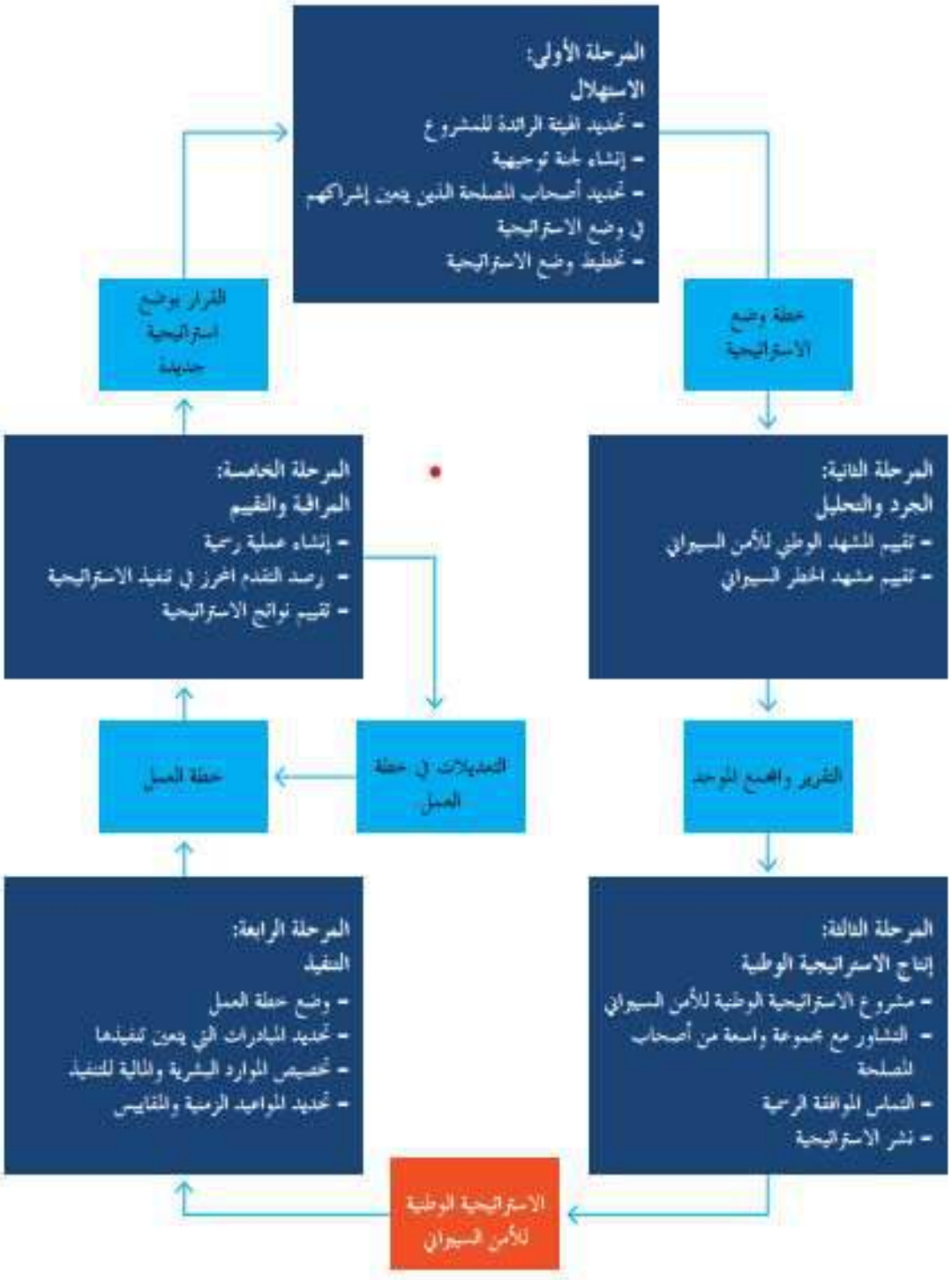
٥- المرحلة الخامسة:- المراقبة والتقييم.

تعد هذه المرحلة من اهم المراحل وتأتي بعد مرحلة التنفيذ حيث تهدف إلى رصد التقدم المحرز في تنفيذ الاستراتيجية، وتقييم نتائج الاستراتيجية ويتضمن ذلك إنشاء عملية رسمية للمراقبة والتقييم، والتأكد من أن جميع المؤشرات الأساسية يتم متابعتها بشكل دوري. كما يجب أن يتم تقديم تقارير دورية لإدارة الاستراتيجية حول التطورات في عملية التنفيذ، والإجراءات التصحيحية التي اتخذت لحل أية مشاكل قد تظهر خلال عملية التنفيذ، ويجب أن يكون هناك تعاون حول المعطيات بشأن الأهداف والإجراءات بين جميع فرق العَمَلِ المسؤولة عَنْ تَطْبِيقِ الاستراتيجية، كذلك يجب أن يتم تقييم نتائج الاستراتيجية بشكل

دوري، وذلك لتحديد ما إذا كانت الأهداف قد تحققت بشكل كامل، وما إذا كان هناك حاجة لإجراء تعديلات على الإستراتيجية. كما ينبغي أن يتم توثيق جميع النتائج والتوصيات المستخلصة من عملية التقييم، والعمل على تطبيق هذه التوصيات في المرحلة التالية من دورة حياة الإستراتيجية.

يعبر الشكل التالي عن ملخص لدورة حياة الاستراتيجية الوطنية للأمن السيبراني

الشكل 1 – دورة حياة الاستراتيجية الوطنية للأمن السيبراني



تعرض بعد ذلك الدليل للممارسات الجيدة في الاستراتيجية الوطنية للأمن السيبراني حيث ركز على مفاهيم محددة اطلق عليها **مجالات التركيز** وهي :-

١- الحوكمة Cybersecurity Governance .

ضرورة وضع بنية منضبطة فعالة للأمن السيبراني الوطني وذلك من خلال تحديد الأهداف والطموحات المرجوة في مجال الأمن السيبراني، وتحديد الأدوار وضمان أعلى مستوى من الدعم لتحقيق هذه الأهداف، كذلك تحديد السلطة المختصة وتحملها المسؤولية عن تنفيذ استراتيجية الأمن السيبراني، وإشراك الهيئات الحكومية وغيرها من القطاعات المتأثرة بتنفيذ هذه الاستراتيجية.

كما ينبغي أن تلتزم بوضع أهداف محددة وقابلة للقياس ويمكن تحقيقها وقائمة على النتائج وعلى الوقت في خطة التنفيذ الخاصة بالاستراتيجية، كما يجب على هذه الإستراتيجية أن تدرك حاجة التخصيص الموارد (مثل: الإرادة السياسية، التمويل، الزمن، والعاملون) لتحقيق نتائج مرضية.

٢- إدارة المخاطر في مجال الامن السيبراني الوطني "National Cybersecurity Risk Management".

مجال التركيز الثاني "إدارة المخاطر" يتعلق بضرورة اعتماد نهج لإدارة المخاطر في مجال الأمن السيبراني الوطني، حيث يتم تحديد وتقييم المخاطر التي يتعرض لها البلد، وذلك من خلال تحديد المخاطر الناشئة عن التبعيات عبر الحدود الوطنية، والعلاقات المتبادلة، وكذلك من خلال إدارة هذه المخاطر على نحو فعال جدًا. كما يجب أن يشمل نهج إدارة المخاطر في مجال الأمن السيبراني كامل دورة الحياة، من الوضع أو التوريد إلى التشغيل والاستبدال .

٣- التأهب والصمود readiness and resilience .

يركز على تعزيز قدرة الدول على التعامل مع الهجمات السيبرانية وتحمل آثارها، وذلك من خلال تطوير قدرات الاستجابة والاستعداد للتعامل مع هذه الهجمات والتصدي لها. يشمل هذا المجال تحديد المخاطر وتقييمها، وتطوير خطط الطوارئ وإنشاء أنظمة لإدارة الأزمات، بالإضافة إلى تحسين قدرات التحقق من الأصول والخدمات المهمة لضمان استمرارية عمليات البنية التحتية المختلفة. كما يشتمل هذا المجال على توفير التدريب والتوعية للفرق المختصة بأمن المعلومات في مختلف المؤسسات واجراء تمارين الامن السيبراني، بغية رفع مستوى التأهب والصمود في حال حدوث أي هجوم سيبراني

٤- خدمات البنية التحتية الحرجة والخدمات الأساسية Critical Infrastructure Protection

يرتكز المجال الرابع "البنية التحتية الحرجة" على تعزيز أمن البنية التحتية المهمة والحرجة في البلدان، وذلك من خلال تطوير استراتيجيات لحماية هذه الأصول وتقليل المخاطر المتعلقة بها. يشمل هذا المجال تحديد الأصول والخدمات الحرجة، وتطوير خطط لإدارة هذه المخاطر. كما يشتمل على توفير التدابير الأمنية لحماية هذه الأصول، بما في ذلك استخدام التقنيات الأمنية المتقدمة وإنشاء نظام مراقبة مستمر لهذه الأصول. كذلك، يشتمل هذا المجال على توفير التدريب والتوعية لفرق أمن المعلومات في مؤسسات البنية التحتية، بغية رفع مستوى حساسية هذه المؤسسات لأي تهديد سيبراني قد يستهدفها مع تعزيز التعاون بينها وبين مختلف الأطراف المعنية والعاملة في هذا المجال.

٥- المقدرة وبناء القدرات وإذكاء الوعي Awareness and Capacity Building.

يتركز هذا المجال "التوعية وبناء القدرات" على تعزيز قدرات الأفراد والمؤسسات والحكومات في مجال الأمن السيبراني، وذلك من خلال تطوير برامج تدريبية وتعليمية لتحسين المهارات والخبرات في

هذا المجال. كما يشمل أيضًا تطوير استراتيجيات لتحفيز الابتكار في مجال الأمن السيبراني، بما في ذلك دعم بحوث التقنية وتطوير حلول جديدة للتحديات المستقبلية. كذلك يشتمل هذا المجال على إذكاء الوعي بأهمية الأمن السيبراني، سواء بصفة عامة أو في مؤسسات محددة، من خلال حملات توعية وإعلامية ووضع مناهج تعليمية للامن السيبراني في المدارس والجامعات .

٦- التشريع والتنظيم Legal and Regulatory Frameworks.

يهدف هذا المجال إلى وضع إطار قانوني وتنظيمي لحماية المجتمع من الجرائم السيبرانية، وتشجيع بيئة سيبرانية آمنة ومأمونة. يشمل هذا المجال تحديد ما يشكل نشاطًا سيبرانيًا غير قانوني، والاعتراف القانوني بالحقوق الفردية والحريات المدنية في البيئة السيبرانية.

كذلك، يهدف هذا المجال إلى إنشاء آليات للامتثال، وبناء قدرات لإنفاذ التشريعات، وإضفاء الطابع المؤسسى على الكيانات الحرجة، وبصورة أكثر تفصيلًا، يتضمن المجال السادس في استراتيجية الأمن السيبراني عدة مبادرات وأنشطة، مثل وضع التشريعات والقوانين المتعلقة بالأمن السيبراني، وتحديد المسؤوليات والواجبات للجهات المختلفة في هذا المجال، ويتضمن هذا الجانب تدريب وتأهيل الكوادر البحثية والشرطية وكذلك القضائية القادرة علة التعامل مع هذا التشريعات اجرائياً وموضوعياً.

كما يشمل هذا المجال إنشاء آليات للامتثال والتحقق من تطبيق التشريعات، وتطوير الإجراءات القانونية لمكافحة جرائم الأمن السيبراني. متضمناً تعزيز التعاون بين الدول في مجال مكافحة جرائم الأمن السيبراني، وتبادل المعلومات والخبرات في هذا المجال .وفى نهاية المطاف، يهدف المجال السادس في استراتيجية الأمن السيبراني إلى تحقيق بيئة سيبرانية آمنة ومأمونة للأفراد والشركات والحكومات، من خلال تطبيق التشريعات والتنظيمات المناسبة لحماية المجتمع من جرائم الأمن السبيران

٧- التعاون الدولي International Cooperation .

يهدف المجال السابع في استراتيجية الأمن السيبراني إلى تعزيز التعاون الدولي في مجال الأمن السيبراني، وذلك من خلال المشاركة في المناقشات والتفاوضات الدولية، وتعزيز التعاون الرسمي وغير الرسمي في الفضاء السيبراني، وتحقيق توافق دولي حول قواعد سلوكية للدول في هذا المجال. كما يهدف إلى تطوير آليات لتبادل المعلومات والخبرات بشأن جرائم الأمن السبيرانى بين دول مختلفة، وتحديد أفضل الممارسات في هذا المجال.

المبحث الثاني

اطار الأمن السيبراني للمعهد الوطني للمعايير والتكنولوجيا "NIST"

أصبح الأمن السيبراني قضية فارقة ومحورية للمؤسسات المختلفة كما أن تحسين الأمن السيبراني يتطلب استخدام إطار عمل مناسب يساعد على تحديد المخاطر وتحديد الإجراءات الأمنية المناسبة لتحسين الأمن السيبراني ويعمل إطار NIST Cybersecurity Framework على تحقيق هذا الهدف من خلال توفير إطار عمل موحد يمكنه تحسين الأمن السيبراني في المؤسسات المختلفة، ويتكون الإطار من خمسة عناصر رئيسية تشمل **التحديد والحماية والاكتشاف والاستجابة والتعافي.**

كما سبق وان قررنا بأن اطار عمل المعهد الوطني للمعايير والتكنولوجيا بشأن الامن السيبراني من اهم وأوضح أطر العمل الخاصة بهذا المجال خاصة على قطاع الاعمال والشركات إضافة للقطاع الحكومي الامر الذي يجعلنا نعطي تعريف عن المعهد ثم عرض لأهم ما يعرض له الاطار في هذا الشأن.

ما هو المعهد الوطني للمعايير والتكنولوجيا [٥]

يمكننا تعريف المعهد الوطني للمعايير والتكنولوجيا او كما يشتهر عالمياً إختصاراً بـ "NIST" (National Institute of Standards and Technology – NIST) بأنه مؤسسة حكومية أمريكية تعمل تحت إشراف وزارة التجارة الأمريكية وقد تأسس هذا المعهد في عام ١٩٠١ بموجب قانون الكونغرس الأمريكي ويضطلع المعهد بصفته المسؤول الأول عن تطوير وتعزيز القياسات والمعايير والتكنولوجيا في الولايات المتحدة، ومقره الرئيسي في ولاية ماريلاند، ويضم مجموعة من المختبرات المتخصصة في العلوم والتكنولوجيا، وكذا مركزاً للأبحاث والتطوير.

يعد المعهد منظمة رائدة في مجال تطوير المعايير الدولية والتحقق من الجودة والتقنيات الحديثة، وتقدم الدعم للصناعة والحكومة والجهات الأكاديمية في الولايات المتحدة وفي جميع أنحاء العالم، ومن بين مجالات عمل المعهد تطوير المعايير الدولية في مجالات من أهمها الأمن السيبراني والتقنية موضوع البحث كما يتميز المعهد بأنه يعمل على تطوير أساليب قياس الجودة والأداء وترسيخها في مختلف الممارسات بما يساعد في تحسين الكفاءة وقلة التكلفة .

ومن بين أهم المساهمات التي قدمها المعهد في مجال الأمان السيبراني هو إطار NIST Cybersecurity Framework الذي يستخدم على نطاق عالمي العالم لتحسين الأمن السيبراني في المؤسسات والحكومات والشركات كما يهدف هذا الإطار إلى توفير إرشادات وأدوات موحدة لإدارة المخاطر السيبرانية وحماية الأصول السيبرانية وضمان الاستجابة السيبرانية ويساعد هذا الإطار المؤسسات على تحسين قدرتها على اكتشاف ومعالجة التهديدات السيبرانية والوقاية منها وطرق صدها والتعافي من اثارها.

اطار الامن السيبراني الخاص بالمعهد الوطني

قام المعهد الوطني للمعايير والتكنولوجيا بوضع عدة أطر لتنظيم وتحسين التعامل مع موضوع الامن السيبراني على مستوى الصناعة والشركات والمؤسسات وعلى المستوى الوطني كذلك ومن ضمن هذه

---

[٥] About National Institute of Standards and Technology

الأطراطار العمل الخاص بالامن السيبراني NIST Cybersecurity Framework (CSF)[٦] الصادر نسخته الأولى عام ٢٠١٤ وما سبقه من ارهاصات للاطار وما تلاه من تحسينات وتعديلات مخطط وصول تحديث لها العام القادم.

عناصر اطار الامن السيبراني NIST CSF "مراحل التعامل والاستجابة"

حدد الاطار خمسة عناصر أساسية يندرج تحتها العديد من تفاصيل الإجراءات والعمليات الدقيقة المنضبطة والمتتابعة في إجراءات محوكمة، وهي ما يشير لها الشكل التالي

العنصر الأول :- التحديد أو التعرف (Identify) .

عنصر التحديد (Identify) هو أحد العناصر الأساسية في إطار NIST Cybersecurity Framework، ويعني تحديد وفهم المخاطر السيبرانية التي تواجه المؤسسة وتحديد الأصول السيبرانية المهمة والحساسة التي يجب حمايتها، تتضمن عملية التحديد في إطار NIST Cybersecurity Framework العديد من الخطوات والأنشطة التي يجب على المؤسسات اتباعها، ومن بين هذه الخطوات:

١- تحديد الأصول السيبرانية: يجب على المؤسسات تحديد الأصول السيبرانية التي تعتبر حيوية وحساسة بالنسبة لها، مثل البيانات الحساسة والمعلومات الخاصة والأنظمة الحيوية والمعدات المتصلة بالشبكة. يجب أيضاً تحديد موقع هذه الأصول وتصنيفها وتقييم قيمتها.

٢- تحديد المخاطر السيبرانية: يجب على المؤسسات تحديد وتقييم المخاطر السيبرانية التي تواجهها وتحديد الأثر المحتمل لهذه المخاطر على الأصول السيبرانية الحيوية وعلى عمليات المؤسسة بشكل عام.

٣- تحديد المتطلبات القانونية والتنظيمية: يجب على المؤسسات تحديد المتطلبات القانونية والتنظيمية المتعلقة بالأمن السيبراني والامتثال لها، مثل متطلبات الامتثال لقواعد الامتثال الصادرة عن هيئات التنظيم واللوائح الحكومية المتعلقة بالأمن السيبراني.

٤- تحديد الأطر العامة للأمن السيبراني: يجب على المؤسسات تحديد الأطر العامة للأمن السيبراني المطبقة في المؤسسة، مثل السياسات والإجراءات والمتطلبات الأمنية المعمول بها. ويجب تقييم هذه الأطر العامة وتحديثها بشكل دوري لضمان التوافق مع التطورات السيبرانية الجديدة.

[٦] NIST Cybersecurity Framework (CSF)

٥- تحديد الفرص والتحديات: يجب على المؤسسات تحديد الفرص والتحديات المتعلقة بالأمن السيبراني، مثل فرص التحول الرقمي والتحول السيبراني والتحديات الجديدة ذات الصلة بالأمن السيبراني، مثل التهديدات السيبرانية الجديدة والهجمات السيبرانية المتطورة ونقص الموارد المتاحة لتنفيذ الأمن السيبراني.

بشكل عام، فإن عنصر التحديد يساعد المؤسسات على فهم وتحديد المخاطر السيبرانية التي تواجهها وتحديد الأصول السيبرانية المهمة والحساسة التي يجب حمايتها، ويمثل خطوة أساسية في إطار NIST Cybersecurity Framework لتحسين الأمن السيبراني وحماية المؤسسات من التهديدات السيبرانية.

العنصر الثاني :- الحماية (Protect) .

عنصر الحماية (Protect) هو العنصر الثاني في إطار NIST Cybersecurity Framework، ويهدف إلى توفير الحماية اللازمة للأصول السيبرانية المهمة من خلال تنفيذ إجراءات الأمن السيبراني اللازمة، ويشتمل عنصر الحماية في إطار NIST Cybersecurity Framework العديد من الخطوات والأنشطة التي يجب على المؤسسات اتباعها، ومن بين هذه الخطوات:

١- تنفيذ الإجراءات الأمنية: يجب على المؤسسات تنفيذ الإجراءات الأمنية اللازمة لحماية الأصول السيبرانية المهمة، مثل تحديد وتنفيذ السياسات والإجراءات الأمنية وتطبيق إجراءات الوصول والتحقق من الهوية والمصادقة والتشفير وغيرها من الإجراءات الأمنية المعمول بها.

٢- تعزيز الوعي الأمني: يجب على المؤسسات تعزيز الوعي الأمني لدى الموظفين والعاملين في المؤسسة، وتوفير التدريب والتعليم اللازمين لهم لزيادة وعيهم بمخاطر الأمن السيبراني وكيفية التعامل معها.

٣- إدارة الهوية والوصول: يجب على المؤسسات تنفيذ إجراءات إدارة الهوية والوصول للتأكد من أن المستخدمين المصرح لهم فقط يتمكنون من الوصول إلى الأصول السيبرانية المهمة، وتطبيق سياسات الوصول والتحققمن الهوية والتفويض والتحكم في الوصول والتسجيل والمراقبة.

٤- تحسين الأمان الفيزيائي: يجب على المؤسسات تحسين الأمان الفيزيائي للأصول السيبرانية المهمة، مثل تأمين الأجهزة والمعدات والمرافق الحيوية وتنفيذ الإجراءات الأمنية اللازمة لحمايتها.

٥- تحسين الأمن السيبراني لسلسلة التوريد: يجب على المؤسسات تحسين الأمن السيبراني لسلسلة التوريد وضمان أن الموردين يلتزمون بمعايير الأمان السيبراني المعمول بها ، وتحديد المخاطر السيبرانية المحتملة المتعلقة بالتوريد وتطبيق الإجراءات الأمنية اللازمة لتقليل هذه المخاطر.

٦- التعامل مع الحوادث السيبرانية: يجب على المؤسسات إعداد خطط الاستجابة للحوادث السيبرانية وتطبيقها للتعامل مع الهجمات السيبرانية والتعرف عليها والتحقق منها والاستجابة لها واستعادة النظام.

يهدف عنصر الحماية في إطار NIST Cybersecurity Framework إلى تحسين الأمن السيبراني للمؤسسات من خلال تنفيذ الإجراءات الأمنية اللازمة لحماية الأصول السيبرانية المهمة وتحسين الوعي الأمني لدى الموظفين والعاملين في المؤسسة على النحو السالف تفصيله حيث أن كل هذه الأنشطة تعمل

على تحسين الأمن السيبراني على النطاق المؤسسي وتحسين قدرتها على التعامل مع التهديدات السيبرانية المحتملة وتحقيق الاستمرارية في العمليات الأساسية للمؤسسة.

العنصر الثالث :- الكشف (Detect) .

عنصر الكشف (Detect) أو الاكتشاف هو العنصر الثالث في إطار NIST Cybersecurity Framework، ويهدف إلى تعزيز قدرة المؤسسة على الكشف المبكر عن الهجمات السيبرانية والأحداث الأمنية غير المرغوب فيها والتحقق منها بشكل فعال.

تشمل أنشطة عنصر الكشف في إطار NIST Cybersecurity Framework العديد من الخطوات والأنشطة التي يجب على المؤسسات اتباعها، ومن بين هذه الخطوات:-

١- تحديد المصادر المحتملة للأحداث الأمنية: يجب على المؤسسات تحديد المصادر المحتملة للأحداث الأمنية غير المرغوب فيها "التهديدات"، مثل السجلات والأحداث المنثقة عن أنظمة الأمان والأجهزة والشبكات وحركة المرور على الشبكة وغيرها من المصادر السيبرانية المحتملة.

٢- تطبيق تقنيات الكشف: يجب على المؤسسات تطبيق تقنيات الكشف المختلفة للكشف عن الأحداث الأمنية غير المرغوب فيها، مثل تحليل السجلات والمراقبة المتعمقة وتحليل السلوك وتحليل الأمن التنبؤي والكشف عن البرمجيات الخبيثة ومراقبة الأمان والتفتيش عن البرمجيات الخبيثة وغيرها من التقنيات السيبرانية.

٣- تحليل الأحداث: يجب على المؤسسات تحليل الأحداث الأمنية المكتشفة لتحديد ما إذا كانت تشكل تهديدًا حقيقيًا أو لا، وتحديد مدى خطورتها وتصنيفها وتبني إجراءات الاستجابة المناسبة لها.

٤- تحسين الأتمتة: يجب على المؤسسات تحسين الأتمتة في عمليات الكشف والتحليل والاستجابة لتحقيق كفاءة وفعالية أكبر، من خلال استخدام أدوات الأتمتة والذكاء الاصطناعي والتعلم الآلي والتحليل الآلي وغيرها من التقنيات الحديثة.

٥- تحسين الاستجابة: يجب على المؤسسات تحسين الاستجابة للأحداث الأمنية غير المرغوب فيها من خلال التقاط الأحداث بشكل سريع وتحليلها وتقديم الرد المناسب للتهديدات الحالية والمستقبلية.

يهدف عنصر الكشف في إطار NIST Cybersecurity Framework إلى تعزيز قدرة المؤسسات على الكشف المبكر عن الهجمات السيبرانية والأحداث الأمنية غير المرغوب فيها والتحقق منها بشكل فعال، وتقليل الأضرار الناجمة عن الهجمات السيبرانية وزيادة استجابة المؤسسة للتهديدات السيبرانية.

كما يساعد عنصر الكشف على تحسين قدرة المؤسسة على تحليل الأحداث الأمنية وتصنيفها واتخاذ الإجراءات المناسبة للتعامل مع التهديدات السيبرانية المحتملة. كما يساعد على تحسين كفاءة وفعالية عمليات الكشف والتحليل والاستجابة من خلال تحسين الأتمتة واستخدام التقنيات الحديثة، مما يسهم في تقليل الوقت اللازم للاستجابة للأحداث الأمنية وتقليل الأضرار الناجمة عنها.

العنصر الرابع :- الاستجابة (Respond) .

عنصر الاستجابة (Respond) هو العنصر الرابع في إطار NIST Cybersecurity Framework، ويهدف إلى تعزيز قدرة المؤسسة على الاستجابة للهجمات السيبرانية وإعادة تأهيل الأنظمة والبيانات المتأثرة وتقليل الأضرار الناجمة عن الهجمات.

تشمل أنشطة عنصر الاستجابة في إطار NIST Cybersecurity Framework العديد من الخطوات والأنشطة التي يجب على المؤسسات اتباعها، ومن بين هذه الخطوات:

١- الاستجابة للحوادث: يجب على المؤسسات وضع خطط الاستجابة للحوادث وتنفيذها عند الحاجة، وتحديد الأدوار والمسؤوليات والإجراءات المناسبة لتنفيذ هذه الخطط وضمان توافر الموارد اللازمة لتنفيذها.

٢- الحد من الأضرار: يجب على المؤسسات اتخاذ الإجراءات اللازمة للحد من الأضرار الناجمة عن الهجمات السيبرانية وإعادة تأهيل الأنظمة والبيانات المتأثرة، وتقييم الأضرار وتحديد الأولويات في إعادة بناء البنية التحتية للمؤسسة.

٣- التحليل الجنائي الرقمي: يجب على المؤسسات القيام بالتحليل الجنائي الرقمي للأحداث السيبرانية والهجمات المتعلقة بها، وجمع الأدلة الرقمية وتقييمها وتحليلها لتحديد المسؤوليات والمصادر والأساليب المستخدمة في الهجوم، وتحديد الأدلة الرقمية التي يمكن استخدامها في التحقيقات الجنائية.

٤- تحسين الأتمتة: يجب على المؤسسات تحسين الأتمتة في عمليات الاستجابة للحوادث، وذلك من خلال استخدام أدوات الأتمتة والذكاء الاصطناعي والتعلم الآلي والتحليل الآلي وغيرها من التقنيات الحديثة، وذلك لتحسين كفاءة وفعالية عمليات الاستجابة وتقليل الوقت اللازم لإعادة تأهيل الأنظمة المتأثرة.

٥- التدريب والتمرين: يجب على المؤسسات تنظيم تدريبات وتمارين دورات تدريبية للموظفين حول كيفية التعامل مع الهجمات السيبرانية وكيفية تنفيذ خطط الاستجابة للحوادث بشكل فعال، وكذلك تنظيم تمارين للاستجابة للحوادث لتحسين قدرة المؤسسة على الاستجابة للهجمات السيبرانية وإعادة تأهيل الأنظمة المتأثرة.

يهدف عنصر الاستجابة في إطار NIST Cybersecurity Framework إلى تعزيز قدرة المؤسسة على الاستجابة للهجمات السيبرانية وإعادة تأهيل الأنظمة والبيانات المتأثرة وتقليل الأضرار الناجمة عن الهجمات، وتحسين قدرة المؤسسة على تنفيذ خطط الاستجابة للحوادث بشكل فعال وتقليل الوقت اللازم لإعادة تأهيل الأنظمة المصابة. كما يساعد عنصر الاستجابة على تحسين قدرة المؤسسة على التحليل الجنائي الرقمي وجمع الأدلة الرقمية والتحقيق في الهجمات السيبرانية. ويساعد أيضاً عنصر الاستجابة على تحسين كفاءة وفعالية عمليات الاستجابة للحوادث من خلال تحسين الأتمتة واستخدام التقنيات الحديثة وتنظيم التدريبات والتمارين للموظفين.

بشكل عام، يعتبر عنصر الاستجابة في إطار NIST Cybersecurity Framework جزءاً أساسياً في الحفاظ وتعزيز الأمان السيبراني للمؤسسات، ويساعد في تحسين القدرة على التعامل مع الهجمات السيبرانية وتقليل الأضرار الناجمة عنها، كما يساعد على زيادة الإدراك لدى المؤسسات حول أهمية الاستجابة الفعالة للهجمات السيبرانية وتنفيذ الخطط اللازمة لذلك.

العنصر الخامس :- التعافي (Recover) .

عنصر التعافي (Recover) هو العنصر الخامس والاخير في إطار NIST Cybersecurity Framework ويهدف إلى توفير الإجراءات والخطط اللازمة لاستعادة الوظائف الأساسية للمؤسسة بعد وقوع هجمات سيبرانية أو حوادث أمنية أخرى.

تشمل أنشطة عنصر التعافي في إطار NIST Cybersecurity Framework العديد من الخطوات والأنشطة التي يجب على المؤسسات اتباعها، ومن بين هذه الخطوات:

١- تحديد الموارد الحساسة والحرجة : يجب على المؤسسات تحديد الموارد الحيوية والبيانات الحساسة والتطبيقات الحيوية والأنظمة الهامة لتحديد أولويات استعادتها في حالة وقوع هجمات سيبرانية أو حوادث أمنية أخرى وهي الموارد الأكثر تأثراً والأوسع انتشاراً.

٢- الإجراءات الاحتياطية: يجب على المؤسسات تنفيذ الإجراءات اللازمة لإجراء النسخ الاحتياطية للبيانات والأنظمة والتطبيقات الحيوية والحساسة وتخزينها في مواقع آمنة وتحديثها بانتظام.

٣- استرداد البيانات: يجب على المؤسسات تنفيذ الإجراءات اللازمة لاسترداد البيانات المفقودة أو التالفة بعد وقوع هجمات سيبرانية أو حوادث أمنية أخرى.

٤- استعادة الأنظمة: يجب على المؤسسات تنفيذ الإجراءات اللازمة لاستعادة الأنظمة المتأثرة وإعادة تأهيلها إلى حالتها الطبيعية بعد وقوع هجمات سيبرانية أو حوادث أمنية أخرى.

٥- اختبار الاستعادة: يجب على المؤسسات اختبار خطط الاستعادة بانتظام وتحديثها بناءً على نتائج الاختبارات، وتدريب الموظفين على كيفية تنفيذ خطط الاستعادة وتحديثهم بشكل دوري.

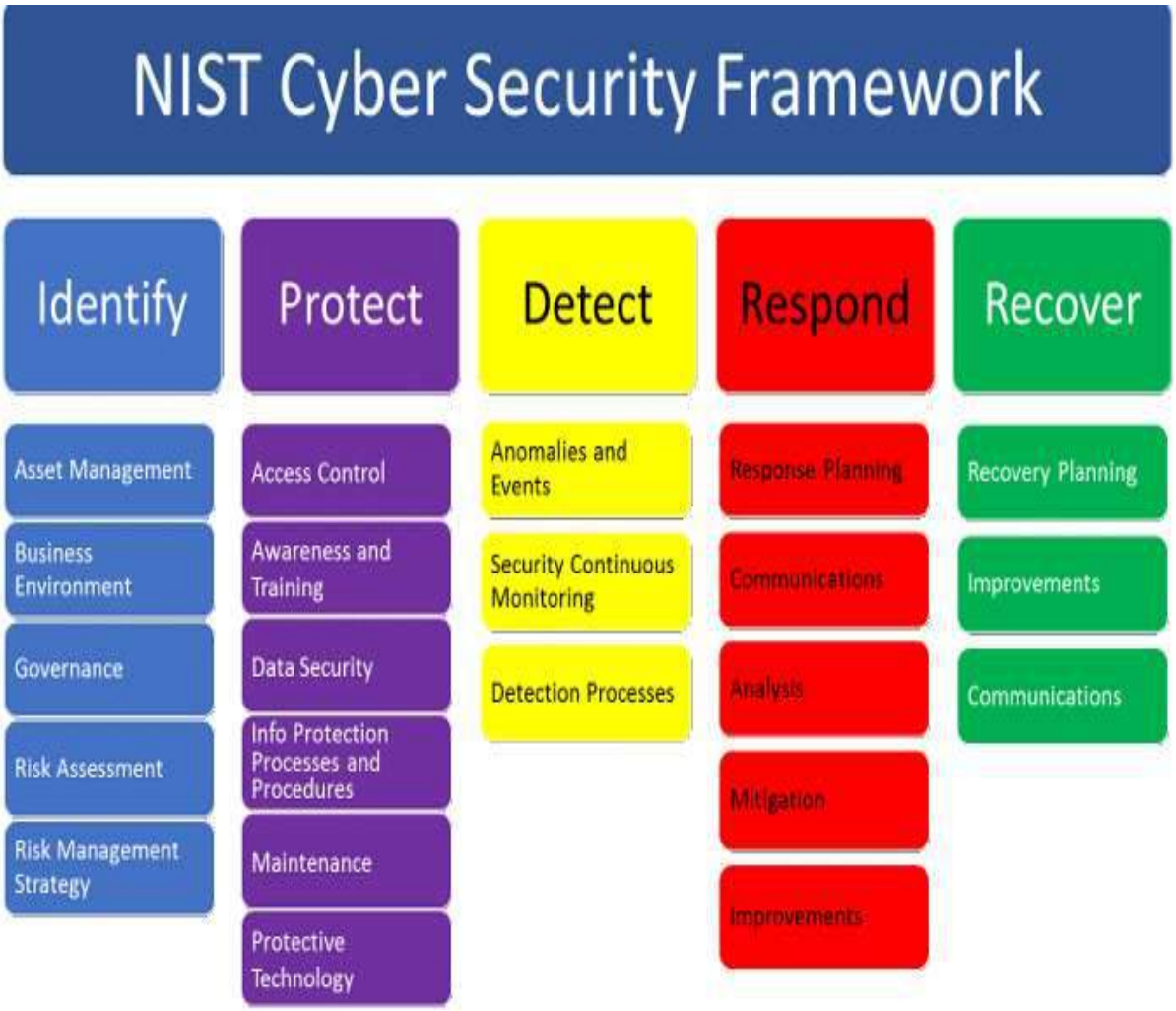
يهدف عنصر التعافي في إطار NIST Cybersecurity Framework إلى توفير الإجراءات والخطط اللازمة لاستعادة الوظائف الأساسية للمؤسسة، وضمان استمرارية العمليات الأساسية للمؤسسة بشكل فعال. وتحديد الموارد الحيوية والأصول الحرجة والبيانات الحساسة وتحديد أولويات استعادتها في حالة وقوع هجمات سيبرانية أو حوادث أمنية أخرى، وتنفيذ الإجراءات اللازمة لإجراء النسخ الاحتياطية للبيانات والأنظمة والتطبيقات الحيوية والحساسة وتخزينها في مواقع آمنة وتحديثها بانتظام، واسترداد البيانات المفقودة أو التالفة بعد وقوع هجمات سيبرانية أو حوادث أمنية أخرى. كما يشمل عنصر التعافي تنفيذ الإجراءات اللازمة لاستعادة الأنظمة المتأثرة وإعادة تأهيلها إلى حالتها الطبيعية بعد وقوع هجمات سيبرانية أو حوادث أمنية أخرى واختبار خطط الاستعادة بانتظام وتحديثها بناءً على نتائج الاختبارات، وتدريب الموظفين على كيفية تنفيذ خطط الاستعادة وتحديثهم بشكل دوري.

بشكل عام، يعتبر عنصر التعافي في إطار NIST Cybersecurity Framework جزءًا مهمًا للحفاظ على استمرارية العمليات الأساسية للمؤسسة وتحسين قدرتها على استعادة البيانات والأنظمة والتطبيقات الحيوية بعد وقوع هجمات سيبرانية أو حوادث أمنية أخرى. كما يساعد عنصر التعافي على تحديد الخطط والإجراءات اللازمة للتعافي بشكل سريع وفعال وتقليل تأثير الهجمات السيبرانية أو الحوادث الأمنية على المؤسسة وعملياتها.

بعد أن تعرضنا سريعاً لأهم مكونات اطار عمل المعهد الوطني للمعايير والتكنولوجيا الخاص بالامن السيبراني وعناصره الخمس الأساسية وما بنطوي عليه من إجراءات صارمة غاية في الأهمية والتركيز والحرفية العالية جداً والقدرة على التعامل مع كل مكونات الامن السيبراني قبل واثناء وبعد وقوع الحادثة الأمنية او الأزمة السيبرانية او الهجمة أياً ما كان مسماها، ننوه الى أن هذا الاطار يمتاز بالتحديث المستمر

والتطوير العلمي القائم على التجربة والاستفادة من الحوادث السابقة وذلك كله في اطار عملي بحت بعيد عن التنظير وفي حالة الامتثال لما ورد في الإطار لابد وان تختلف مرونة المؤسسة او الدولة وقدرتها في التعامل مع هذه الحوادث .[٧]

ويمكننا تلخيص جميع ما سبق بالنسبة لهذا الاطار في الشكل التالي



إضافة للاطار السابق تناوله قام المعهد بوضع عديد من الإطارات العمل النموذجية للأمن السيبراني ومنها اطار عمل الامن السيبراني للبنى التحتية الحرجة وغيرها من الإطارات القطاعية المتخصصة يمكن التعمق فيها والاستفادة منها بالرجوع للموقع الالكتروني للوكالة او التواصل المباشر معها

[٧] the Cybersecurity Framework

المبحث الثالث

اطار عمل الوكالة الأوروبية للأمن السيبراني "enisa"

مقدمة

تساهم الوكالة الأوروبية لأمن المعلومات والشبكات في وضع سياسة الاتحاد الأوروبي للأمن السيبراني، وتعزز مصداقية منتجات تكنولوجيا المعلومات والاتصالات والخدمات والعمليات مع برامج شهادة الأمان السيبراني، وتتعاون مع الدول الأعضاء والهيئات الأوروبية، وتساعد أوروبا على التحضير للتحديات السيبرانية في المستقبل.

تعريفها

تعد (الوكالة الأوروبية لأمن المعلومات والشبكات) (European Network and Information Security Agency - ENISA) والتي تم انشائها في عام ٢٠٠٤ هي وكالة تابعة للاتحاد الأوروبي تعمل على تعزيز قدرة دول الاتحاد الأوروبي ومنظمات القطاع الخاص على منع وكشف والاستجابة للتهديدات السيبرانية وقد تم تغيير الاسم في عام ٢٠١٩ الى الوكالة الأوروبية للأمن السيبراني (European Union Agency for Cybersecurity) مع الإبقاء على الاختصار القديم لها enisa لها كما هو .

تعمل وكالة الاتحاد الأوروبي للأمن السيبراني على تطوير خطة عمل استراتيجية محددة للأمن السيبراني. تهدف هذه الخطة إلى تحسين قدرة الاتحاد الأوروبي على التصدي للتهديدات السيبرانية وحماية الشبكات والمعلومات الحيوية.

تتضمن الخطة الاستراتيجية الحالية للأمن السيبراني في ENISA العديد من المبادرات والأنشطة التي تشمل تحسين التعاون بين الدول الأعضاء وتعزيز الوعي والتدريب في مجال الأمن السيبراني وتطوير المعايير الأوروبية للأمن السيبراني وتوفير المشورة الفنية في هذا المجال، إضافة الى تعزيز القدرات الأوروبية للتحقق من الأمان السيبراني وتحسين نظم الاستجابة للطوارئ السيبرانية وتعزيز البحث والابتكار في مجال الأمن السيبراني.

يتم تنفيذ هذه المبادرات والأنشطة من خلال التعاون مع الدول الأعضاء والشركاء الآخرين في القطاع الخاص والأكاديمي والمجتمع المدني.

تتنوع وتتعدد مجالات عمل الوكالة في أكثر من نشاط وخطة عمل تخص تحسين الأمن السيبراني لدى الدول الأعضاء ولكن مت يهمنا التركيز عليه وعرضه في هذه الدراسة الموجرة بعض الخطوط العريضة التي لا يمكن اهمالها والتي نحددها فيما يلي :-

أولاً:- الأهداف الاستراتيجية لعمل الوكالة في مجال الامن السيبراني[٨] .

١- تعزيز الوعي الأمني وتعزيز الثقافة الأمنية في المؤسسات والمنظمات والمجتمعات.

٢- دعم تطوير وتحسين قدرات الأمن السيبراني في أوروبا.

[٨] National Cyber Security Strategy ENISA NCSS

٣- تعزيز التعاون والتنسيق بين الدول الأوروبية والمؤسسات والمنظمات المختلفة في مجال الأمن السيبراني.

٤- توفير الدعم والمساعدة للمؤسسات والمنظمات في التصدي للتهديدات السيبرانية والحوادث الأمنية.

٥- تطوير المعايير والممارسات والأدوات الأمنية اللازمة لتحقيق الأمن السيبراني في أوروبا.

٦- تعزيز القدرة على التعامل مع التهديدات السيبرانية الجديدة والناشئة.

٧- تقييم وتحسين الأمن السيبراني في القطاعات الحيوية والحكومية والخدمات الرقمية والأسواق الرقمية.

٨- توفير الدعم والمساعدة في مجال الأمن السيبراني للمواطنين والمستخدمين.

٩- تعزيز البحث والتطوير في مجال الأمن السيبراني وتطبيق التقنيات الحديثة لتحقيق الأمن السيبراني.

١٠- العمل على تعزيز الشفافية والمساءلة في مجال الأمن السيبراني، وذلك من خلال توفير المعلومات والتوجيهات والنصائح والتحليلات الأمنية الشاملة للمؤسسات والمنظمات والمجتمعات.

تسعى ENISA من خلال هذه الأهداف إلى تعزيز الأمن السيبراني في أوروبا وتعزيز القدرة على التصدي للتهديدات الأمنية المتعددة التي تواجه المؤسسات والمنظمات في العصر الرقمي. وتعتبر هذه الأهداف هي الأساس لعمل الوكالة وتوجهاتها الاستراتيجية.

منهجية تنفيذ هذه الأهداف

تعتمد الوكالة الأوروبية لأمن الشبكات والمعلومات (ENISA) في بناء وتنفيذ استراتيجية الأمن السيبراني على منهجية شاملة ومتكاملة، تشتمل على عدة مراحل، وهي كالتالي:

تحليل الوضع الحالي: يتم في هذه المرحلة تحليل الوضع الحالي للأمن السيبراني في أوروبا، ومن ثم تحديد المخاطر والتهديدات السيبرانية المحتملة، وتحديد النواحي التي تحتاج إلى تحسين وتطوير لتعزيز الأمن السيبراني في المنطقة.

وضع الأهداف والاستراتيجية: تعتمد ENISA في هذه المرحلة على تحليل الوضع الحالي لوضع الأهداف والاستراتيجية الأساسية لتحسين الأمن السيبراني في أوروبا، وتحديد خطط العمل اللازمة لتحقيق هذه الأهداف، بما في ذلك تطوير السياسات والإجراءات والتقنيات الأمنية السيبرانية وتحسين قدرات الأمن السيبراني للمؤسسات والحكومات.

تطبيق الاستراتيجية: حيث يتم تطبيق الاستراتيجية المعتمدة، وتنفيذ خطط العمل المحددة لتحسين الأمن السيبراني في أوروبا. وتشمل هذه المرحلة تقديم الدعم التقني والفني للمؤسسات والحكومات في تحسين قدراتهم الأمن السيبراني، وتطوير الأدوات والتقنيات الأمنية السيبرانية المتقدمة، وتوفير التدريبات والورش العمل والدورات التدريبية للمستخدمين والمدراء التنفيذيين.

تقييم الأداء والتحسين المستمر: تعتمد ENISA في هذه المرحلة على تقييم الأداء والتحسين المستمر للاستراتيجية وخطط العمل المنفذة، وتحديد النواحي التي تحتاج إلى تحسين وتطوير لتحقيق الأهداف المحددة. وتستخدم ENISA تقنيات التقييم المستمر وتحليل البيانات لتحديد النواحي التي تحتاج إلى التحسين وتطوير الاستراتيجية، وتعمل على تحسين الخدمات والأدوات المقدمة للمؤسسات والحكومات في أوروبا.

ويتم تنفيذ هذه المنهجية بالتعاون مع الجهات المعنية في القطاع العام والخاص والمؤسسات الأكاديمية والأبحاث، وذلك لضمان توفير الدعم والمشورة والخبرة اللازمة لتحسين الأمن السيبراني في أوروبا. وتسعى ENISA دائمًا للتحسين المستمر وتطوير الخدمات والأدوات المقدمة، والتأكد من تحقيق الأهداف المحددة في استراتيجية الأمن السيبراني.

ثانياً:- دورة حياة الاستراتيجية Enisa NCSS lifecycle

دورة حياة الاستراتيجية NCSS Life Cycle هي عبارة عن عملية تصميم وتنفيذ الاستراتيجيات الأمنية السيبرانية المتكاملة والمستدامة، وتهدف إلى تحسين قدرات الأمن السيبراني للمؤسسات والمنظمات والحكومات. ويمكن تلخيص دورة حياة الاستراتيجية NCSS Life Cycle في النقاط التالية:

١- التخطيط: يتضمن التعرف على أهداف الأمن السيبراني والتحديات المتعلقة بالأمن السيبراني وتحديد الأولويات والمخاطر والمتطلبات.
٢- التحليل: تحليل البيئة السيبرانية وتقييم المخاطر وتحليل السياسات واللوائح والقدرات الحالية لتحديد الفرص والتحديات والتهديدات وتحديد متطلبات الأمن السيبراني.
٣- التصميم: تصميم استراتيجية الأمن السيبراني وتحديد الخطط والأدوات والموارد اللازمة لتحقيق هذه الاستراتيجية.
٤- التنفيذ: تنفيذ الخطط والأدوات والموارد المحددة في المرحلة السابقة وتطبيق استراتيجية الأمن السيبراني.
٥- الرصد والتقييم: تقييم أداء استراتيجية الأمن السيبراني ورصد التحديات والتهديدات وتحديث الاستراتيجية بشكل دوري لضمان استمرارية الأمن السيبراني.
٦- التحسين المستمر: تحسين استراتيجية الأمن السيبراني وتحسينها بشكل مستمر بناءً على تقييم الأداء وتحديث الخطط والأدوات والموارد المستخدمة فيها.

يتضمن دورة حياة الاستراتيجية NCSS Life Cycle أيضًا مفهوم الاستمرارية والمرونة، وهو مفهوم يهدف إلى تحديث الاستراتيجية وتحسينها باستمرار لتلبية التحديات الجديدة في بيئة الأمن السيبراني المتغيرة. وتقوم ENISA توفير الدعم والمشورة والتوجيهات للمؤسسات والمنظمات في جميع مراحل دورة حياة الاستراتيجية NCSS Life Cycle، وتقديم الخبرة والمعرفة في مجال الأمن السيبراني لمساعدتهم على تحسين قدراتهم وتطبيق أفضل الممارسات في هذا المجال. وبالإضافة إلى ذلك، يمكن لـ ENISA توفير المساعدة في تطوير خطط الطوارئ والاستجابة لحالات الأمن السيبراني وتحسين قدرة المؤسسات والدول على التعامل مع التهديدات السيبرانية.

ثالثاً:- الإطار الوطني للتقييم السيبراني Enisa NCAF

NCAF هو اختصار لـ "الإطار الوطني للتقييم السيبراني" (National Cybersecurity Assessment Framework)[٩] وهو أداة تم تطويرها بواسطة الوكالة الأوروبية للأمن السيبراني (ENISA) لتقييم قدرات الأمن السيبراني في الدول الأعضاء في الاتحاد الأوروبي.

يستخدم هذا الإطار الوطني للتقييم السيبراني NCAF لتقييم قدرات الأمن السيبراني في الدول الأعضاء، ويعتمد على مجموعة من المعايير والممارسات الأمنية السيبرانية المعترف بها دوليًا. ويتمثل الهدف الرئيسي لهذا الإطار في توفير تقييم شامل وموحد لقدرات الأمن السيبراني في الدول الأعضاء، وتقديم التوصيات والإرشادات اللازمة لتحسين هذه القدرات وتعزيز الأمان السيبراني في المستقبل.

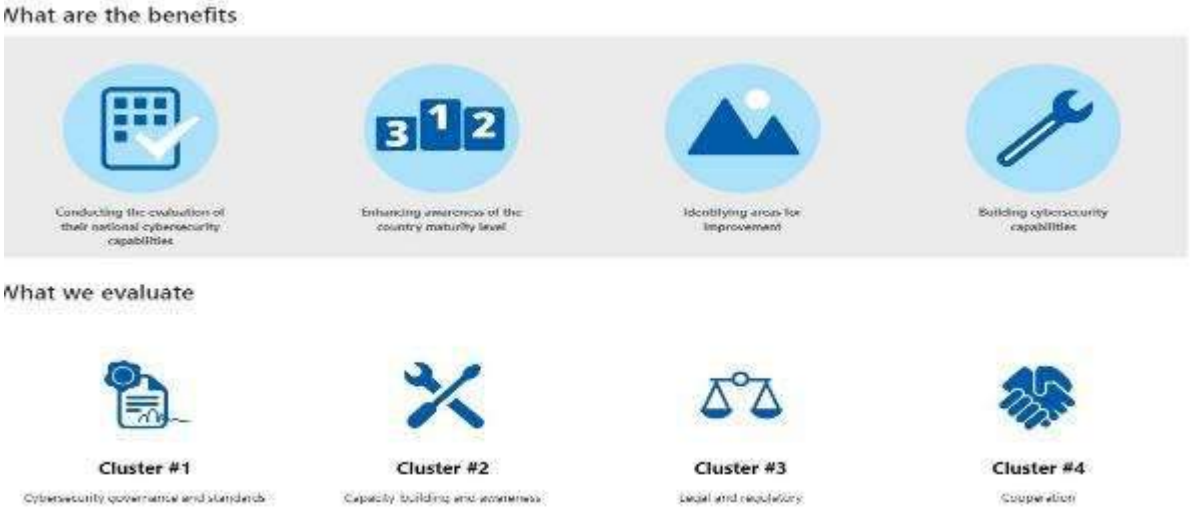
[٩] National Cybersecurity Assessment Framework tool

يساعد NCAF المسؤولين الحكوميين والمدراء التنفيذيين في تحديد مستوى الأمن السيبراني في دولهم وتحديد النواحي التي تحتاج إلى تحسين وتطوير، من خلال تقييم مخاطر الأمن السيبراني وتحليل السياسات والإجراءات والتقنيات المستخدمة في الدولة.

وتعتمد ENISA في تطبيق NCAF على عدة عناصر أساسية، بما في ذلك الأدوات والإرشادات والتدريب والتقييم، وتهدف إلى تطوير وتحسين قدرات الأمن السيبراني في الدول الأعضاء في الاتحاد الأوروبي وتعزيز الأمان السيبراني في المنطقة بشكل عام.

وتتضمن مراحل تطبيق NCAF تقييم مخاطر الأمن السيبراني وتحليل السياسات والإجراءات والتقنيات المستخدمة في الدولة، وتحديد نواحي التحسين وتطوير الخطط العمل لتعزيز الأمان السيبراني. ويمكن للدول الأعضاء في الاتحاد الأوروبي استخدام NCAF كأداة لتحسين قدرات الأمن السيبراني وتطبيق أفضل الممارسات الأمنية السيبرانية المعترف بها دوليًا، وتعزيز الأمان السيبراني في المنطقة. والحصول على الدعم والمشورة والتوجيهات من ENISA في تطبيق NCAF وتحسين قدراتهم في الأمن السيبراني.

الشكل التالي يوضح اهداف وفوائد التقييم في هذا الاطار



رابعاً:- الاداوات والمؤشرات التي تقدمها الوكالة

تقدم الوكالة العديد من الأدوات التفاعلية التي تساعد الدول في تقييم مقدراتها السيبرانية كما انها تقدم الدعم اللازم لهم من الناحية الاستشارية والتقنية والفنية لتحسين الأمن السيبراني في أوروبا، ومن بين هذه الأدوات والمؤشرات:

١- أدوات تحليل التهديدات والمخاطر: حيث توفر أدوات تحليل التهديدات والمخاطر السيبرانية للمؤسسات والحكومات، والتي تساعد على تحديد المخاطر والتهديدات وتقييم الأضرار المحتملة وتحديد الإجراءات الوقائية اللازمة.

٢- أدوات إدارة الحوادث السيبرانية: توفر ENISA أدوات إدارة الحوادث السيبرانية للمؤسسات والحكومات، تتمثل في أدوات لتحليل وتقييم وإدارة الحوادث السيبرانية والتي تساعد على الاستجابة الفعالة للهجمات السيبرانية وتقليل الأضرار.

٣- أدوات تحسين الأمن السيبراني: تقدم ENISA أدوات لتحسين الأمن السيبراني للمؤسسات والحكومات، والتي تشمل أدوات لتحسين الحماية من الهجمات السيبرانية وتحسين عمليات الرصد والكشف المبكر عن الهجمات السيبرانية وتطوير السياسات والإجراءات الأمنية السيبرانية.

٤- مؤشرات الأمن السيبراني: توفر ENISA مؤشرات الأمن السيبراني لتقييم مستوى الأمن السيبراني في أوروبا، والتي تساعد على تحديد النواحي التي تحتاج إلى تحسين وتطوير وتقييم فعالية الإجراءات الأمنية المتخذة وتحسينها. وتشمل هذه المؤشرات عدة مجالات منها: مؤشرات الأمان السيبراني للحكومات والمؤسسات، ومؤشرات الأمن السيبراني للمستهلكين، ومؤشرات الأمن السيبراني للشركات والمؤسسات الصغيرة والمتوسطة.

٥- تقدم كذلك العديد من الدراسات والأبحاث ودراسات الحالة وأدوات التقييم الحي والخرائط التفاعلية بصفة مستمرة ودائمة ومتطورة .

خامساً: إطار حوكمة استراتيجيات الأمن السيبراني .[١٠]

A Governance Framework for National Cybersecurity Strategies

في شهر فبراير من العام الجاري قامت الوكالة بإصدار هذا الاطار المرجعي الذي يركز على الممارسات الجيدة حول إطار الحوكمة لدعم تنفيذ الاستراتيجية الوطنية NCSS في الاتحاد الأوروبي. والهدف الرئيسي من هذا المخطط الإحصائي هو تقديم نظرة عامة على النتائج الرئيسية للدراسة، وربطها بالعناصر الرئيسية لإطار الحوكمة المقترح ودعمها بمشاركة إحصائيات مفيدة. علاوة على ذلك، وتتمثل أهدافه في تحديد الممارسات الجيدة التي تساهم في تصميم إطار حوكمة فعال للأمن السيبراني، وتحديد الدور الذي يتعين على الجهات المختلفة تحمله في هذا المجال كما يسلط هذا التقرير الضوء على مجموعة من الممارسات الجيدة للعناصر المختلفة للحوكمة التي وضعتها دول أوروبا لضمان إطار فعال لتنفيذ NCSSs الحالية والمستقبلية لدول الاتحاد الأوروبي، .أما منهجيته فتتضمن جمع البيانات من الأبحاث المكتبية والمقابلات مع الخبراء والمعنيين، وتحليل البيانات المجمعة وتعريف الممارسات الجيدة وتحقق منها عن طريق الخبراء الوطنيين ويحتوي هذا الاطار على العديد من العناصر الهامة والارشادات المفيدة والتي تجعله يستحق القراءة ولكن لا يسعنا المجال لعرض تفاصيلها الان .

[١٠] اصدار لإطار حوكمة استراتيجيات الأمن السيبراني الصادر عن المعهد الأمريكي للمعاييروالتكنولوجيا

الفصل الثاني

مؤشرات قياس الامن السيبراني واهميتها

ان أي اتفاق في المجتمع الدولي دائما يقابله التزام ولقياس مدى التزام الدول والأطراف في الاتفاقات لا بد من أدوات للقياس ومؤشرات لبيان معدل التقدم او الإخفاق الحاصل وعندما نتحدث عن الامن السيبراني فان الابعاد تتعدد والمصالح تتشابك لان هذا التقييم .

وهذة المؤشرات للأمن السيبراني من أهم العوامل التي تحدد مدى قدرة الدول على حماية بنيتها التحتية والمواطنين والشركات والمؤسسات من التهديدات السيبرانية كما تعد جزء من المقدرة العسكرية للدولة والمكانة الاقليمية والهيمنة العالمية والقدرة على الردع وصد الاخرين عن العبث بمقدراتها إضافة لكون اصبح جزءاً من التقييم العسكري والأمني وداعم للاقتصاد والاستثمار في الدول.

الامر الذي دعا المجتمع الدولي الى إيجاد اليات لقياس الأداء زمدى الالتزام ومستوى التقدم خلال مدى معينة، فظهرت العديد من المؤشرات الدولية والعالمية ومنها :-

١. مؤشر الأمن السيبراني العالمي[١١] Global Cybersecurity Index (GCI) وهو مؤشر يصدره مركز الأمن السيبراني العالمي، في الاتحاد الدولي للاتصالات ITU ويقيس مدى قدرة الدول على حماية بنيتها التحتية السيبرانية والمواطنين والشركات والمؤسسات من التهديدات السيبرانية، ويتم تنفيذه بشكل دوري بناءً على خمسة محاور رئيسة؛ المحور القانوني والمحور التقني والمحور التنظيمي ومحور بناء القدرات ومحور التعاون، وذلك من خلال تحليل أداء الدول في ٨٠ مؤشرًا فرعيًا، بهدف رفع مستوى الأمن السيبراني وتعزيز تبادل الخبرات ومشاركة التجارب بين دول العالم[١٢] .
٢. مؤشر الأمن السيبراني للاتحاد الأوروبي :Network and Information Security (NIS) وهو مؤشر يصدره الاتحاد الأوروبي، ويقيس مدى قدرة الدول الأعضاء في الاتحاد على حماية بنيتها التحتية السيبرانية والمواطنين والشركات والمؤسسات من التهديدات السيبرانية. ويتم حساب المؤشر والتقييم على أساس عدة عوامل، مثل الحماية السيبرانية والتحكم في الأمن السيبراني وادارته والتوعية السيبرانية والتدريب والتعاون الدولي وتقييم المخاطر ويتم تطبيق هذا المؤشر على مختلف القطاعات ، بما في ذلك القطاعات الحكومية والخاصة والمؤسسات الصغيرة والمتوسطة الحجم تم إطلاقه في عام ٢٠١٨ وتم تطويره بالتعاون مع وكالة الاتحاد الأوروبي للأمن السيبراني[١٣](ENISA) .
٣. مؤشر الامن السيبراني الوطني[١٤] National Cyber Security Index (NCSI) يستخدم لتقييم مستوى الأمن السيبراني في البلاد وتحديد المجالات التي تحتاج إلى تحسين .ويتم إصدار المؤشر من قبل مركز الأمن السيبراني الوطني في استونيا (NCSC)، ويتم تحديثه بانتظام ونشره على موقع NCSC. ويتم تقييم المؤشر على أساس عدة معايير، بما في ذلك مستوى الحماية من الهجمات السيبرانية ومستوى الوعي بالأمن السيبراني والتعاون بين القطاعين العام والخاص في مجال الأمن السيبراني.

---

[١١] Global Cybersecurity Index
[١٢] الموقع الرسمي للمركز الوطني الارشادي للأمن السيبراني السعودي
[١٣] (European Network and Information Security Agency - ENISA)
[١٤] National Cyber Security Index (NCSI

بالإضافة لهذة المؤشرات توجد العديد من المؤشرات الأخرى ومنها Cybersecurity Exposure Index (CEI) و Cyber Threat Index و Global Cybersecurity Outlook و Cybersecurity legislation and regulations ولكننا سنقصر العرض على مؤشرين فقط الأول وهو الأهم والاشهر والاوثق عالمياً مؤشر الأمن السيبراني العالمي GCI الصادر عن الاتحاد الدولي للاتصالات والثاني مؤشر الامن السيبراني الوطني NCSI الصادر عن جهة اكاديمية مستقلة في دولة استونيا .

المبحث الأول

المؤشر العالمي للأمن السيبراني Global Cybersecurity Index (GCI)

يعتبر المؤشر العالمي للأمن السيبراني واحد من أهم التقارير العالمية في مجال الأمن السيبراني السنوية. بدأ هذا المؤشر منذ عام ٢٠٠٧ بتقرير واحد ولكنه ازداد ليصدر ٦ تقارير بحلول عام ٢٠١٩ ، حيث يقيم امن ١٦٥ دولة ومناطق مستقلة حول العالم في مجالات السياسات والتشريعات والبنية التحتية وقدرات مكافحة الجرائم الإلكترونية وبناء القدرات والتعاون الدولي. تقوم مجموعة من الخبراء المستقلين بإعداد تقرير سنوي لكل دولة يقيم جاهزيتها لمواجهة التهديدات الإلكترونية على أساس معايير شاملة وموضوعية ، ثم يرتب ترتيب الدول من ١ إلى ١٦٥ تنازليًا حسب نتائج التقييم.

يعتبر تقرير المؤشر العالمي للأمن السيبراني مرجعاً هاماً لصانعي السياسات والأوساط الأكاديمية والصناعية ، حيث يمثل التقييم الأكثر شمولاً للقدرات الإلكترونية للدول ويساعد هذا التقرير الدول في تحديد اولوياتها الوطنية في مجال أمن المعلومات ووضع استراتيجيات لتطوير قدراتها. كما يساعد المنظمات الدولية على فهم كيفية دعم الدول ومساعدتها في بناء قدراتها في مجال تكنولوجيا المعلومات والاتصالات.

يغطي هذا المؤشر حالياً ١٨٢ دولة وإقليماً حول العالم ووصلت الى ١٩٦ دولة وإقليم ويقيّم جاهزيتها في مجال أمن المعلومات وفقاً لستة محاور رئيسية هي: السياسات والاستراتيجيات الوطنية، والبنية التشريعية والتنظيمية، والبنية التحتية الفنية، والقدرات الوطنية للاستجابة للحوادث الإلكترونية، وبناء القدرات على المستويين الوطني والدولي، وأخيراً التعاون الدولي من خمس دعائم وفقاً للاصدار الخامس منه .

يعتمد المؤشر في تقييمه على منهجية علمية تعتمد على مجموعة من المؤشرات الفرعية ضمن كل محور من المحاور الستة. تم تطوير هذه المؤشرات بالتعاون مع فريق من الخبراء الدوليين المستقلين في مجال أمن المعلومات وحوكمة الإنترنت من أجل ضمان الشفافية والموضوعية. يتم تقييم كل دولة على حدة من قبل فريق من الخبراء المستقلين الذين يعدون تقريراً سنوياً لكل دولة يلخص نقاط القوة والضعف في بيئة أمن المعلومات فيها.

يعتمد المؤشر في عملية تقييم الدول على مصادر متنوعة من بيانات لكل دولة تشمل التقارير والدراسات الصادرة عن الحكومات والمنظمات الدولية إضافة إلى التعليقات والمدخلات من خبراء محليين. يتم التحقق من صحة هذه المعلومات ومقارنتها قبل استخدامها في عملية التقييم.

تساعد نتائج هذا المؤشر الدول على وضع خطط وبرامج محددة لتحسين وضع أمن المعلومات لديها، كما يستخدم من قبل المنظمات الدولية لتقديم الدعم اللازم للدول لبناء قدراتها. لذا فإن المؤشر يلعب دوراً هاماً في تعزيز أمن المعلومات على الصعيد العالمي من خلال تسليط الضوء على مواطن الضعف وتقديم التوصيات المناسبة لمعالجتها و دعم الدول في جهودها لخلق بيئة آمنة رقمياً.

مجال التطبيق

الرقم القياسي العالمي"المؤشر العالمي" للأمن السيبراني GCI هو رقم قياسي مركب يجمع مجموعة متنوعة من مؤشرات الأمن السيبراني في مقاييس، استنادا إلى الدعائم الخمس للبرنامج العالمي للأمن السيبراني GCA وهذه الدعائم تشكل الدعائم الخمس للرقم القياسي العالمي للأمن السيبراني. وتتمثل الأهداف الرئيسية للرقم القياسي العالمي للأمن السيبراني GCI في قياس ما يلي : -

١- أنواع ومستويات وتطور الالتزامات الوطنية المتعلقة بالأمن السيبراني بمرور الزمن
٢- التقدم المحرز في الالتزام بالأمن السيبراني من منظور عالمي
٣- التقدم المحرز في الالتزام بالأمن السيبراني من منظور إقليمي
٤- فجوة الالتزام بالأمن السيبراني: الفرق بين البلدان من حيث مستوى التزامها في مبادرات بالأمن السيبراني

ويهدف الرقم القياسي العالمي للأمن السيبراني إلى مساعدة البلدان في تحديد مجالات التحسين في مضمار الأمن السيبراني، مما يساعد على رفع المستوى الإجمالي للأمن السيبراني على الصعيد العالمي. ويجمع الرقم القياسي أيضا الممارسات الرشيدة التي يمكن للبلدان أن تتعلم منها بغية تحسين ممارساتها في مجال الأمن السيبراني واعتماد نهج أكثر اتساقاً.

محاور التقييم [١٥]في تقرير المؤشر العالمي للامن السيبراني " دعائم ومجالات الالتزام "

ويعبر عنها الشكل التالي

ونوردها تفصيلاً وبحسب وثائق الاتحاد الدولي للاتصالات المنظمة لذلك كما يلي

١- التدابير القانونية:

وهي الأدوات التشريعية، مثل القوانين واللوائح والسياسات، وتُعرف الحقوق، والمسؤوليات، والحماية المقدمة بشأن القضايا الرئيسية المتعلقة بالأمن السيبراني، مثل مسألة حظر سلوك جنائي محدد أو فرض الحد الأدنى من المتطلبات التنظيمية .

التشريع من التدابير الحاسمة لتوفير إطار منسق للكيانات لتهيئة نفسها لقاعدة تشريعية وتنظيمية مشتركة، سواء فيما يتعلق بمسألة حظر سلوك جنائي محدد أو فرض الحد الأدنى من المتطلبات التنظيمية .ويمكن قياس البيئة القانونية انطلاقاً من وجود المؤسسات القانونية والأطراف الفعالة التي تتعامل مع الأمن السيبراني والجريمة السيبرانية ، وذلك بالتحقق من وجود مؤشرين هما قانون الجريمة السيبرانية و لوائح للأمن السيبراني .

[١٥] Global Cybersecurity Agenda (GCA)

٢- التدابير التقنية:

بدون وجود تدابير وقدرات تقنية مناسبة لكشف الحوادث والتعاطي معها، تظل الدول الأعضاء والكيانات التابعة لها عرضة للمخاطر السيبرانية التي يمكن أن تقوض فوائد التكنولوجيات الرقمية. ومن ثم يتعين على الدول الأعضاء أن تمتلك القدرة على وضع استراتيجيات وتحديد معايير مقبولة للحد الأدنى من الأمن وبرامج اعتماد للتطبيقات والأنظمة البرمجية. ويمكن قياس التدابير التقنية بناءً على مدى وجود المؤسسات والأطر التقنية التي تتعامل مع الأمن السيبراني والتي تقرها أو تستحدثها الدول الأعضاء، وتتألف من افرقة التصدي للحوادث الحاسوبية الوطنية والحكومية وكذا الافرقة القطاعية CERT/CIRT/CSRIT ، الاطار الوطني لتنفيذ المعايير ومنها الوكالات التالية: المنظمة الدولية للتوحيد القياسي ISO ، والاتحاد الدولي للاتصاالت ITU وفريق مهام هندسة الإنترنت IETF ومعهد مهندسي الكهرباء والإلكترونيات IEEE وتحالف حلول صناعة الاتصالات ATIS ومنظمة تطوير معايير المعلومات المنظمة OASIS ومشروع شراكة الجيل الثالث GPP٣ والمشروع ٢ لشراكة الجيل الثالث ٢GPP٣ و IAB ،وجمعية الإنترنت (ISOC ،(و ISG ،و ISI ،والمعهد الأوروبي لمعايير الاتصالات (ETSI ،(وISF ،و RFC ،و ISA ،واللجنة الكهرتقنية الدولية (IEC ،(و NERC ،و NIST ،و FIPS ،و PCI ،و DSS ،وغيرها .

٣- التدابير التنظيمية:

التدابير التنظيمية والإجرائية ضرورية من أجل التنفيذ السليم للمبادرات الوطنية. فيجب على الدولة العضو تحديد هدف استراتيجي واسع، مع خطة شاملة من أجل التنفيذ والمتابعة والقياس. ويتعين إنشاء هياكل على غرار الوكالات الوطنية من أجل تنفيذ استراتيجيات الأمن السيبراني وتقييم نجاح أو فشل الخطة. ويمكن قياس الهياكل التنظيمية بناءً على وجود وعدد المؤسسات والاستراتيجيات التي تنظم تطوير الأمن السيبراني على الصعيد الوطني.

وننصمن وضع الاستراتيجية الوطنية للامن السيبراني والسياسة الوطنية لها وتحديد الوكالة المسؤولة ومقاييس الامن السيبراني و استراتيجيات ومبادرات حماية الأطفال على الأنترنت COP

٤- تدابير تنمية القدرات:

تنمية القدرات عنصر مالزم للتدابير القانونية والتقنية والتنظيمية. ويمكن لفهم التكنولوجيا والمخاطروالتداعيات في مجال الأمن السيبراني أن يساعد على وضع الأفضل من التشريعات والسياسات والاستراتيجيات والتنظيم للأدوار والمسؤوليات المختلفة. وتشمل تنمية القدرات تطوير المعارف والمهارات بين السكان الأساسيين والمهنيين الذين يتطرق عملهم إلى الأمن السيبراني، فضلاً عن المتخصصين ضمن القطاع.

ويجب ان تشمل على حملات التوعية بالامن السيبراني و تدريب العاملين في مجال الامن السيبراني والبرامج التعليمية المتعلقة بالأمن السيبراني كجزء من المناهج الأكاديمية الوطنية وبرامج البحث والتطوير D&R في مجال الأمن السيبراني والصناعة الوطنية للأمن السيبراني واية اليات تحفيز حكومية او تدابير او حوافز .

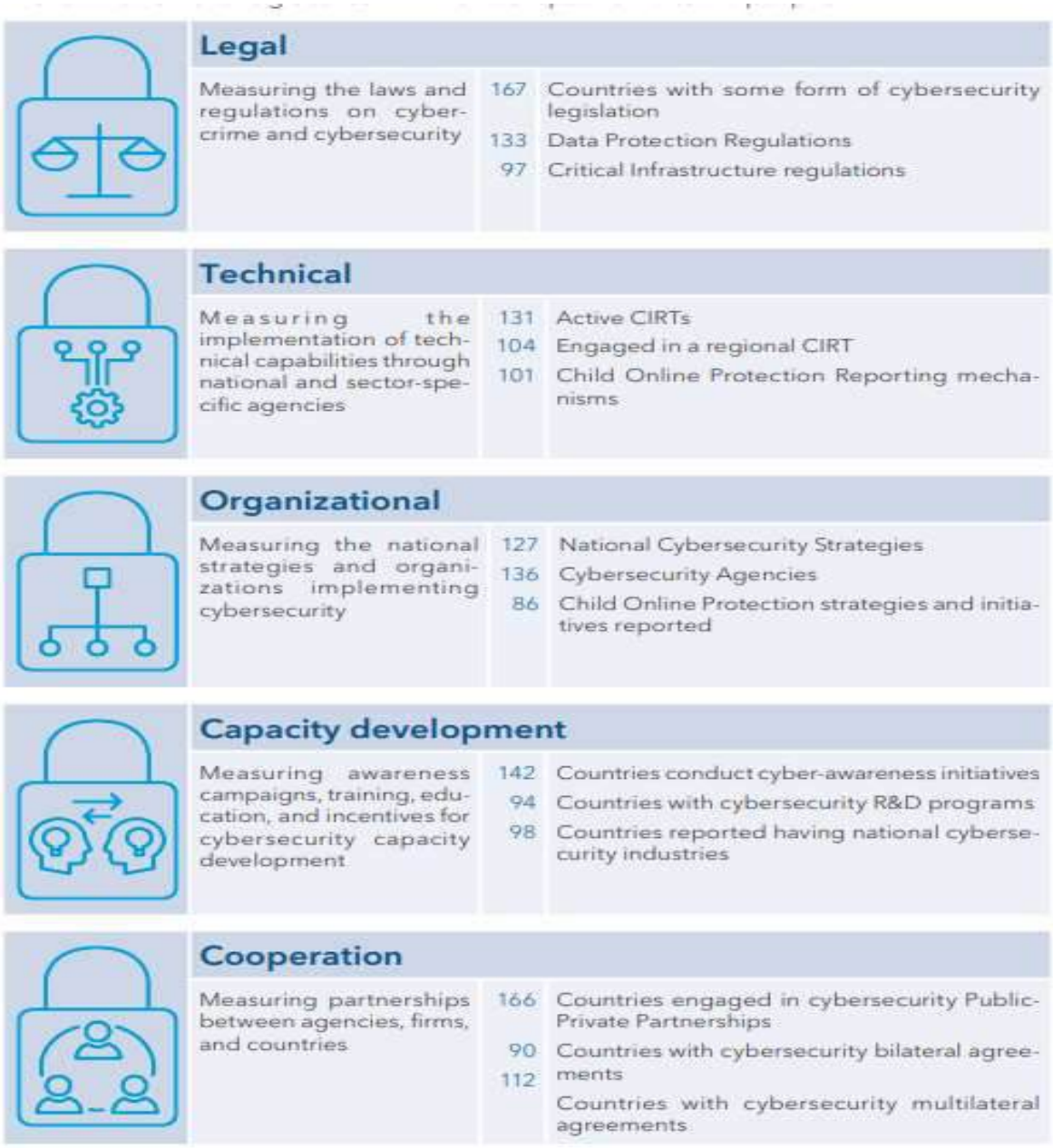
٥- التدابير التعاونية:

تتكلل جهود الأمن السيبراني بالمزيد من النجاح عندما تعتمد على جميع القطاعات والتخصصات المتأثرة، ويتعين الاضطلاع بها باتباع نهج شمولي متعدد أصحاب المصلحة. ويعزز التعاون الحوار والتنسيق ويمكن من إيجاد مجال أكثر شمولية لتطبيق الأمن السيبراني. ويمكن أن يشمل التعاون أنشطة

من قبيل المبادرات المشتركة وتبادل المعلومات والدورات التدريبية وغيرها من الأنشطة التي تربط بين المهنيين والمسؤولين وسائر الجهات الفاعلة التي تسعى إلى تحسين الأمن السيبراني.

ويمكن التحقق من حصول هذا التعاون من خلال الاتفاقات الثنائية [١٦]بشأن الأمن السيبراني والاتفاقات متعددة الأطراف بشأن الأمن السيبراني واتفاقات المساعدة القانونية المتبادلة بشأن الأمن السيبراني والشراكات بين القطاعين العام والخاص والشراكات بين الوكالات .[١٧]

شكل يبين المعايير والنتائج وفقاً للتقرير الأخير للاتحاد الدولي للاتصالات



[١٦] اشكال الشراكة بين القطاعين العام والخاص موقع البنك الدولي
[١٧] The Global Cybersecurity Index (GCI)

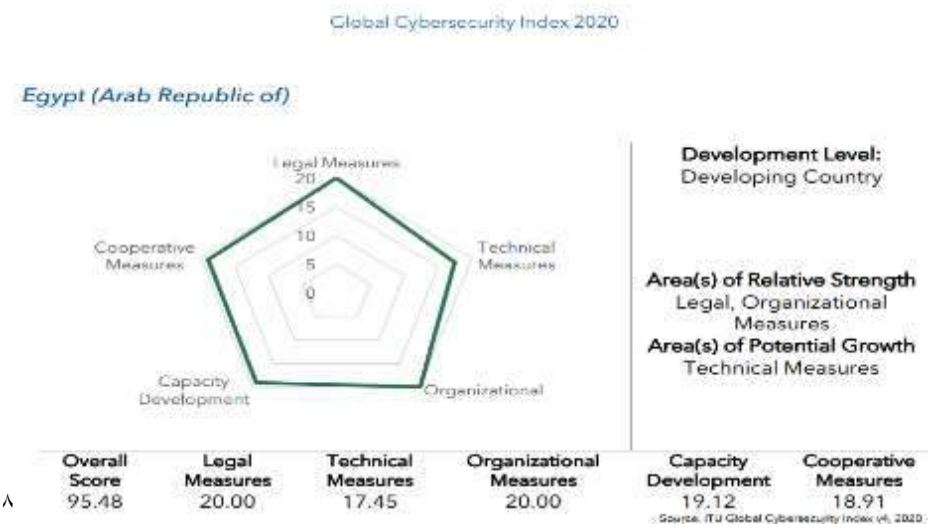
ترتيب مصر وفقاً للمؤشر العالمي للأمن السيبراني

يختلف عدد وشكل الأسئلة ومعايير التقييم وتتطور من عام الى اخر وتزداد المنهجية وضوحاً على جميع مستويات التقييم في المؤشر، وقد كانت مصر في طليعة دول العالم التي ساهمت في وجود التقارير الصادرة عن المؤشر منذ نشأته .

مؤشرالأمن السيبراني GCI الصادر عن الاتحاد الدولي للاتصالات كشف عن احتلال مصر خلال ٢٠٢٠ المركز ٢٣ عالميا بين ١٨٢ دولة بـ ٩٥,٤٥ درجة، بينما تصدرت أمريكا المؤشر بـ ١٠٠ درجة، تلتها بريطانيا في المركز الثاني بـ ٩٩,٥٤ درجة، ثم السعودية في المركز الثاني مكرر بـ ٩٩,٥٤ درجة، كاشفا عن أن مصر اتخذت خطوات هامة لدعم الأمن السيبراني من أهمها: تأسيس مجلس أعلى للأمن السيبرانى في عام ٢٠١٥ ووضع استراتيجية وطنية للأمن السيبراني ٢٠١٧-٢٠٢١، إلى جانب تأسيس المركز الوطني للاستعداد لطوارئ الحاسبات والشركات . EG-CERT .

صدر عن المؤشر أربعة إصدارات حتى الان ويتم الاعداد للاصدار الخامس علماً بأن هذه الإصدارات غير دورية حتى الان فقد صدرت في أعوام ٢٠١٤ و٢٠١٧ و٢٠١٨ و٢٠٢٠ وقد احتلت مصر مراكز متقدمة في هذا المؤشر على النحو التالي :-

شكل مقتبس من تقرير الاتحاد الدولي للاتصالا ت GCI٢٠٢٠ يبين وضع مصر في التقرير علماً بانها احتلت المركز الثاني افريقياً والرابع عربياً والثالث والعشرون عالمياً في هذا التقرير



١٨

عالمياً : ترتيب مصر

٢٠١٤ في المركز "٩"[١٩] التاسع مكرر

٢٠١٧ في المركز "١٤" الرابع عشر

٢٠١٨ في المركز "٢٣" الثالث والعشرون

٢٠٢٠ في المركز "٢٣" الثالث والعشرون [٢٠]

[١٨] Global Cybersecurity Index ٢٠٢٠

[١٩] وزارة الاتصالات وتكنولوجيا المعلومات المركز الإعلامي

[٢٠] موقع اليوم السابع : معلومات الوزراء: مصر ٢٣ عالميًا بين ١٩٤ دولة فى الأمن السيبرانى

عربياً : ترتيب مصر

٢٠١٤ في المركز "٣" الثالث / عمان الأولى / قطر الثانية

٢٠١٧ في المركز"٢" الثاني / عمان الأولى

٢٠١٨ في المركز "٤" الرابع / السعودية الأولى / عمان الثانية / قطر الثالثة

٢٠٢٠ في المركز "٤" الرابع /السعودية الأولى / الامارات الثانية / عمان الثالثة

افريقياً : ترتيب مصر

٢٠١٤ في المركز "١" الأولى افريقياً

٢٠١٧ في المركز" ١" الأولى افريقياً

٢٠١٨ في المركز "٢" الثاني افريقيا / الأولى موريشيوس

٢٠٢٠ في المركز "٢" الثاني افريقيا / الأولى موريشيوس

تساهم مصر بفاعلية في اعداد هذة الإصدارات الخاصة بالمؤشر وتعد من الشركاء الفاعلين فيه [٢١]

[٢١] GCI ٢٠٢٠ WEIGHTAGE PROCESS AND PARTNERS ITU

المبحث الثاني

المؤشر الوطني للأمن السيبراني National Cyber Security Index (NCSI)

يعتبر المؤشر الوطني للأمن السيبراني National Cyber Security Index (NCSI) من أهم المؤشرات التي تستخدم لقياس مدى تطور الدول في مجال الأمن السيبراني. وهو مؤشر عالمي يصدره مركز الأمن السيبراني الوطني في إستونيا، ويقوم بتقييم مستوى الأمن السيبراني في الدول المشاركة فيه. ويتم تحديث المؤشر سنوياً، حيث يتم إصدار تقرير يتضمن نتائج التقييم وترتيب الدول في المؤشر.

تعتمد عملية تقييم المؤشر على مجموعة من المعايير والمؤشرات التي تشمل السياسات والاستراتيجيات الخاصة بالأمن السيبراني، وكذلك القدرة على التعامل مع الهجمات الإلكترونية والحماية منها، والتوعية والتدريب والتطوير التقني، بالإضافة إلى القدرة على التعاون الدولي في مجال الأمن السيبراني.

ويمثل المؤشر الوطني للأمن السيبراني مصدراً مهماً للمعلومات والبيانات المتعلقة بالأمن السيبراني، حيث يساعد على تحديد المجالات التي تحتاج إلى تحسين وتعزيز في الدول المشاركة، ويعمل على توفير إطار للتعاون الدولي في مجال الأمن السيبراني، حيث يتضمن تقييماً لأكثر من ١٦٠ دولة حول العالم. ويتميز المؤشر بأنه يشمل الدول المتقدمة والنامية على حد سواء، ويعتمد على معايير موحدة لتقييم جميع الدول المشاركة في المؤشر.

ويتم تقييم الدول المشاركة في المؤشر على سبعة مجالات رئيسية، وهي السياسات والإستراتيجيات والقوانين والتشريعات، والحماية الفعالة من الهجمات الإلكترونية، والقدرة على الكشف عن الهجمات والتحقق منها، والتوعية والتدريب والتطوير التقني، والتعاون الدولي، بالإضافة إلى القدرة على الإستجابة للحوادث السيبرانية وإدارتها.

ويعتمد المؤشر الوطني للأمن السيبراني على منهجية تقييم شاملة ودقيقة، حيث يتم جمع البيانات والمعلومات من مصادر مختلفة ومتعددة، ويتم تحليلها وتقييمها بشكل دقيق وشامل. وتوفر البيانات المقدمة من قبل المؤشر الوطني للأمن السيبراني معلومات قيّمة للدول والمؤسسات التي تعمل في مجال الأمن السيبراني، حيث تساعد على تحديد النقاط القوية والضعف في هذا المجال، وبالتالي تمكنها من تحسين أدائها وتعزيز قدراتها في الأمن السيبراني.

ويمكن الإستفادة من المؤشر الوطني للأمن السيبراني في تطوير السياسات والإستراتيجيات الخاصة بالأمن السيبراني، وفي تعزيز التعاون الدولي في هذا المجال، وكذلك في توفير المعلومات القيمة للمؤسسات والشركات التي تعمل في مجال التكنولوجيا والإنترنت. ويعتبر المؤشر الوطني للأمن السيبراني أداة مهمة لتعزيز الأمن السيبراني في جميع أنحاء العالم، وللمساهمة في تحقيق التنمية المستدامة والاقتصاد الرقمي.

يعتبر المؤشر الوطني للأمن السيبراني NCSI مؤشر تفاعلي للغاية حتى اننا وجود صعوبة في عرضه وتبسيط منهجيته ولكن سنوجزها قدر الإمكان ويتم فيها أولاً تحديد المخاطر السيبرانية الرئيسية ثم تحديد القدرات والتدابير الأمنية اللازمة ثم اختيار الجوانب الهامة والقابلة للقياس وبعدها تطوير مؤشرات الأمن السيبراني واخيرً تجميع مؤشرات الأمن السيبراني في صورة تقارير.

يتم ذلك من خلال **رؤية** مفادها تطوير أداة شاملة لقياس الأمن السيبراني توفر معلومات عامة دقيقة وحديثة حول الأمن السيبراني عالمياً، من خلال بناء مؤشرات دقيقة وأدوات واضحة ووثائق مفيدة.

اطار الامن السيبراني الوطني [٢٢]

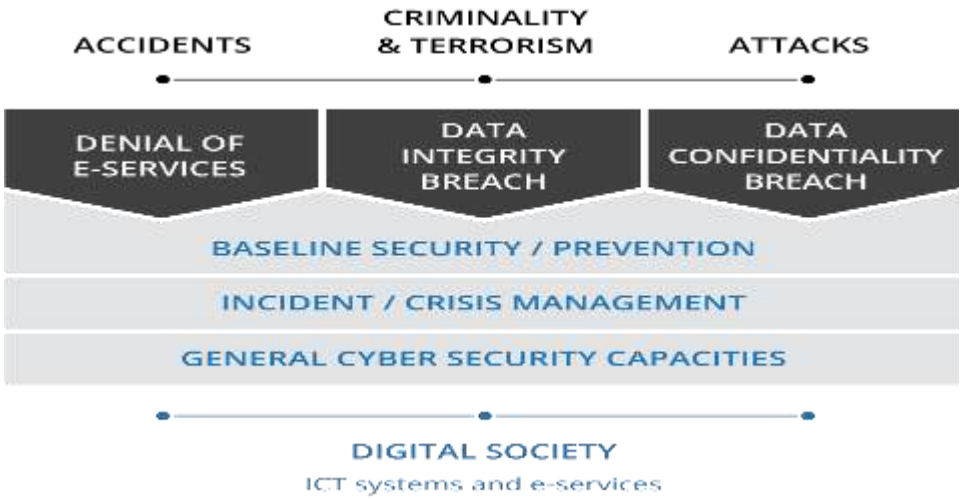
تم تطوير مؤشرات مركز الأمن السيبراني الوطني وفقًا لإطار الأمن السيبراني الوطني حيث يتم تقديم المخاطر السيبرانية الأساسية وهي:

١. حجب الخدمات الالكترونية - عدم إمكانية الوصول إلى الخدمات .

٢. اختراق سلامة البيانات والتعديل غير المصرح به

٣. انتهاك سرية البيانات - تعرض السرية

تؤثر هذه المخاطر بشكل مباشر على الوظائف الطبيعية للأنظمة الوطنية للمعلومات والاتصالات ومن كافة أنظمة تكنولوجيا المعلومات والاتصالات وكذلك تؤثر على الخدمات الإلكترونية (بما فيها الخدمات الإلكترونية الحرجة او الحساسة)، ولكي يتمكن البلد من إدارة هذه الأخطار السيبرانية، يجب أن يكون لديه قدرات مناسبة للحصول على أمان سيبراني أساسي، وإدارة الحوادث، وتطوير الأمن السيبراني بشكل عام.



التركيز والنطاق

يركز مركز الأمن السيبراني الوطني على الجوانب القابلة للقياس للأمن السيبراني التي تم تنفيذها من قبل الحكومات المركزية، وتشمل:

١. التشريعات المعمول بها - الأنظمة القانونية واللوائح والأوامر الخ.

٢. الوحدات المنشأة - المنظمات والإدارات الموجودة وما إلى ذلك.

٣. تنسيق الأشكال - اللجان والفرق العاملة وما إلى ذلك.

٤. النتائج - السياسات والتمارين والتقنيات والمواقع الإلكترونية والبرامج وما إلى ذلك.

[٢٢] NATIONAL CYBER SECURITY FRAMEWORK

ألية العمل في المؤشر الوطني للأمن السيبراني وتطويره

NCSI DEVELOPMENT PROCESS

١. تحديد الأخطار السيبرانية على المستوى الوطني.

٢. تحديد التدابير والقدرات الأمنية السيبرانية.

٣. اختيار الجوانب الهامة والقابلة للقياس.

٤. تطوير مؤشرات الأمن السيبراني.

٥. تجميع مؤشرات الأمن السيبراني.

أسس ومعايير التقييم في المؤشر الوطني للأمن السيبراني NCSI.

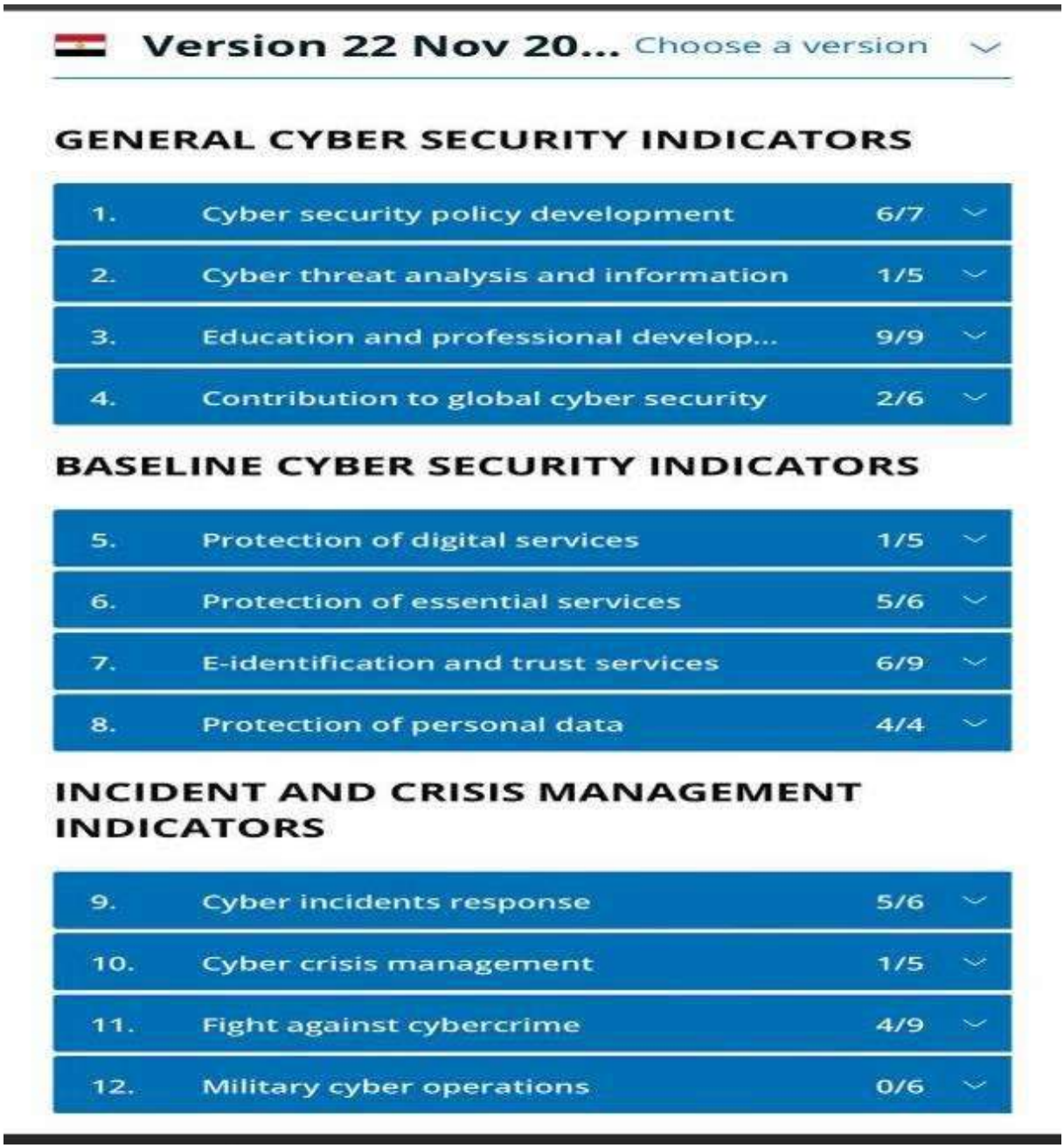
يتخذ المؤشر معيار علمية محددة وواضحة وتتسم بالشفافية والمرونة فقد قسم تلك المعايير على ثلاث فئات أساسية ينبثق عن كل منها أربعة فروع او مكونات رئيسية بإجمالي ١٢ مكون يندرج تحتهم عدد ٦٤ مؤشر فرعي لكل مؤشر ثقل وتقدير معين يقدر بنقطة أو أقل أو اكثر حسب وزن ذلك المؤشر على التفصيل التالي :-

١- مؤشرات الأمن السيبراني العامة .
   - تطوير سياسة الأمن السيبراني .
   - تحليل التهديدات السيبرانية والمعلومات .
   - التعليم والتطوير المهني .
   - المساهمة في الأمن السيبراني العالمي .
٢- مؤشرات الأمن السيبراني الأساسية.
   - حماية الخدمات الرقمية.
   - حماية الخدمات الرقمية الأساسية.
   - خدمات تحديد الهوية والثقة الإلكترونية.
   - حماية البيانات الشخصية.
٣- مؤشرات إدارة الحوادث والأزمات.
   - الاستجابة للحوادث السيبرانية.
   - إدارة الأزمات السيبرانية.
   - محاربة جرائم الأمن السيبراني.
   - العمليات العسكرية السيبرانية.

- كل مجال فرعي مما سبق يأتي أسفله عدد من الأسئلة لكل منها وزن مختلف يتم على أساسه منح نقاط واجراء التقييم وبعد صدور التقرير يتم النشر مدعوماً برابط الجهة او الدليل او مصدر ونوع الإجابة على المؤشر المطلوب.

تقييم مصر وفقاً للمؤشر الوطني للأمن السيبراني NCSI

صدر عن المؤشر ثلاث تقارير أولها في مارس ٢٠١٨ والثاني في مايو ٢٠١٨ والثالث في نوفمبر ٢٠٢١ وتحتل مصر بحسب التقرير الأخير المركز ٦٠ عالمياً بمجموع نقاط ٥٧،١٤ % على النحو المبين تفاصيله بالشكل التالي [٢٣]



[٢٣] حالة مصر وفق تقرير ٢٠٢١ للمؤشر الوطني للأمن السيبراني

- وفي رأينا الشخصي في الختام حتى وان لم يكن لهذا المؤشر حظ من الشهرة والتقدير الدولي الا اننا نراه مصدر ثري للمعلومات والبيانات الموثقة عن الأمن السيبراني وبذات الطريقة التي تستخدمها الوكالة الأوروبية للأمن السيبراني ، كما انه يساعد في تقييم مدى تطور الدول في هذا المجال. ويمكن استخدام المعلومات والبيانات المقدمة من المؤشر في تحسين الأداء وتعزيز القدرات في مجال الأمن السيبراني، وتحديد نقاط القوة والضعف وتطوير السياسات والإستراتيجيات الخاصة بالأمن السيبراني. ويعكس المؤشر أهمية الأمن السيبراني في العالم الرقمي الحالي، ويعمل على تحقيق التنمية المستدامة والاقتصاد الرقمي.

حاتم جعفر

القاهرة أغسطس ٢٠٢٤