جمهورية مصر العربية
رئاسة مجلس الوزراء
المجلس الأعلى للأمن السيبراني

الاستراتيجية الوطنية للأمن السيبراني (٢٠١٧-٢٠٢١)

الاستراتيجية الوطنية للأمن السيبراني (٢٠١٧-٢٠٢١)

> أمن الفضاء المعلوماتي جزء أساسى من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه، على النحو الذي ينظمه القانون

مـــادة (٣١) من الـدسـتـــور المصـري (ينـــاير ٢٠١٤)

مقـــدمـة

في إطار جهود الدولة لدعم الأمن القومي وتنمية المجتمع المصري، ومع تزايد التهديدات والتحديات المستقبلية فى المجال السيبراني والمجتمع الرقمي ولرصد ومجابهة المخاطر والتهديدات المتزايدة، وانطلاقًا من الأهداف التي دعت الي انشاء المجلس الأعلى لتأمين البني التحتية للاتصالات والمعلومات (المجلس الأعلى للأمن السيبراني) التابع لرئاسة مجلس الوزراء، برئاسة وزير الاتصالات وتكنولوجيا المعلومات، وتكليفه بوضع استراتيجية لتأمين البني التحتية للاتصالات والمعلومات بشكل متكامل لتوفير البيئة الآمنة لمختلف القطاعات لتقديم الخدمات الإلكترونية المتكاملة، تم اعدد هذه الوثيقة الاستراتيجية الوطنية للأمن السيبراني.

وتتضمن الاستراتيجية عددًا من البرامج التي تدعم الأهداف الاستراتيجية للأمن السيبراني. كما توضح توزيع الأدوار بين الجهات الحكومية والقطاع الخاص ومؤسسات الاعمال والمجتمع المدني وما ستقوم به الدولة من إجراءات للتقدم نحو تحقيق تلك الأهداف. فضلاً عن ذلك، تقدم الاستراتيجية ملامح خطة عمل تمتد على مدار الأعوام ٢٠١٧-٢٠٢١. وقد تم وضع الخطة مرتبة وفقًا للأهداف، مع التأكيد علي أهمية الشراكة المجتمعية بين الأجهزة الحكومية والقطاع الخاص ومؤسسات الاعمال والمجتمع المدني لتنفيذ تلك الأهداف والإجراءات ذات الصلة، بما يدعم التحول نحو اقتصاد رقمي متكامل يحقق طموحات المواطنين في تنمية اجتماعية واقتصادية شاملة ويحمي مصالحهم، ويحافظ علي مصالح الدولة العليا ويسهم في نهضتها وازدهارها ورخاءها.

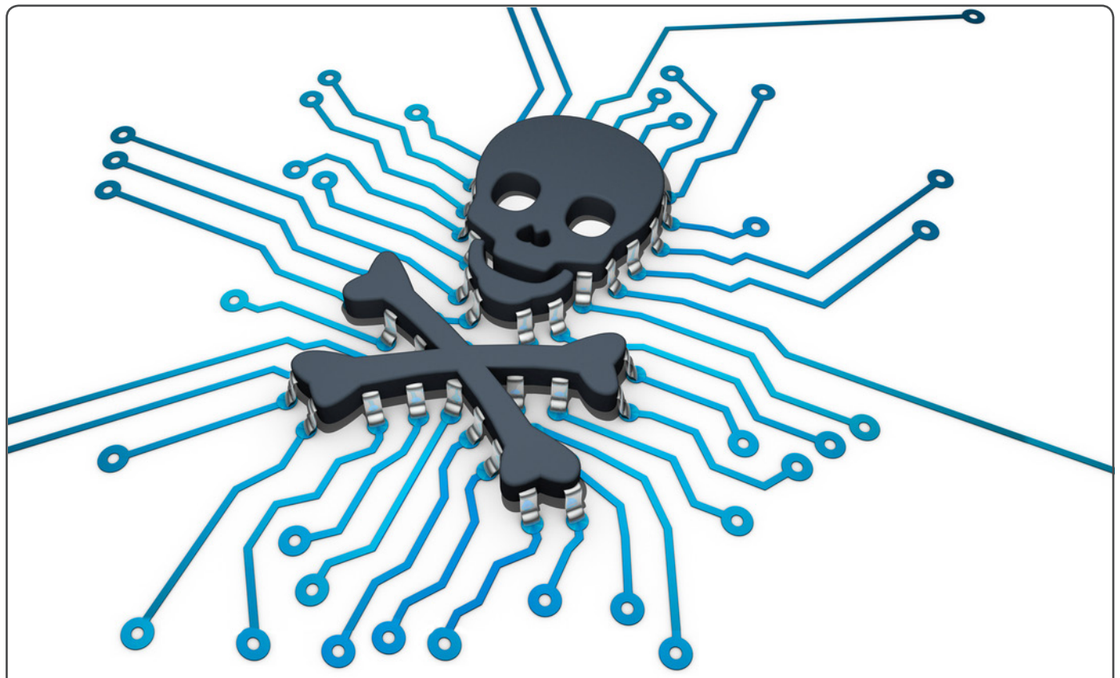
خلفيـــه

شهدت الثلاث عقود الماضية انتشارا متصاعدا لأعداد مستخدمي شبكة الانترنت والهواتف الذكية واستخداماتها في مجالات الاعمال والتجارة والخدمات الحكومية والتعليم والمعرفة والترفيه والسياحة والرعاية الصحية وغيرها من الأنشطة الاقتصادية والاجتماعية والثقافية. ومع الفرص التي يمثلها النمو المستمر في اعداد مستخدمي شبكات الاتصالات والانترنت والانتشار المتزايد في المعاملات والخدمات الالكترونية، تبرز أهمية مواجهة الاخطار والتحديات التي تستهدف البني التحتية للاتصالات والمعلومات حيث أنها تهدد المعاملات وتقديم الخدمات بوجه عام، وتقلص الثقة في الخدمات والاعمال الالكترونية بوجه خاص.

وأهـــم تـلك التحـديـات والأخطـــار السيبرانية هي:

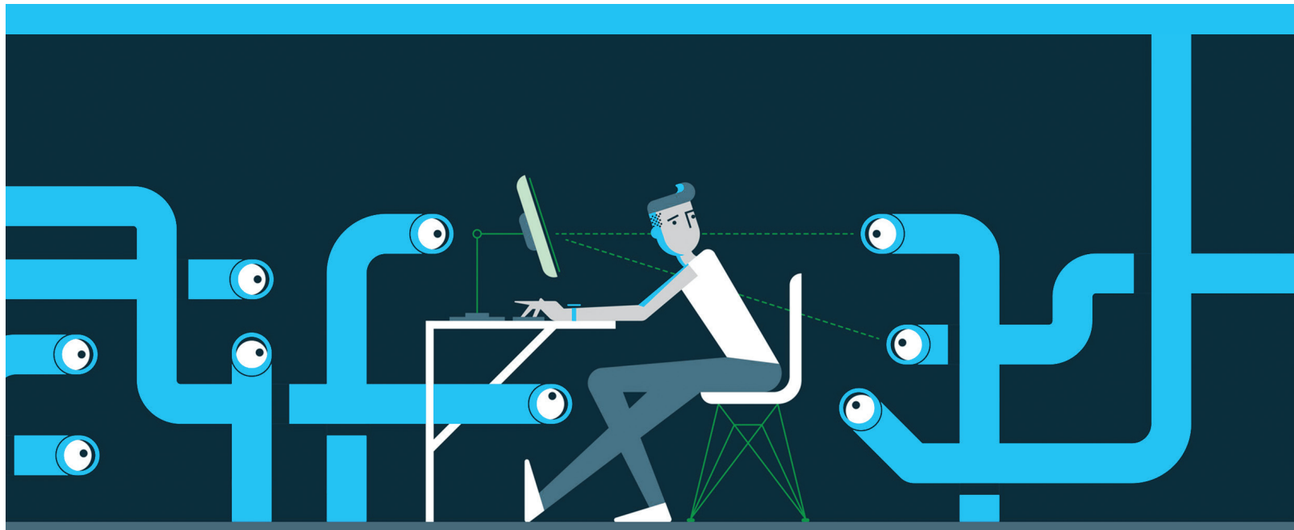
▪ خطر اختراق وتخريب البني التحتية للاتصالات وتكنولوجيا المعلومات

ظهرت انماطا جديدة خطيرة للغاية من الهجمات السيبرانية تستهدف إعاقة الخدمات الحيوية، وكذلك نشر برمجيات خبيثة وفيروسات لتخريب أو تعطيل البني التحتية للاتصالات وتكنولوجيا المعلومات ونظم التحكم الصناعية الحيوية وخاصة في المرافق الهامة (منشآت الطاقة النووية والبترول والغاز الطبيعي والكهرباء والطيران والنقل بأنواعه وقواعد البيانات والمعلومات القومية والخدمات الحكومية والرعاية الصحية والاسعاف العاجل وغيرها)، وذلك عبر عدة قنوات تشمل الشبكات اللاسلكية والذاكرة النقالة بالإضافة الي القنوات الأخرى الشائعة (البريد الالكتروني ومواقع الانترنت والشبكات الاجتماعية وشبكات الاتصالات السلكية)، مما يؤثر تأثيرا ملموسا علي البني التحتية لتلك المنشآت والمرافق وعلي الخدمات والاعمال المرتبطة بها، وقد ثبت عمليا أنها ليست بمنأى عن التعرض للهجمات السيبرانية الشرسة حتي لو كانت غير متصلة بالإنترنت.



▪ خطـر الارهـاب والحـرب السيبـرانية

انتشرت مؤخرا نوعية خطيرة من الهجمات والجرائم السيبرانية تعتمد علي تقنيات متقدمة (كالحوسبة السحابية والذكاء الاصطناعي وانترنت الاشياء)، وأجهزة تنصت علي شبكات الاتصال (السلكية واللاسلكية)، و برمجيات لفك شفرة ولاختراق لأنظمة الشبكات والحاسبات وقواعد البيانات، وبرمجيات لتشفير العمليات المشبوهة، وبرمجيات خبيثة لاختراق أنظمة أمن الشبكات والحاسبات لتسخيرها في القيام بعمليات اجرامية وتعاملات مشبوهة دون علم أصحابها فيما يسمي بالشبكات الآلية، حيث يمكن أن تضم شبكة آلية واحدة عشرات أو مئات الألاف أو ملايين من الحواسب أو الأجهزة المتصلة بالإنترنت (انترنت الأشياء) التي يمكن استخدامها لشن هجمات متنوعة، مثل الهجمات الموزعة لإعاقة الخدمات علي شبكات ومواقع مستهدفة لأغراض اجرامية كالتخريب والإرهاب والتهديد والترهيب والابتزاز. وفي حين أنه من المرجح أن تطوير الفيروسات المعقدة والشرسة يتم علي مستوي متقدم ويستلزم منظومة خبرات مركبة لا تتوافر الا في الدول المتقدمة تقنيا، وذلك لأغراض استراتيجية وحربية يمكن لتلك الدول استخدامها بدلا من (أو الي جانب) الهجمة العسكرية التقليدية فيما يسمي بالحروب السيبرانية ، الا أنه قد بدأ بالفعل نقل هذه الانماط واستنساخها من قبل التنظيمات الارهابية والتشكيلات العصابية الدولية للاستخدام في العمليات الارهابية وفي الجرائم المنظمة وفي تهديد وتعطيل البني التحتية للاتصالات والمعلومات، وبالتالي يتوقع العديد من الخبراء في مجال الأمن السيبراني تنامي انتشار الهجمات السيبرانية الشرسة في الفترة القادمة.



خطـــر ســـرقـة الهـــوية الـــرقمية والبيـــانـــات الخـــاصة

تعد سرقة الهوية الرقمية من أخطر الجرائم التي تهدد مستخدمي الانترنت ومستقبل الخدمات الالكترونية، حيث قد تتعرض البيانات الشخصية للمستخدم الي السرقة بهدف انتحال شخصيته والاستيلاء علي ممتلكاته وامواله أو للزج باسمه في تعاملات مشبوهة أو غير قانونية. وعادة ما يستعين سارق الهوية بمعلومات موجودة بالفعل علي الانترنت، وبخاصة علي مواقع شبكات التواصل الاجتماعية والمهنية المفتوحة أو قواعد البيانات والمعلومات القومية والشبكات الخاصة بالخدمات الحكومية وخدمات الضمان الاجتماعي وشبكات الرعاية الصحية ومواقع التجارة الالكترونية والاسواق الافتراضية وشبكات المدفوعات الالكترونية والصرافات الآلية وبورصة الاوراق المالية، فضلا علي أنه قد تتعرض الادوات والانظمة المستخدمة في اجراء المعاملات الالكترونية للسرقة أو التخريب مما يشكل خطرا كبيرا علي مصالح المستخدمين ومستقبل الخدمات الالكترونية وقد تؤثر الهجمات الموسعة علي القطاع المالي الوطني بوجه عام. كما قد تتعرض البيانات الخاصة بالمؤسسات العامة والشركات للسرقة مما يكبدها خسائر فادحة مادية وادبية، فضلا عن الاضرار بسمعتها وخسارتها لعملائها وأصولها الأدبية، مما قد يضر بالاقتصاد الوطني بوجه عام.

أهـــم القـــطـــاعـــات الحيـــوية المستـهـدفـة

- **قطاع الاتصالات وتكنولوجيا المعلومات**

بما يشمل شبكات الاتصالات السلكية واللاسلكية، والكوابل البحرية والارضية، وابراج الاتصالات، والاقمار الصناعية للاتصالات، ومراكز التحكم في الاتصالات، وشركات تقديم خدمات الاتصالات والانترنت.

- **قطاع الخدمات المالية**

ويضم شبكات ومواقع البنوك، وشبكات ومواقع تقديم المعاملات المصرفية، وشبكات الدفع الالكتروني، وشبكات ومواقع البورصة، وشركات تداول الأوراق المالية، وشبكات الخدمات المالية البريدية.

- **قطاع الطاقة**

ويضم نظم وشبكات ومحطات التحكم في انتاج وتوزيع الكهرباء والبترول والغاز، ومحطات السد العالي، ومحطات الطاقة النووية، وغيرها.

- **قطاع الخدمات الحكومية**

ويشمل بوابة ومواقع الحكومة الالكترونية، ومواقع الجهات والمؤسسات الحكومية، وقواعد البيانات والمعلومات القومية وأهمها قاعدة بيانات الرقم القومي والشبكات والمواقع المتصلة بها.

- **قطاع النقل والمواصلات**

ويشمل النقل البري والبحري والجوي والنيلي، ويضم كافة نظم ومراكز وشبكات التحكم في القطارات والمترو، وشبكات المرور، ونظم التحكم في الملاحة الجوية والبحرية.

- **قطاع الصحة وخدمات الإسعاف العاجل**

ويضم شبكات الإغاثة والاسعاف، وبنوك الدم، ونظم وشبكات المستشفيات، وشبكات ومواقع تقديم الرعاية الصحية.

- **قطاع الاعلام والثقافة**

ويشمل شبكات ونظم ومواقع الخدمات الإعلامية والبث.

- **وذلك بالإضافة الي المواقع الرسمية للدولة والقطاعات ذات التأثير علي النشاط الاقتصادي مثل الاستثمار والسياحة والتجارة والصناعة والزراعة والري والتعليم بمختلف مستوياته.**

العنـــاصر الـرئيسية لخطـــورة التـهـديـــدات السيبـــرانية

ترجع خطورة التهديدات السيبرانية الي ثلاث عناصر رئيسية هي:

- **استنادها الي تقنيات متقدمة ومتطورة**

غالبا ما تكون تلك التقنيات حكرا علي دولا معدودة وشركات كبري، كما أن كثير من تلك التقنيات سرية وغير متاحة للتصدير، وقد تحتوي النسخ المتاحة منها للتصدير علي أبواب خلفية أو ثغرات تجعلها مصدرا لتهديدات اضافية.

- **سرعة وسهولة انتشارها**

حيث أن نشر الفيروسات الخبيثة أو شن هجمات اعاقة الخدمات وغيرها من الأخطار السيبرانية يمكن أن يحدث بسرعة فائقة وسهولة في ظل انتشار واتساع نطاق استخدام شبكات الاتصالات وتكنولوجيا المعلومات، ونظرا لسهولة شن الهجمات وبث الفيروسات عبر الحدود من أي مكان وبأرخص التكاليف، كما يصعب وقد يستحيل تعقب مصدر تلك التهديدات والأخطار في الوقت المناسب لتداركها والتغلب عليها.

- **اتساع نطاق تأثيرها**

سواء من حيث التأثير المباشر أو غير المباشر علي البني التحتية وما قد يتبعه من اضرار أو خسائر فادحة، وكذلك من حيث امكانية الاضرار بمصالح الجهات العامة والخاصة والتأثير علي جموع كبيرة من المواطنين (آلاف أو ملايين) بصورة مفاجئة وفي وقت قصير وعن بعد.

ان الهجمات والجرائم السيبرانية بطبيعتها تتعدي الحدود الجغرافية للدول، وعادة ما تعتمد علي شبكات الجريمة المنظمة بشقيها التقليدي والتقني. ولذا يجب أن تشمل مواجهة تلك الهجمات والجرائم الآليات التقليدية للتعاون الدولي لمكافحة الجرائم، بالإضافة الي أطر تشريعية وتنظيمية وآليات خاصة للتعامل مع المستحدثات التقنية المرتبطة بها. فالمواجهة الفاعلة للهجمات والجرائم السيبرانية تستلزم التعاون والتنسيق على المستوي الوطني بين شركاء اتاحة وتشغيل البني التحتية في القطاعات الحيوية وشركاء تقديم الخدمات من الجهات الحكومية والمؤسسات والشركات، بالإضافة الي التعاون والتنسيق على المستويين الدولي والإقليمي مع المنظمات الدولية والتجمعات الإقليمية والمنتديات العالمية المهنية والتخصصية.

الـهـدف الاستراتيجي

"مواجهة المخاطر السيبرانية وتعزيز الثقة في البني التحتية للاتصالات والمعلومات وتطبيقاتها وخدماتها في شتي القطاعات الحيوية وتأمينها من أجل تحقيق بيئة رقمية آمنة وموثوقة للمجتمع المصري بمختلف أطيافه".

ركـــائز التـــوجه الاستـــراتيجي لـمـواجهة الاخـــطـار السيبـرانية

يمكن تحديد أهم ركائز الاستعداد لمواجهة الأخطار السيبرانية فيما يلي:

- الدعم السياسي والمؤسسي الاستراتيجي والتنفيذي: ويشمل ذلك الوعي بخطورة التهديدات السيبرانية وضرورة التعامل معها كأولوية وبأعلى قدر من الجدية، مع الاهتمام بالاستعداد المسبق بما يشمل الخطط الاستراتيجية والتنفيذية وخطط الطوارئ وآليات التنسيق العرضي واعداد الكوادر والتجهيزات التقنية واللوجستية.

- الاطار التشريعي: وضع الاطار التشريعي الملائم لأمن الفضاء السيبراني ومكافحة الجرائم السيبرانية وحماية الخصوصية وحماية الهوية الرقمية وأمن المعلومات، وذلك بمشاركة من الاطراف المعنيين، وذوي الخبرة في القطاع الخاص ومؤسسات المجتمع المدني، مع الاسترشاد بالخبرات والتجارب والبرامج الدولية ذات الصلة، مع اعداد وتدريب المتخصصين في انفاذ القانون في الجهات القضائية والشرطية.

- الإطار التنظيمي والتنفيذي: وضع الإطار التنظيمي وانشاء منظومة وطنية لحماية أمن الفضاء السيبراني وتأمين البني التحتية للاتصالات وتكنولوجيا المعلومات ونظم وقواعد البيانات والمعلومات القومية وبوابات الخدمات الحكومية والمواقع الحكومية على الانترنت، وذلك بإعداد وتفعيل ما يعرف بفرق الاستعداد والاستجابة لطوارئ الحاسبات والشبكات، في القطاعات الحيوية على المستوي الوطني، انطلاقا من التجربة الرائدة في قطاع الاتصالات وتكنولوجيا المعلومات. تكون هذه الفرق مسئولة عن أعمال المتابعة الامنية لشبكات الاتصالات والمعلومات الوطنية والحواسب المتصلة بها، وعن التعامل مع أية أخطار سيبرانية تهددها أو هجمات سيبرانية توجه اليها، وعن التوعية والاعداد لمواجهتها.

- البحث العلمي والتطوير و تنمية صناعة الأمن السيبراني: تشجيع ودعم وتنمية البحث العلمي والتطوير ودعم التعاون بين الجهات البحثية والشركات الوطنية، خاصة في مجال تحليل البرمجيات الخبيثة المتقدمة، ومجال تحليل الأدلة الرقمية، وفي مجال حماية وتأمين نظم التحكم الصناعية، ومجال تطوير أجهزة وأنظمة تأمين النظم والشبكات، ومجال التشفير والتوقيع الالكتروني، ومجال حماية البني التحتية للاتصالات وتكنولوجيا المعلومات، ومجال تأمين الحواسب السحابية وحماية قواعد البيانات الكبرى ومجال تقنيات الذكاء الاصطناعي وانترنت الأشياء.

- تنمية الكوادر البشرية والخبرات اللازمة لتفعيل منظومة الأمن السيبراني في مختلف القطاعات، بالتعاون والشراكة مع القطاع الخاص والجامعات ومؤسسات المجتمع المدني.

- التعاون مع الدول الصديقة والمنظمات الدولية والاقليمية ذات الصلة: ويشمل تبادل الخبرات وتنسيق المواقف في مجال أمن الفضاء السيبراني ومكافحة الجرائم السيبرانية، حيث أن تلك الجرائم لا تعترف بالحدود الجغرافية أو السياسية.

- التوعية المجتمعية: وضع وتنفيذ خطط وحملات للتوعية المجتمعية بالفرص والمزايا التي تقدمها الخدمات الالكترونية المؤمنة للأفراد والمؤسسات، وبأهمية الأمن السيبراني لحماية تلك الخدمات من المخاطر والتحديات التي قد تواجهها، فضلا عن حماية الخصوصية وإطلاق برامج حماية الاطفال والنشء على الانترنت.

آليـــة التنـفيذ

المجلس الأعلى لتأمين البني التحتية للاتصالات وتكنولوجيا المعلومات (المجلس الأعلى للأمن السيبراني):

تبنت وزارة الاتصالات وتكنولوجيا المعلومات الدعوة لتشكيل مجلس أعلي لحماية البني التحتية للاتصالات وتكنولوجيا المعلومات (المجلس الأعلى للأمن السيبراني) يتبع مجلس الوزراء يرأسه وزير الاتصالات وتكنولوجيا المعلومات، وتمثل فيه الأطراف المعنيين بالأمن القومي وبإدارة وتشغيل البني التحتية في القطاعات الحيوية والمرافق العامة، وذوي الخبرة في القطاع الخاص والجهات البحثية والتعليمية. حيث يتولى المجلس وضع استراتيجية وطنية للأمن السيبراني ولمواجهة الهجمات السيبرانية، كما يتولى الاشراف على تنفيذ تلك الاستراتيجية، مع ضرورة تحديثها تمشيا مع التطورات التقنية المتلاحقة. وقد بدأ المجلس عمله التمهيدي في يناير ٢٠١٥، وقام رئيس مجلس الوزراء باعتماد تشكيل المكتب التنفيذي للمجلس ولجنته الفنية وتوصيف مهامه في يونيو ٢٠١٦.

أهــم البــرامج الاستـراتيجية في المـرحلة الحـــالية (٢٠١٧-٢٠٢١)

١ برنامج لتطوير الاطار التشريعي الملائم لأمن الفضاء السيبراني ومكافحة الجرائم السيبرانية وحماية الخصوصية وحماية الهوية الرقمية

٣ برنامج لحماية الهوية الرقمية (برنامج المواطنة الرقمية)، وتفعيل البني التحتية اللازمة لدعم الثقة في التعاملات الالكترونية بوجه عام وفي الخدمات الحكومية الالكترونية بوجه خاص

٥ برنامج لدعم البحث العلمي والتطوير وتنمية صناعة الأمن السيبراني

٢ برنامج تطوير منظومة وطنية متكاملة لحماية أمن الفضاء السيبراني وتأمين البني التحتية للاتصالات وتكنولوجيا المعلومات

٤ برنامج لإعداد الكوادر البشرية والخبرات اللازمة لتفعيل منظومة الأمن السيبراني في مختلف القطاعات

٦ برنامج للتوعية المجتمعية بالفرص والمزايا التي تقدمها الخدمات الالكترونية للأفراد والمؤسسات والجهات الحكومية، وبأهمية الأمن السيبراني لحماية تلك الخدمات من المخاطر والتحديات التي قد تواجهها

١- برنامج لتطوير الاطار التشريعي الملائم لأمن الفضاء السيبراني ومكافحة الجرائم السيبرانية وحماية الخصوصية وحماية الهوية الرقمية

وذلك بمشاركة من الاطراف المعنيين، وذوي الخبرة في القطاع الحكومي والخاص والاكاديمي ومؤسسات المجتمع المدني، مع الاسترشاد بالخبرات والتجارب والبرامج الدولية ذات الصلة، والاتفاقية الافريقية لأمن الفضاء السيبراني التي أقرها مؤخرا مجلس الاتحاد الافريقي، حيث أن وجود أي فراغ تشريعي بشأن الجرائم السيبرانية، قد يضر ضرراً بالغاً بمنظومة المعاملات الإلكترونية والخدمات الالكترونية. فمما لا شك فيه أن « مبدأ شرعية الجرائم والعقوبات « والذى يشكل أحد أهم المبادئ الراسخة والذى يقضى بأنه لا جريمة ولا عقوبة إلا بنص « يستوجب عدم إمكانية التوسع فى تطبيق النصوص العقابية وتجريم أفعال لم تتناولها التشريعات القائمة أو تتعرض لها بعقوبة مناسبة، ومن ثم يجب علي الدول ملاحقة هذا التطور بصياغة قواعد تشريعية جديدة وملائمة لمواجهة تلك الجرائم المعاصرة التى تهدد اعتبارات الثقة والأمان فى المعاملات الإلكترونية التى تكتسب أهمية كبرى يوماً بعد يوم.

٢- برنامج تطوير منظومة وطنية متكاملة لحماية أمن الفضاء السيبراني وتأمين البني التحتية للاتصالات وتكنولوجيا المعلومات

وذلك بإعداد وتفعيل ما يعرف بفرق الاستجابة لطوارئ الحواسبComputer Emergency Response (or Readiness) Teams (CERTs) أو فرق مواجهة حوادث أمن الحواسبComputer Security Incidents Response Teams (CSIRTs)، في القطاعات الحيوية علي المستوي الوطني، انطلاقا من التجربة الرائدة في قطاع الاتصالات وتكنولوجيا المعلومات. تكون هذه الفرق مسئولة عن أعمال المتابعة الامنية لشبكات الاتصالات والمعلومات الوطنية والحواسب المتصلة بها، وعن التعامل مع أية أخطار سيبرانية تهددها أو هجمات سيبرانية توجه اليها، وعن التوعية والاعداد لمواجهتها.

٣- برنامج لحماية الهوية الرقمية (برنامج المواطنة الرقمية)، وتفعيل البني التحتية اللازمة لدعم الثقة في التعاملات الالكترونية بوجه عام وفي الخدمات الحكومية الالكترونية بوجه خاص

مثل بنية المفتاح المعلن(Public Key Infrastructure (PKI ، التي يعتمد عليها التوقيع الالكتروني وتنظمها وتشرف عليها هيئة تنمية صناعة تكنولوجيا المعلومات، وتشمل مركز السلطة الجذرية للتصديق الالكتروني بالهيئة، والسلطة الحكومية للتصديق الالكتروني بوزارة المالية، وشركات مرخص لها من الهيئة لتقديم خدمات التوقيع الالكتروني. يعتمد البرنامج على تشكيل لجنة عليا للمواطنة الرقمية تقوم بإعداد رؤية استراتيجية (على المستوي القومي) للمواطنة الرقمية وخطة عمل لتحويل مفهوم المواطنة الرقمية الي واقع ملموس واطلاق مشروعات قومية تستهدف تطبيقات موسعة تسهم في تيسير وتأمين التعاملات الالكترونية، اعتمادا علي البنية التحتية التي تم انشاءها.

٤- برنامج لإعداد الكوادر البشرية والخبرات اللازمة لتفعيل منظومة الأمن السيبراني في مختلف القطاعات

بالتعاون والشراكة بين الجهات الحكومية والقطاع الخاص والجامعات ومؤسسات المجتمع المدني، اعتمادا على التجربة الرائدة التي قام بها الجهاز القومي لتنظيم الاتصالات.

٥- برنامج لدعم البحث العلمي والتطوير وتنمية صناعة الأمن السيبراني

من خلال دعم برامج ومشروعات التعاون بين الجهات البحثية والشركات الوطنية؛ وخاصة في مجال تحليل البرمجيات الخبيثة المتقدمة ومجال تحليل الأدلة الرقمية، وفي مجال حماية وتأمين نظم التحكم الصناعية، ومجال تطوير أجهزة وأنظمة تأمين النظم والشبكات، ومجال التشفير والتوقيع الالكتروني، ومجال حماية البني التحتية للاتصالات وتكنولوجيا المعلومات، ومجال تأمين الحواسب السحابية وحماية قواعد البيانات الكبرى ومجال تقنيات الذكاء الاصطناعي وانترنت الأشياء. كما يلزم كأولوية قصوى انشاء مراكز أو معامل وطنية لاعتماد الانظمة والاجهزة والبرمجيات والتطبيقات المستخدمة في الجهات الحيوية وفي البني التحتية الهامة.

٦- برنامج للتوعية المجتمعية بالفرص والمزايا التي تقدمها الخدمات الالكترونية للأفراد والمؤسسات والجهات الحكومية، وبأهمية الأمن السيبراني لحماية تلك الخدمات من المخاطر والتحديات التي قد تواجهها

على أن تشمل احتفاليات وحملات سنوية موسعة على مستوي الجمهورية والمؤتمرات والندوات وورش العمل النوعية في مختلف القطاعات، وأن تخاطب مختلف المستويات، بدءا من المستوي القيادي وحتي الأطفال وطلاب المدارس والجامعات والمواطن البسيط. ويلزم اصدار ونشر تقارير دورية للتوعية بأهم الاخطار السيبرانية وآليات مواجهتها وبالجهود التي تبذل والأنشطة ذات الصلة بمجال الامن السيبراني.

ان مواجهة الأخطار والجرائم السيبرانية تحتاج ايمانا صادقا وجهدا دؤوبا وشراكة مجتمعية موسعة تشمل الجهات الحكومية والقطاع الخاص والمؤسسات البحثية والتعليمية ومنظمات الاعمال والمجتمع المدني لتعظيم الاستفادة من الفرص المتميزة التي تتيحها تقنيات الاتصالات والمعلومات الحديثة في شتي مجالات التنمية الاقتصادية والاجتماعية والثقافية، مع حماية مجتمعنا من مخاطر وأضرار الجرائم والهجمات السيبرانية.