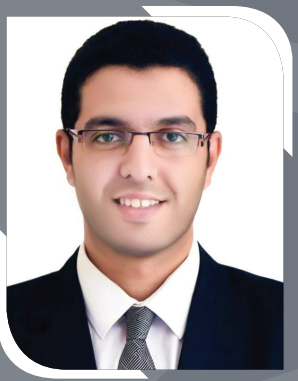
دور الاتفاقيات الدولية والإقليمية فى مجال الأمن السيبرانى وموقف الدولة المصرية منها

■ القاضى.د/ محمد أحمد لبيب أحمد
نائب رئيس محكمة الاستئناف

■ القاضى/ هيثم محمد بهاء القاضى
رئيس محكمة الاستئناف



■ مستشار/مصطفى أحمد كمال
وكيل مجلس الدولة

■ ملخص البحث:

أصبح الأمن السيبرانى من المجالات التى لا غنى عنها فى عالمنا، وهذا بسبب الحاجة إليه للتصدى للهجمات والجرائم الإلكترونية، لذا كان من المتعين على المجتمع الدولى أن يتصدى لهذا الغزو الإجرامى التقنى بسن المزيد من التشريعات والقوانين العقابية والإجرائية التى تتناسب وخطورة هذه الجرائم ووضع المزيد من الضوابط اللازمة لمواجهتها.

من أجل ذلك اتخذت المنظمات الدولية مبادرات عدة فى مجال مكافحة الجريمة السيبرانية من قبل العديد من المنظمات كالاتحاد الدولى للاتصالات والمعهد الوطنى للمعايير والتكنولوجيا والوكالة الأوروبية للأمن السيبرانى.

كما اهتم المجتمع الدولى الأوروبى والأجنبى بتنظيم مجال تقنية المعلومات وبذل العديد من الجهود التشريعية من أجل التصدى لظاهرة الإجرام المعلوماتى، وكان من بين أهم هذه الجهود ما صدر عن الاتحاد الأوروبى من اتفاقية بودابست لمكافحة جرائم المعلوماتية والتى عنيت بشكل أساسى بمواءمة عناصر القانون الموضوعى الجنائى المحلى والأحكام المتصلة بالجرائم فى مجال الجريمة الإلكترونية وإلى إنشاء نظام سريع وفعال للتعاون الدولى الاتفاقية.

كما أصدرت جامعة الدول العربية الاتفاقية العربية لمكافحة جرائم تقنية المعلومات والتى تهدف إلى تعزيز التعاون بين الدول العربية فى مجال مكافحة جرائم تقنية المعلومات لدرء أخطار هذه الجرائم حفاظا على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها.

كما شهدت مصر حراكًا قويًا فى مجال أمن المعلومات والشبكات حيث سعت نحو بناء وتأسيس منظومة حديثة قادرة على حماية الفضاء السيبرانى المصرى ، حيث تم إنشاء المجلس الأعلى للأمن السيبرانى برئاسة وزير الاتصالات وتكنولوجيا المعلومات، ويضم المجلس ممثلين من الحكومة والقطاع الخاص والمجتمع المدنى، كما قامت بإنشاء المركز المصرى للاستجابة لطوارئ الحاسب الآلى «سيرت» والتابع للجهاز القومى لتنظيم الاتصالات، وأنشأت مركز الاستجابة لطوارئ الحاسب الآلى للقطاع المالى والتابع للبنك المركزى ثم أصدرت الاستراتيجية الوطنية للأمن السيبرانى لجمهورية مصر العربية. ٢٠١٧-٢٠٢١، وأعقبها صدور الاستراتيجية الوطنية للأمن السيبرانى لجمهورية مصر العربية ٢٠٢٣-٢٠٢٧.

■ Abstract:

Cybersecurity has become an indispensable field in our world due to the need to combat cyber-attacks and electronic crimes. Therefore, it is imperative for the international community to address this technological criminal invasion by enacting more legislative and punitive measures and procedural laws that match the severity of these crimes and by establishing necessary regulations to confront them.

For this purpose, various international organizations have taken several initiatives in the field of combating cybercrime, including the International Telecommunication Union, the National Institute of Standards and Technology, and the European Union Agency for Cybersecurity.

The European and international communities have also focused on regulating the field of information technology, making significant legislative efforts to combat the phenomenon of cybercrime. Among the most important of these efforts is the Budapest Convention on Cybercrime issued by the European Union, which aims primarily to harmonize the elements of substantive criminal law and provisions related to cybercrimes and to establish a rapid and effective system for international cooperation under the convention.

Additionally, the League of Arab States issued the Arab Convention on Combating Information Technology Crimes, aiming to enhance cooperation among Arab countries in the field of combating IT crimes.

Egypt has also witnessed strong momentum in the field of information and network security. The Supreme Council for Cybersecurity was established, chaired by the Minister of Communications and Information Technology, and includes representatives from the government, private sector, and civil society. Egypt also established the Egyptian Computer Emergency Readiness Team (EG-CERT), affiliated with the National Telecommunication Regulatory Authority, and created the Financial Sector Computer Emergency Readiness Team affiliated with the Central Bank. Furthermore, Egypt issued the National Cybersecurity Strategy for 2017-2021, followed by the National Cybersecurity Strategy for 2023-2027.

الكلمات المفتاحية:

الأمن السيبرانى، اتفاقيات تقنية المعلومات، الجريمة السيبرانية، اتفاقية بودابست، الجريمة/الجرائم المعلوماتية، سيرت، الهجمات السيبرانية

■ مُقدمة:

صاحب ظهور الحاسب الآلى والتوسع فى استخدام شبكة الإنترنت بعض الآثار السلبية والمخاطر المترتبة على هذا التوسع الكبير، وعلى ذلك فقد توجهت الأنظار إلى الاهتمام بالأمن السيبرانى، ومن ثم ظهرت الأهمية القصوى لتعاون الفاعلين فى المجتمع الدولى نحو وضع أطر تنظيمية ومؤسسية لتنسيق مختلف الجهود الوطنية التى تبذلها الدول نحو حماية الفضاء السيبرانى والتصدى للأخطار السيبرانية المتزايدة.

وكان على رأس هذه المنظمات منظمة الأمم المتحدة، كما اتخذت العديد من المنظمات الدولية مبادرات عدة فى مجال مكافحة الجريمة السيبرانية، من قبل ذلك على سبيل المثال الجهود التى بذلها الاتحاد الدولى للاتصالات، ومنظمة الشرطة الجنائية الدولية (الإنتربول).

بالإضافة إلى الجهود الدولية التى تقوم بها المنظمات الدولية المذكورة أعلاه، فإن هناك جهوداً دولية أخرى تقوم بها منظمات دولية ذات طابع إقليمى، وهو ما ظهر جليًا حين اجتمع المجلس الأوروبى عام ٢٠٠١ فى العاصمة المجرية بودابست، حيث أُبرمت الاتفاقية الأوروبية الدولية لمكافحة الإجرام السيبرانى (الإجرام عبر الإنترنت)، وقد صارت تلك الاتفاقية هى الأساس القانونى العالمى لمكافحة الإجرام السيبرانى.

كما كان لجامعة الدول العربية جهودٌ فى هذا الصدد حيث أصدرت الجامعة الاتفاقية العربية لمكافحة جرائم تقنية المعلومات عام ٢٠١٠م.

كما شهدت مصر حراكًا قويًا فى مجال أمن المعلومات والشبكات، حيث سعت مصر نحو تأسيس وبناء منظومة قادرة على حماية الفضاء السيبرانى المصرى، فقد تم إنشاء المجلس الأعلى للأمن السيبرانى، كما قامت بإنشاء المركز المصرى للاستجابة لطوارئ الحاسب الآلي «سيرت»، كما تم إنشاء مركز الاستجابة لطوارئ الحاسب الآلى للقطاع المالى والتابع للبنك المركزى ثم أصدرت الاستراتيجية الوطنية للأمن السيبرانى ٢٠١٧-٢٠٢١، وأعقبها صدور الاستراتيجية الوطنية للأمن السيبرانى٢٠٢٣-٢٠٢٧.

■ أولاً: أهمية البحث:

لقد أحدثت تكنولوجيا المعلومات والاتصالات ثورة شاملة فى جميع نواحى الحياة، وزادت هيمنة تكنولوجيا المعلومات والاتصالات على نسق الحياة العام، وصاحب ظهور الحاسب الآلى والتوسع فى استخدام شبكة الإنترنت فى مجالات الحياة المختلفة ظهور بعض الآثار السلبية والمخاطر المترتبة على هذا التوسع الكبير، إذ كلما زاد الاعتماد على هذه التقنيات فى التنمية تزداد المخاطر الخاصة بحماية المعلومات، ومع تزايد الاعتماد العالمى على تكنولوجيا المعلومات والاتصالات تزايد أيضًا التعرض للجرائم السيبرانية، إذ أصبح الفضاء السيبرانى عرضة للانتهاكات من قبل مخترقى الشبكات سواء أكانوا دولاً أو غيرها ممن يملكون هذه التقنيات المعلوماتية.

وعلى ذلك فقد توجهت الأنظار إلى الاهتمام وبشدة إلى الأمن السيبرانى، وأصبح الحفاظ عليه

حفاظًا على الأمن القومى للدول، لذا أصبح أمن الفضاء السيبرانى يدخل ضمن أولويات العديد من الدول، ودفعت التهديدات المتزايدة لأمن الفضاء السيبرانى العديد من الدول للعمل على بذل جهود مضنية لاستحداث قوانين لمكافحة الجريمة السيبرانية، ولذلك بات من الضرورى توحيد الجهود الدولية لوضع الأطر القانونية والتنظيمية والإجرائية لمواجهة المخاطر السيبرانية، وآثارها على المستوى الدولى لمواجهة تهديدات أمن الفضاء السيبرانى، وتعزيز أشكال التعاون الدولى فى سبيل مكافحتها (عبد الحليم، ص ٢٠).

وبناءً على ذلك تتجلى أهمية البحث فى حداثة تهديدات الأمن السيبرانى وغموضها بالنسبة لقطاع عريض من الأفراد، وفى التأثير الذى تحدثه هجمات الأمن السيبرانى على الأفراد والمؤسسات بل والمجتمعات بأسرها، وأخيرًا فى الأهمية العالمية لحماية الأمن السيبرانى والتصدى للهجمات السيبرانية المتزايدة، ومن ثَم فتبرز الحاجة لإثراء المكتبة العربية بمجهود بحثى يساهم فى سد الفجوة المعرفية وتقييم الجهود الحالية المبذولة فى مصر فى هذا المجال سعيًا للمشاركة فى تقديم مقترحات تطويرها، بما من شأنه تحقيق المصلحة القومية للدولة.

■ ثانيًا: أهداف البحث (أسباب اختيار الموضوع البحثى):

لا جدال فى أن تباين الأطر التشريعية الوطنية من قوانين ولوائح وتنظيمات التى تسنها مختلف الدول لمواجهة الجرائم السيبرانية تعد واحدة من الصعوبات التى تواجه المجتمع الدولى فى تنسيق الجهود للحد من هذه الجريمة، لأن مجرمى الأمن المعلوماتى يستغلون هذا الاختلاف، حيث ترتكب جرائمها عبر حدود الدول التى يكون فيها خطر تطبيق القوانين على المجرمين فيها أقل من غيرها من الدول الأخرى.

فالسيادة الوطنية للدول أمر لا يمكن تجاهله، إلا أن المخاطر والتحديات التى يواجهها المجتمع الدولى اقتضت ضرورة تنسيق الجهود بين الدول لتحقيق المصلحة العليا للمواطن، ولذا كان ينبغى إبرام اتفاقيات دولية لمواجهة هذه الجرائم لتضع الخطوط العريضة التى تتبعها مختلف الدول عند وضع الإطار التشريعى والتنظيمى للتصدى لجرائم الأمن السيبرانى.

■ ثالثًا: منهج البحث:

تتطلب دراسة هذا الموضوع تنوع مناهج البحث، وعدم اقتصارها على منهج واحد، وذلك لخدمة أهداف البحث، لذا سوف نتبع فى دراستنا مناهج البحث التالية:

الأسلوب النظرى فى بحث الأمن السيبرانى والذى يرتكز على دراسة وتحليل النظريات والمفاهيم المتعلقة بالأمن السيبرانى وتطبيقها فى السياقات العملية، وفهم الأسس النظرية للتهديدات السيبرانية والمعالجات الأمنية، وذلك من خلال دراسة الأبحاث والمصادر المنشورة حول الأمن السيبرانى من خلال البحث فى المقالات العلمية والكتب والتقارير، وصولاً لتحليل وتفسير السلوك السيبرانى، وهو ما من شأنه أن يساهم فى فهم الظواهر والعمليات المعقدة وتطوير النظريات

والأطر الفكرية التى تساهم فى تحسين استراتيجيات الأمن السيبرانى.

كما تتطلع هذه الدراسة إلى إجراء تحليل متعمق للتشريعات الدولية المتعلقة بالأمن السيبرانى وتوثيق النتائج، معتمدة فى ذلك على المناهج الآتية:

أولاً: المنهج الاستقرائى: والذى يعتمد على استقراء آراء الفقه وأحكام القضاء، حول الموضوعات التى يناقشها البحث، للوقوف على نقاط الخلاف، وبيان الراجح منها.

ثانيًا: المنهج التحليلى: وذلك بهدف تحليل النصوص القائمة، للوقوف على مدى ملاءمتها للموضوعات التى يناقشها البحث.

ثالثًا: المنهج المقارن: وذلك بمقارنة الوضع القانونى فى الاتفاقات الدولية المختلفة.

■ رابعًا: خطة البحث:

لإعطاء فكرة متكاملة وإرساء بنيان متكامل لموضوع بحثنا. فقد خصصنا مبحثاً تمهيدياً تناولنا فيه ماهية الأمن السيبرانى، وتم تقسيمه على النحو التالى:

المطلب الأول: التعريف بالأمن السيبرانى والمصطلحات المستخدمة فى هذا المجال.

المطلب الثانى: لمحة تاريخية عن الأمن السيبرانى.

المطلب الثالث: أهمية الأمن السيبرانى.

المطلب الرابع: أهداف الأمن السيبرانى.

ثم تناولنا فى المبحث الأول الاتفاقيات الدولية والإقليمية فى مجال الأمن السيبرانى، على التفصيل الآتي:

المطلب الأول: جهود منظمة الأمم المتحدة فى مجال مكافحة الجريمة المعلوماتية

المطلب الثانى: جهود المنظمات الدولية فى مجال مكافحة الجريمة السيبرانية

الفرع الأول: دور الاتحاد الدولى للاتصالات (ITU) فى مجال الأمن السيبرانى.

الفرع الثانى: دور المعهد الوطنى للمعايير والتكنولوجيا (NIST) فى مجال الأمن السيبرانى.

الفرع الثالث: دور الوكالة الأوروبية للأمن السيبرانى (ENISA) فى مجال الأمن السيبرانى.

المطلب الثالث: دور الاتفاقيات الإقليمية فى مجال مكافحة الجريمة المعلوماتية.

الفرع الأول: اتفاقية بودابست لمكافحة الجريمة السيبرانية.

الفرع الثانى: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

وتناولنا فى المبحث الثانى الجهود المصرية فى مجال الأمن السيبرانى وقد قسمناه إلى ستة مطالب، على التفصيل الآتي:

المطلب الأول: المجلس الأعلى للأمن السيبرانى.

المطلب الثانى: المركز المصرى للاستجابة لطوارئ الحاسب الآلى (سيرت).

المطلب الثالث: مركز الاستجابة لطوارئ الحاسب الآلى للقطاع المالى والمصرفى.

المطلب الرابع: الاستراتيجية الوطنية للأمن السيبرانى لجمهورية مصر العربية ٢٠١٧-٢٠٢١.
المطلب الخامس: الاستراتيجية الوطنية للأمن السيبرانى لجمهورية مصر العربية ٢٠٢٣-٢٠٢٧.
المطلب السادس: نتائج الجهود المصرية فى مجال الأمن السيبرانى.

المبحث التمهيدى
ماهية الأمن السيبراني

من خلال هذا المبحث، نهدف إلى إلقاء الضوء على ماهية الأمن السيبرانى، فنوضح أولاً ما هو المقصود بالأمن السيبرانى من حيث التعريف به وإبراز أهم المصطلحات المستخدمة فى هذا المجال، ثم نستعرض بإيجاز لمحة تاريخية موجزة عن الأمن السيبرانى بالقدر الذى يخدم أهداف هذا المبحث، ثم نتطرق لبيان الأهمية المتزايدة للأمن السيبرانى، وأخيرًا نقف على أهم أهداف الأمن السيبرانى.

المطلب الأول: التعريف بالأمن السيبرانى والمصطلحات المستخدمة فى هذا المجال

معنى كلمة سيبرانى: يقصد بكلمة سيبرانى الشيء المرتبط بالحاسب الآلى أو شبكات الحاسب الآلى بمختلف أنواعها (مثل شبكة الإنترنت) أو بالاتصالات الإلكترونية على وجه العموم (Cambridge Dictionary)، وقد اصطلح على أن تُطلق كلمة سيبرانى على كل ما يتعلق بالشبكات الإلكترونية الحاسوبية، وشبكة الإنترنت، ومثلاً عندما نقول الفضاء السيبرانى، فهذا يعنى الفضاء الإلكترونى.

أما بخصوص مصطلح الأمن السيبرانى فلا يوجد تعريف جامع مانع متفق عليه بين مختلف الأدبيات ومختلف الممارسين حوله، ولكن يمكن تعريفه بشكل موجز بأنه عمل كل الوسائل اللازمة لحماية الفضاء السيبرانى من الهجمات السيبرانية، وذلك من خلال مجموعة من الوسائل المستخدمة تقنيًا وتنظيميًا وإداريًا فى منع الوصول غير المشروع للمعلومات الإلكترونية ومنع استغلالها بطريقة غير قانونية ونظامية (العنزى، ١٤٤٣هـ، ص ٢٢).

وقد تصدت العديد من الوثائق الصادرة من بعض المنظمات الدولية الحكومية مثل الاتحاد الدولى للاتصالات إلى وضع تعريفات للأمن السيبرانى، ومن ذلك فقط عرفت التوصية (ITU-T X.1205) الصادرة عن الاتحاد الدولى للاتصالات الأمن السيبرانى بأنه مجموعة الأدوات والسياسات والمفاهيم الأمنية والضمانات الأمنية والمبادئ التوجيهية ونَهَج إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات وسبل الضمان والتكنولوجيات التى يمكن استخدامها فى حماية البيئة السيبرانية والمنظمة وأصول المستعملين. وتشمل المنظمة وأصول المستعملين تجهيزات الحواسيب الموصولة، والموظفين، والبنية التحتية، والتطبيقات، والخدمات، وأنظمة الاتصالات، والحصيلة الكلية للمعلومات المرسلة أو المخزنة فى البيئة السيبرانية (Overview of cybersecurity).

ويمكن أن نستنتج من التعريف المذكور أعلاه ومن غالبية التعريفات الأخرى المتوفرة للظاهرة محل الدراسة «الأمن السيبراني» أن هناك ثلاثة عناصر أو جوانب أساسية للأمن السيبرانى، وهى كما يلى:

١- الوقاية: استخدام وتنفيذ السياسات والتدابير والممارسات المتاحة لعرقلة أى وصول أو انتهاكات محتملة غير مصرح بها.

٢- الكشف: تحديد التهديدات ونقاط الضعف المحتملة الموجودة داخل الأنظمة والأجهزة المحمية.

٣- الاستجابة: تحديد وتنفيذ أفضل الحلول اللازمة لإيقاف أو إصلاح أو تخفيف تأثير ونتائج الحوادث والانتهاكات الأمنية.

ويقصد بمصطلح الفضاء السيبرانى -كما عرّفه المعهد الوطنى للمعايير والتقنية بالولايات المتحدة الأمريكية- مجال عالمى داخل البيئة المعلوماتية يتكون من شبكة مستقلة من البنى التحتية لأنظمة المعلومات ويتضمن ذلك شبكات الإنترنت وشبكات الاتصالات وأنظمة الحاسب الآلى والمعالجات وأجهزة التحكم المدمجة (NIST).

وأخيرًا فيقصد بمصطلح الهجمات السيبرانية عملية هجوم إلكترونى على نظام أو مؤسسة أو فرد يهدف إلى تعطيل الأصول أو سرقتها أو إتلافها؛ حيث قد تكون تلك الأصول رقمية (مثل البيانات أو المعلومات أو حساب المستخدم)، أو خدمات رقمية (مثل الاتصالات) أو أصولاً مادية ذات مكون إلكترونى (مثل نظام التحكم فى العمليات الموجود فى مبنى أو طائرة أو منشأة للتكرير النووى). عادةً ما تسعى مثل هذه الهجمات إلى تعريض سرية الأصول الرقمية أو سلامتها أو إمكانية توافرها للخطر (James, 2016, p34) .

المطلب الثانى: لمحة تاريخية عن الأمن السيبرانى

يعود تاريخ نشأة الأمن السيبرانى إلى سبعينيات القرن العشرين، وهو الوقت الذى لم تكن فيه بعض المصطلحات شائعة مثل برامج التجسس والفيروسات والديدان الإلكترونية، ونظرًا لارتفاع معدل الجرائم الإلكترونية برزت هذه المصطلحات فى عناوين الأخبار اليومية، وعند العودة بالزمن إلى وقت نشأة الأمن السيبرانى كانت أجهزة الكمبيوتر والإنترنت لا تزال قيد التطوير، وكان من السهل التعرف على التهديدات التى قد يتعرض لها الحاسوب.

ثم فى ثمانينيات القرن العشرين ابتكر العالم روبرت تى موريس أول برنامج فيروس إلكترونى، والذى حاز على تغطية إعلامية هائلة نظرًا لانتشاره بين الأجهزة وتسبّبه بأعطال فى الأنظمة، فحُكِم على موريس بالسجن والغرامة، وكان لذلك الحكم دور فى تطوير القوانين المتعلقة بالأمن السيبرانى.

ثم فى تسعينيات القرن العشرين تتوالى أحداث تطوّر الأمن السيبرانى بمرور الزمن، وذلك مع تطور الفيروسات التى تصيب الأجهزة، حيث أصبح العالم على اطلاع بالمخاطر الإلكترونية. ومن أبرز الإجراءات المُتخذة فى تسعينيات القرن العشرين وضع بروتوكولات حماية المواقع الإلكترونية

مثل (HTTP)، وهى من أنواع البروتوكولات التى تتيح للمستخدم وصولاً آمنًا لشبكة الإنترنت.

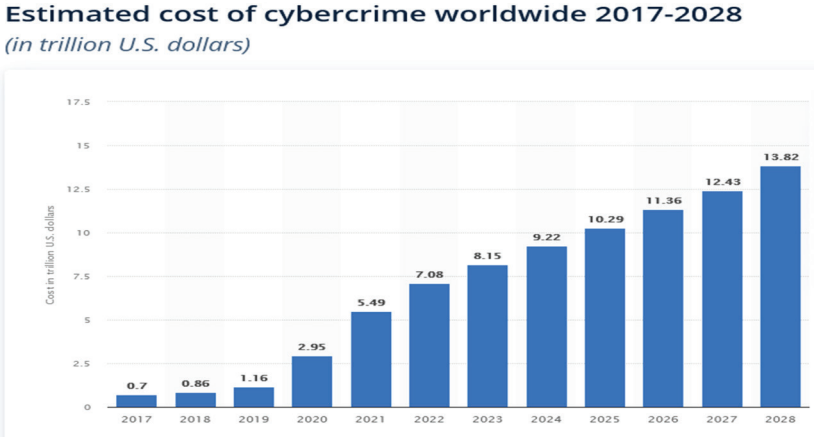
وهكذا استمر تطور الهجمات الإلكترونية والجرائم الإلكترونية، ومعها تطور الأمن السيبرانى حتى وصلنا إلى التقدم والتعقيد الذى وصلنا له، ففى العالم الرقمى الذى نعيش فيه اليوم أضحى الأمن السيبرانى مهماً كأهمية أنظمة الدفاع العسكرية، فالهجمات الإلكترونية المتطورة تستطيع أن تسبب أضرارًا تعجز عنها الحروب سواء كانت اقتصادية أو حتى بشرية، إننا نعتمد اليوم على الحواسيب وشبكة الإنترنت فى كل شيء تقريبًا (Middleton,Bruce,2017,p35).

المطلب الثالث: أهمية الأمن السيبرانى:

تُستخدم التكنولوجيا الحديثة فى كل جانب من جوانب أنشطتنا اليومية تقريبًا. أصبح العالم رقميًا بوتيرة متزايدة. يعتمد الأفراد والشركات وحتى الحكومات اليوم بشكل كبير على التكنولوجيا الحديثة. ولهذا السبب أصبح الأمن السيبرانى أمرًا هامًا وأساسيًا.

وتظهر الإحصائيات تزايد وتيرة وتكاليف الجرائم الإلكترونية على مستوى العالم، ونذكر فيما يلى بعض هذه الإحصائيات والتقديرات، والتى تعكس بوضوح تزايد أعداد الهجمات الإلكترونية والخسائر المالية الضخمة الناجمة عن الجرائم الإلكترونية، فوفقًا لتقرير تكلفة اختراق البيانات الصادر عن شركة IBM لعام ٢٠٢٣، «بلغ متوسط تكلفة اختراق البيانات فى عام ٢٠٢٣ مبلغ وقدره ٤,٤٥ مليون دولار أمريكى».

شكل رقم (١) التكلفة المقدرة للجرائم الإلكترونية[١]



أما على المستوى الدولى فبلغت تكلفة الجرائم الإلكترونية مبلغ ٨,١٥ تيرليون دولار أمريكى عام ٢٠٢٣ ويعكس الرسم البيانى السابق التوقعات العالمية للتكلفة المقدرة للجرائم الإلكترونية.

وبشكل عام، فإن للهجمات السيبرانية تأثيراً شديداً على الأفراد والشركات والحكومة والمجتمع؛ وسيتم تسليط الضوء على ذلك بإيجاز فى الفقرات القليلة التالية.

يشمل تأثير الهجمات السيبرانية على الأفراد حدوث خسائر مالية من خلال اختراق

(١) انظر، «تقرير تكلفة خرق البيانات ٢٠٢٣» الصادر عن شركة IBM، وهي شركة برمجيات رائدة للحاسب متعددة الجنسيات ، التقرير متاح باللغة الإنجليزية على الرابط:https://www.ibm.com/reports/data-breach؛ آخر دخول للموقع بتاريخ ٢٠٢٤/٠٣/٠٣
انظر التكلفة التقديرية للجرائم الإلكترونية عالميًا ٢٠١٧-٢٠٢٨»، والمتاحة على الرابط:
https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide؛ أخر دخول للموقع ٢٠٢٤/٣/٣

الحسابات المالية أو إتمام معاملات مالية غير مصرح بها، وكذلك احتمال سرقة الهوية (قد يؤدى ذلك بدوره إلى خسارة مالية إضافية أو حتى عواقب قانونية)، بالإضافة إلى التأثير السلبى على السمعة حال ترتب نشر معلومات أو صور خاصة نتيجة للهجمات الإلكترونية، وربما تصل العواقب إلى حدوث الإجهاد العقلى نتيجة الضغوط النفسية والعصبية (Benson, 2020, P73,74 Mcalane,).

يعد تأثير الهجمات السيبرانية على الأعمال أمرًا بالغ الأهمية لأن هذه الهجمات قد تؤدى إلى:

١- اضطرابات تشغيلية مثل فشل النظام أو التوقف عن العمل مما يؤدى إلى الحد من قدرة الشركة على أداء الأعمال بشكل طبيعى.

٢- الخسائر المالية بسبب التكاليف المتكبدة لإصلاح نتائج الهجوم مثل استعادة الأنظمة والأجهزة المتضررة، ودفع الفدية إن تم طلبها ولم يمكن تفادى دفعها، والخسارة المحتملة لأصول الملكية الفكرية، وتسوية التعقيدات القانونية المحتملة الناتجة عن الاضطرابات التشغيلية وعدم الامتثال للقوانين.

٣- الإضرار بالسمعة بسبب الكشف عن معلومات حساسة أو الفشل فى تقديم الخدمات أو تسليم المنتجات فى الوقت المناسب، وهذا بدوره قد يؤثر سلبًا على الثقة مع مختلف أصحاب المصلحة فى العمل وبالتالى تقويض سمعة المؤسسة وصورتها (Kala.2023).

قد يشمل تأثير الهجمات السيبرانية على الحكومات ما يلى:

١-الاضطرابات التشغيلية للخدمات العامة الحيوية مثل خدمات الرعاية الصحية وخدمات الشرطة.

٢-التأثير على ثقة الجمهور (الإضرار بالسمعة)، لأن المواطنين قد يشعرون بالقلق بشأن جودة الخدمات العامة ودرجة أمانها، لذا قد يصبحون قلقين بشأن إمكانية الكشف عن معلوماتهم الشخصية من قواعد البيانات الحكومية.

٣-الآثار المالية، لأن إصلاح الخسائر الناجمة عن الاختراقات قد يكلف مبالغ طائلة ولأنه مع تزايد هجمات الفدية قد تجد بعض المؤسسات العامة نفسها مضطرة إلى دفع فدية لتحرير المعلومات من قواعد بياناتها.

٤-مخاوف تتعلق بالأمن القومى، لأن الهجمات السيبرانية قد تستخدم لمهاجمة وكالات إنفاذ القانون أو الوكالات العسكرية الحساسة لأغراض التجسس أو التخريب أو لغير ذلك من الأغراض.

ونتيجة للمخاطر الجمة والجسيمة للهجمات السيبرانية وللأهمية الكبرى للأمن السيبرانى فقد أوصى صندوق النقد الدولى فى تقرير حديث له بضرورة تكاتف المجتمع الدولى لتعزيز التعاون المشترك من أجل حماية المنشآت المالية.(Nelson, Maurer,2021)

المطلب الرابع: أهداف الأمن السيبرانى

لما كان هدف الأمن السيبرانى النهائى هو تأمين الأجهزة والشبكات والمعلومات، والحفاظ عليها أمام أى اختراق أو هجمات أيًا كان نوعها، إلا أنّ هذا ليس كافيًا لتقريب المفهوم ووضع معايير الأمان حتى لخبراء الأمن السيبرانى، لهذا السبب قاموا بابتكار نموذج أو مثلث CIA الذى يجمع بين المفاهيم الثلاثة الأساسية للأمن السيبرانى، وهى:

أولاً: السرية Confidentiality، هى المرادف للخصوصية Privacy، والهدف منها هو منع أى وصول غير مصرح إلى البيانات.

ثانيًا: السلامة أو النزاهة Integrity، والحفاظ على البيانات دقيقة وسليمة من أى تعديل أو تغيير غير مُصرح به من قبل أى مخترق أو شخص ليس لديه الصلاحيات لفعل هذا.

ثالثًا: التوافر Availability، وذلك بجعل البيانات متاحة ومتوفرة وقابلة للاستخدام دائمًا وفى أى وقت من قبل الأشخاص الذين لديهم سلطة القيام بهذا، فهو يضمن عدم إعاقة النظام أو تعطيله من قبل الهجمات المختلفة (السمحانى، ٢٠٢٠، ص ١١).

المبحث الأول

الاتفاقيات الدولية والإقليمية فى مجال الأمن السيبراني

فى معرض تناولنا لماهية الأمن السيبرانى، أوضحنا الأهمية القصوى لتعاون الفاعلين فى المجتمع الدولى من دول ومنظمات دولية حكومية كانت أو غير حكومية، نحو وضع أطر تنظيمية ومؤسسية لتنسيق مختلف الجهود الوطنية التى تبذلها الدول نحو حماية الفضاء السيبرانى، والتصدى للأخطار السيبرانية المتزايدة لما لها من نتائج جسيمة على النحو المذكور أعلاه فى المبحث التمهيدى من هذه الدراسة.

وتلعب العديد من الهيئات والمنظمات والمجالس الدولية دورًا ملحوظًا فى تيسير وتنسيق إبرام الاتفاقيات الدولية فى مجال الأمن السيبرانى، وذلك فى محاولة منها لترسيخ وجوب التعاون الدولى لمواجهة الجرائم السيبرانية، وعلى رأس هذه المنظمات منظمة الأمم المتحدة والمجلس الأوروبى وبعض الهيئات الأخرى.

وعليه فإذا كنا قد انتهينا من الوقوف على ماهية الأمن السيبرانى، فإننا نستعرض فيما يلى جهود منظمة الأمم المتحدة فى مجال مكافحة الجريمة السيبرانية، ثم جهود باقى المنظمات الدولية فى ذات المجال، ونختتم باستعراض موجز لدور الاتفاقيات الإقليمية فى مجال مكافحة الجريمة السيبرانية.

المطلب الأول

جهود منظمة الأمم المتحدة فى مكافحة الجريمة السيبرانية

اتخذ المجلس الاقتصادى والاجتماعى التابع للأمم المتحدة توصية بأن تأخذ المنظمة الدولية على عاتقها دورًا رئيسًا فى رسم سياسة منع الجريمة وتحقيق العدالة الجنائية الدولية، وقد تحقق

ذلك بموافقة الجمعية العامة للأمم المتحدة فى العام ١٩٥٠م على التوصية التى بموجبها تم إنشاء اللجنة الاستشارية لخبراء منع الجريمة ومعاملة المجرمين التى يقع على عاتقها مهمة مكافحة الجريمة وتقديم المشورة للأمين العام وإيجاد البرامج ووضع الخطط ورسم سياسات لتدابير دولية فى مجال منع الجريمة ومعاملة المجرمين. وبعد انعقاد مؤتمر الأمم المتحدة لمنع الجريمة ومعاملة المجرمين فى كيوتو باليابان عام ١٩٧٠م، تم استبدال اللجنة الاستشارية بلجنة منع الجريمة ومكافحتها بناء على توصية للمجلس الاقتصادى والاجتماعى عام ١٩٧١م.

والذى يعنينا فى هذه الدراسة هو جهود الأمم المتحدة من خلال مؤتمراتها الخاصة بمنع الجريمة ومعاملة المجرمين المتعلقة بالجرائم التقنية أو جرائم الحاسب الآلى وهنا نشير إلى أن مؤتمر الأمم المتحدة السابع لمنع الجريمة ومعاملة المجرمين الذى تم انعقاده فى مدينة ميلانو بإيطاليا فى العام ١٩٨٥م (عباينة، ٢٠٠٩، ص ١٥٦).

قد انبثقت عنه مجموعة من القواعد التوجيهية والتى اكتملت صياغتها فى الأبحاث الإقليمية التحضيرية للمؤتمر الثامن الذى أجاز هذه المبادئ والذى عقد فى هافانا بكوبا فى العام ١٩٩٠م.

حيث أكد المؤتمر على وجوب تطبيق التطورات الجديدة فى مجال العلم والتكنولوجيا فى كل مكان لصالح الجمهور وبالتالى لمنع الجريمة على نحو فعال، كما أكد على أن التكنولوجيا بما أنها قد تولّد أشكالاً جديدة من الجرائم فإنه ينبغى اتخاذ تدابير ملائمة ضد حالات إساءة الاستعمال لصور التكنولوجيا الحديثة، ويمكن إجمال توصيات مؤتمر هافانا للعام ١٩٩٠م وذلك طبقا للمبادئ التالية:

١-تحديث القوانين الجنائية الوطنية بما فى ذلك التدابير المؤسسية.
٢- تحسين أمن الحاسب الآلى والتدابير المنيعة.
٣- اعتماد إجراءات تدريب كافية للموظفين والوكالات المسئولة عن منع الجريمة الاقتصادية والجرائم المتعلقة بالحاسب الآلى والتحرى والادعاء فيها.
٤-تلقين آداب الحاسب الآلى كجزء من مفردات مقررات الاتصالات والمعلومات واعتماد سياسات تعالج المشكلات المتعلقة بالمجنى عليهم فى تلك الجرائم.
٥- زيادة التعاون الدولى من أجل مكافحة هذه الجرائم (عباينة، ٢٠٠٩، ص ١٥٨).

المطلب الثاني
جهود المنظمات الدولية فى مجال مكافحة الجريمة السيبرانية

اتخذت العديد من المنظمات الدولية مبادرات عدة فى مجال مكافحة الجريمة السيبرانية، من قبل ذلك على سبيل المثال الجهود التى بذلها الاتحاد الدولى للاتصالات، منظمة الشرطة الجنائية الدولية (الإنتربول)، مؤسسة الإنترنت للأسماء والأرقام المخصصة، والمنظمة الدولية للمعايير (التوحيد القياسى)، واللجنة الكهرو-تقنية الدولية وفرق عمل هندسة الإنترنت، وغيرها من المنظمات والمؤسسات الدولية التى عنيت بالجرائم السيبرانية.

وفى الفقرات القليلة المقبلة نتناول أهم الجهود التى تقوم عليها بعض أهم المنظمات الدولية

فى مجال الأمن السيبرانى، فنتناول أولاً جهود الاتحاد الدولى للاتصالات، ثم جهود المعهد الوطنى للمعايير والتقنية بالولايات المتحدة الأمريكية، وأخيرًا جهود وكالة الاتحاد الأوروبى للأمن السيبرانى.

الفرع الأول
دور الاتحاد الدولى للاتصالات (ITU) فى مجال الأمن السيبرانى

الاتحاد الدولى للاتصالات هو وكالة تابعة للأمم المتحدة المتخصصة فى مجال تكنولوجيا المعلومات والاتصالات، وتأسس فى عام ١٨٦٥ لتسهيل التوصيلية العالمية وتحسين الاتصالات الدولية. ويعد الاتحاد الدولى للاتصالات المنظمة الرئيسية المسئولة عن تطوير المعايير الدولية لتكنولوجيا المعلومات والاتصالات، وتعزيز التوصيلية العالمية (Global Connectivity) وتحسين الوصول إلى تكنولوجيا المعلومات والاتصالات فى جميع أنحاء العالم [٢].

وفى إطار سعى الاتحاد الدولى للاتصالات لتأكيد القيام بدوره فى وضع وتطوير المعايير الدولية الخاصة بمجتمع الاتصالات وتكنولوجيا المعلومات أطلق الاتحاد دليلاً لوضع الاستراتيجية الوطنية للأمن السيبرانى وتم تعديلها أكثر من مرة، وفى الإصدار الأخير لهذا الدليل قام الاتحاد ببيان وتحديد الأطراف الفاعلة فى منظومات الأمن السيبرانى للدول والغرض من وضعه.

وقد شارك فى وضع هذا الدليل اثنا عشر شريكًا دوليًا كان من أبرزهم وكالة الاتحاد الأوروبى للأمن السيبرانى إضافة لعدد من المنظمات الحكومية الدولية والمنظمات الدولية والقطاع الخاص والمجتمع المدنى.

وقد تحدد فى مستهل الدليل الغرض الأساسى لهذا الدليل «وهو توجيه القادة الوطنيين وواضعى السياسات لدى وضع استراتيجية وطنية للأمن السيبرانى وذلك بهدف وضع إطار مفيد ومرن وسهل الاستخدام لتحديد سياق رؤية البلد الاجتماعية والاقتصادية والموقف الأمنى الراهن».

كما يتحدد نطاق الدليل حسبما توضح فيه ليشمل مختلف جوانب تحديات الأمن السيبرانى المتمثلة فى الحوكمة والسياسة والجوانب التشغيلية والتقنية والقانونية وصولاً للمبادئ الشاملة والممارسات الجيدة حتى يتم صياغة الاستراتيجية مع الأخذ فى الاعتبار الواقع، وهو الإجراءات «العملية» التى تتخذها الدول فى مختلف مراحل الاستراتيجية وبين محتوى النص الفعلى للاستراتيجية (جعفر، القاضى، ولبيب، ٢٠٢٣، ص ٩٢،٩٣) .

تم تحديد الجمهور المستهدف من الدليل بأنهم أولاً القادة الوطنيون وواضعو السياسات لتطوير استراتيجية وطنية للأمن السيبرانى، ثم مجموعة أصحاب المصلحة الآخرين ومنهم الحكوميون والمنظمات التنظيمية ومقدمو خدمات تكنولوجيا المعلومات والاتصالات والمؤسسات الأكاديمية ومؤسسات البحوث.

نعرض بعد ذلك الدليل للممارسات الجيدة فى الاستراتيجية الوطنية للأمن السيبرانى، حيث ركز على مفاهيم محددة أطلق عليها مجالات التركيز وهى:

(2)-www.itu.int

١-الحوكمة.

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

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

٢-إدارة المخاطر فى مجال الأمن السيبرانى الوطنى.

مجال التركيز الثانى «إدارة المخاطر» يتعلق بضرورة اعتماد نهج لإدارة المخاطر فى مجال الأمن السيبرانى الوطنى؛ حيث يتم تحديد وتقييم المخاطر التى 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 فى مجال الأمن السيبرانى كامل دورة الحياة، من الوضع أو التوريد إلى التشغيل والاستبدال.

٣-التأهب والصمود.

يركز على تعزيز قدرة الدول على التعامل مع الهجمات السيبرانية وتحمل آثارها، وذلك من خلال تطوير قدرات الاستجابة والاستعداد للتعامل مع هذه الهجمات والتصدى 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 فى مختلف المؤسسات وإجراء تمارين الأمن السيبرانى، بغية رفع مستوى التأهب والصمود فى حال حدوث أى هجوم سيبرانى.

٤-خدمات البنية التحتية الحرجة والخدمات الأساسية.

يرتكز المجال الرابع «البنية التحتية الحرجة» على تعزيز أمن البنية التحتية المهمة والحرجة فى 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 فى ذلك استخدام التقنيات الأمنية المتقدمة وإنشاء نظام مراقبة مستمر لهذه الأصول. كذلك، يشتمل هذا المجال على توفير التدريب والتوعية لفرق أمن المعلومات فى مؤسسات البنية التحتية، بغية رفع مستوى حساسية هذه المؤسسات لأى تهديد سيبرانى قد يستهدفها مع تعزيز التعاون بينها وبين مختلف الأطراف المعنية والعاملة فى هذا المجال.

٥-المقدرة وبناء القدرات وإذكاء الوعى.

يتركز هذا المجال «التوعية وبناء القدرات» على تعزيز قدرات الأفراد والمؤسسات والحكومات فى مجال الأمن السيبرانى، وذلك من خلال تطوير برامج تدريبية وتعليمية لتحسين المهارات والخبرات فى هذا المجال. كما يشمل أيضًا تطوير استراتيجيات لتحفيز الابتكار فى مجال الأمن السيبرانى، بما فى ذلك دعم بحوث التقنية وتطوير حلول جديدة للتحديات المستقبلية. كذلك يشتمل هذا المجال على إذكاء الوعى بأهمية الأمن السيبرانى، بصفة عامة وفى مؤسسات محددة، من خلال حملات توعية وإعلامية ووضع مناهج تعليمية للأمن السيبرانى فى المدارس والجامعات.

٦-التشريع والتنظيم.

يهدف هذا المجال إلى وضع إطار قانونى وتنظيمى لحماية المجتمع من الجرائم السيبرانية، وتشجيع بيئة سيبرانية آمنة ومأمونة. يشمل هذا المجال تحديد ما يشكل نشاطًا سيبرانيًا غير قانونى، والاعتراف القانونى بالحقوق الفردية والحريات المدنية فى البيئة السيبرانية.

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

٧-التعاون الدولى.

يهدف المجال السابع فى استراتيجية الأمن السيبرانى إلى تعزيز التعاون الدولى فى مجال الأمن السيبرانى، وذلك من خلال المشاركة فى المناقشات والتفاوضات الدولية، وتعزيز التعاون الرسمى وغير الرسمى فى الفضاء السيبرانى، وتحقيق توافق دولى حول قواعد سلوكية للدول فى هذا المجال. كما يهدف إلى تطوير آليات لتبادل المعلومات والخبرات بشأن جرائم الأمن السيبرانى بين دول مختلفة، وتحديد أفضل الممارسات فى هذا المجال.

الفرع الثاني
دور المعهد الوطنى للمعايير والتكنولوجيا (NIST) بالولايات المتحدة الأمريكية فى مجال الأمن السيبراني

يعد المعهد الوطنى للمعايير والتكنولوجيا – أو كما يشتهر عالميًا اختصارًا (NIST) مؤسسة حكومية أمريكية تعمل تحت إشراف وزارة التجارة الأمريكية وقد تأسس هذا المعهد فى عام ١٩٠١، ويضم المعهد – بصفته المسئول الأول عن تطوير وتعزيز القياسات والمعايير والتقنية فى الولايات المتحدة الأمريكية – مجموعة من المختبرات المتخصصة فى العلوم والتكنولوجيا، وكذا مركزًا للأبحاث والتطوير [٣].

(3)-www.nist.gov/about-nist

إطار الأمن السيبرانى الخاص بالمعهد الوطنى:

قام المعهد الوطنى للمعايير والتكنولوجيا بوضع عدة أطر لتنظيم وتحسين التعامل مع موضوع الأمن السيبرانى على مستوى الصناعة والشركات والمؤسسات وعلى المستوى الوطنى كذلك، ومن ضمن هذه الأطر إطار العمل الخاص بالأمن السيبرانى الصادر نسخته الأولى عام ٢٠١٤ وما سبقه من إرهاصات للإطار وما تلاه من تحسينات وتعديلات مخطط وصول تحديث لها العام القادم.

حدد الإطار خمسة عناصر أساسية يندرج تحتها العديد من تفاصيل الإجراءات والعمليات الدقيقة المنضبطة والمتتابعة فى إجراءات حوكمة، وهو ما سنتناوله على النحو التالى:

العنصر الأول: التحديد أو التعرف (Identify).

يعنى تحديد وفهم المخاطر السيبرانية التى تواجه المؤسسة وتحديد الأصول السيبرانية المهمة والحساسة التى يجب حمايتها، تتضمن عملية التحديد العديد من الخطوات التى يجب على المؤسسات اتباعها، ومن بين هذه الخطوات:

١- **تحديد الأصول السيبرانية:** يجب على المؤسسات تحديد الأصول السيبرانية التى 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 التى 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 السيبرانى والامتثال لها، مثل متطلبات الامتثال لقواعد الامتثال الصادرة عن هيئات التنظيم واللوائح الحكومية المتعلقة بالأمن السيبرانى.

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

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

العنصر الثانى: الحماية (Protect).

يهدف هذا العنصر إلى توفير الحماية اللازمة للأصول السيبرانية المهمة من خلال تنفيذ إجراءات الأمن السيبرانى اللازمة، ويشتمل عنصر الحماية على العديد من الخطوات التى يجب على المؤسسات اتباعها، ومنها الآتى بيانه:

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 الوعى الأمنى:** يجب على المؤسسات تعزيز الوعى الأمنى لدى الموظفين والعاملين فى المؤسسة، وتوفير التدريب والتعليم اللازمين لهم لزيادة وعيهم بمخاطر الأمن السيبرانى 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 والتحقق من الهوية والتفويض والتحكم فى الوصول والتسجيل والمراقبة.

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

٥-**تحسين الأمن السيبرانى لسلسلة التوريد:** يجب على المؤسسات تحسين الأمن السيبرانى لسلسلة التوريد وضمان أن الموردين يلتزمون بمعايير الأمان السيبرانى 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.

العنصر الثالث: الكشف (Detect).

يهدف هذا العنصر إلى تعزيز قدرة المؤسسة على الكشف المبكر عن الهجمات السيبرانية والأحداث الأمنية غير المرغوب فيها والتحقق منها بشكل فعال.

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»[٤] واستخدام التقنيات الحديثة، مما يسهم فى تقليل الوقت اللازم للاستجابة للأحداث الأمنية وتقليل الأضرار الناجمة عنها.

العنصر الرابع: الاستجابة (Respond).

يهدف هذا العنصر إلى تعزيز قدرة المؤسسة على الاستجابة للهجمات السيبرانية وإعادة تأهيل الأنظمة والبيانات المتأثرة وتقليل الأضرار الناجمة عن الهجمات. وتشمل أنشطة هذا العنصر العديد من الخطوات التى يجب على المؤسسات اتباعها، ومن بين هذه الخطوات:

(٤) الأتمتة Automation هي مجموعة من العناصر أو العمليات الحاسوبية والميكانيكية والكهروميكانيكية التي تعمل بأقل تدخل بشري أو بدون تدخل بشرى، وتُستخدم الأتمتة Automation عادةً لتحسين تشغيل مصنع صناعي أو شركة وغيرها من المجالات المنتجة والمستعدة لمواكبة التحول الرقمي

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

٢-**الحد من الأضرار:** يتعين اتخاذ المؤسسات للإجراءات اللازمة للحد من الأضرار الناجمة عن الهجمات السيبرانية وإعادة تأهيل الأنظمة والبيانات المتأثرة، وتقييم الأضرار وتحديد الأولويات فى إعادة بناء البنية التحتية للمؤسسة.

٣-**التحليل الجنائى الرقمى:** يجب على المؤسسات القيام بالتحليل الجنائى الرقمى للأحداث السيبرانية والهجمات المتعلقة بها، وجمع الأدلة الرقمية وتقييمها وتحليلها لتحديد المسئوليات والمصادر والأساليب المستخدمة فى الهجوم، وتحديد الأدلة الرقمية التى يمكن استخدامها فى التحقيقات الجنائية.

٤-**تحسين الأتمتة:** يجب على المؤسسات تحسين الأتمتة فى عمليات الاستجابة للحوادث، وذلك من خلال استخدام أدوات الأتمتة والذكاء الاصطناعى والتعلم الآلى والتحليل الآلى 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.

بشكل عام، يعتبر عنصر الاستجابة جزءًا أساسيًا فى الحفاظ وتعزيز الأمان السيبرانى للمؤسسات، ويساعد فى 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: التعافى (Recover)

يهدف هذا العنصر إلى توفير الإجراءات والخطط اللازمة لاستعادة الوظائف الأساسية للمؤسسة بعد وقوع هجمات سيبرانية أو حوادث أمنية أخرى. تشمل أنشطة عنصر التعافى العديد من الخطوات والأنشطة التى 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 فى حالة وقوع هجمات سيبرانية أو حوادث أمنية أخرى وهى الموارد الأكثر تأثراً والأوسع انتشارًا.

٢-**الإجراءات الاحتياطية:** يجب على المؤسسات تنفيذ الإجراءات اللازمة لإعداد نسخ احتياطية للبيانات والأنظمة والتطبيقات الحيوية والحساسة وتخزينها فى 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 دورى (جعفر، القاضى، ولبيب، ٢٠٢٣، ص ١١٥،١١٦) .

الفرع الثالث

دور الوكالة الأوروبية للأمن السيبرانى (ENISA) فى مجال الأمن السيبراني

تعمل وكالة الاتحاد الأوروبى للأمن السيبرانى – تتبع منظمة الاتحاد الأوروبى وتم إنشاؤها فى عام ٢٠٠٤ – على تعزيز قدرة دول الاتحاد ومنظمات القطاع الخاص بدول الاتحاد على منع وكشف والاستجابة للتهديدات السيبرانية.

تقوم الوكالة بتطوير خطط استراتيجية وخطط عمل تنفيذية محددة للأمن السيبرانى، تهدف هذه الخطط إلى تحسين قدرة الاتحاد الأوروبى على التصدى للتهديدات السيبرانية وحماية الشبكات والمعلومات الحيوية. وتتضمن الخطة الاستراتيجية الحالية للأمن السيبرانى فى الوكالة العديد من المبادرات والأنشطة التى تشمل تحسين التعاون بين الدول الأعضاء وتعزيز الوعى والتدريب فى مجال الأمن السيبرانى وتطوير المعايير الأوروبية للأمن السيبرانى وتوفير المشورة الفنية فى هذا المجال.

وتعمل الوكالة على تحقيق عدد من الأهداف الاستراتيجية فى مجال الأمن السيبرانى يمكن إيجازها فيما يلى:

١-تعزيز الوعى الأمنى وتعزيز الثقافة الأمنية فى المؤسسات والمنظمات والمجتمعات.

٢-دعم تطوير وتحسين قدرات الأمن السيبرانى فى أوروبا.

٣-تعزيز التعاون والتنسيق بين الدول الأوروبية والمؤسسات والمنظمات المختلفة فى مجال الأمن السيبرانى.

٤-توفير الدعم والمساعدة للمؤسسات والمنظمات فى التصدى للتهديدات السيبرانية والحوادث الأمنية.

٥-تطوير المعايير والممارسات والأدوات الأمنية اللازمة لتحقيق الأمن السيبرانى فى أوروبا.

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

٧-تقييم وتحسين الأمن السيبرانى فى القطاعات الحيوية والحكومية والخدمات الرقمية والأسواق الرقمية.

٨-توفير الدعم والمساعدة فى مجال الأمن السيبرانى للمواطنين والمستخدمين.

٩-تعزيز البحث والتطوير فى مجال الأمن السيبرانى وتطبيق التقنيات الحديثة لتحقيق الأمن السيبرانى.

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

المطلب الثالث

دور الاتفاقيات الإقليمية فى مجال مكافحة الجريمة المعلوماتية

بالإضافة إلى الجهود الدولية التى تقوم بها المنظمات الدولية المذكورة أعلاه، فإن هناك جهوداً دولية أخرى تقوم بها منظمات دولية ذات طابع إقليمى، ولا تقل تلك الجهود أهمية عن الجهود التى تقوم بها المنظمات والمؤسسات الدولية متعددة الأطراف (تشمل دولاً من أكثر من منطقة جغرافية).

وقد ظهر دور المنظمات الإقليمية فى مجال مكافحة الجرائم السيبرانية جليًا من خلال ما قدمته تلك المنظمات من اتفاقيات فى هذا المجال، حيث اجتمع المجلس الأوروبى عام ٢٠٠١ فى العاصمة المجرية بودابست فى ٢٣ نوفمبر ٢٠٠١، للتشاور حول هذه الظاهرة الإجرامية المستحدثة والاتفاق على بنود واضحة لمكافحة جرائم تقنية المعلومات، وقد أبرمت الاتفاقية الأوروبية الدولية لمكافحة الإجرام السيبرانى (الإجرام عبر الإنترنت)، وقد صارت تلك الاتفاقية هى الأساس القانونى العالمى لمكافحة الإجرام السيبرانى. كما كان لمنظمة جامعة الدول العربية جهودٌ فى هذا الصدد حيث أصدرت الجامعة الاتفاقية العربية لمكافحة جرائم تقنية المعلومات عام ٢٠١٠م.

وعليه خلال الفقرات القليلة المقبلة نتناول اتفاقية بودابست (الاتفاقية المتعلقة بالجريمة الإلكترونية)، ثم الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

الفرع الأول

اتفاقية بودابست لمكافحة الجريمة السيبرانية

تم تبنى اتفاقية بودابست لمكافحة الجريمة السيبرانية بعد أعمال واجتماعات للجنة الأوروبية المعنية بمشاكل الإجرام جاوزت الخمس سنوات، وقد جاءت هذه الاتفاقية نتيجة محاولات عديدة منذ ثمانينيات القرن العشرين حتى ظهرت بشكلها النهائى فى ٢٠٠١/١١/٢٣م فى بودابست، وتعكس هذه الاتفاقية حرص مجلس أوروبا على التصدى للاستخدام غير المشروع للحاسبات وشبكات المعلومات. وقد جاءت الاتفاقية نتيجة مشاورات طويلة بين الحكومات وأجهزة الشرطة وقطاع الكمبيوتر، والتى صيغت فى مجلس أوروبا بمساعدة عدة دول منها الولايات المتحدة الأمريكية، وتمثل الاتفاقية ركيزة أساسية منذ دخولها حيز النفاذ فى الأول من يوليو لعام ٢٠٠٤ على مستوى الدول أعضاء مجلس الاتحاد الأوروبى(سليمان، وعبدالحليم، ص ٣٤).

وكان للاتفاقية السبق فى وضع قائمة للجرائم التى يجب على الدول المصادقة عليها أن تجرمها فى قوانينها الداخلية، وتعد الاتفاقية هى الأولى فى مجال مكافحة جرائم الإنترنت وشملت العديد من جرائم الإنترنت منها: الإرهاب، تزوير بطاقات الائتمان، دعارة الأطفال وتعمد الاتفاقية إلى تنسيق القوانين الجديدة فى دول عديدة.

ولأهمية الاتفاقية محل الدراسة فقد وقعت عليها ثلاثون دولة بما فى ذلك أربعة دول من غير الأعضاء فى مجلس أوروبا، وهى كندا واليابان وجنوب إفريقيا والولايات المتحدة الأمريكية، إذ أنّ هذه الاتفاقية مفتوحة للدول الأعضاء في مجلس أوروبا وكذلك للدول من خارج المجلس، وقد انضمت لها العديد من الدول من غير أعضاء مجلس أوروبا وقد بلغ عدد الدول المنضمة لها حتى يونيو ٢٠٢٣ عدد ٨٩ دولة منها تونس في غضون النصف الثاني من ذات العام ، وعلى الرغم من أن العديد من الدول غير الأوروبية قد انضمت إلى الاتفاقية، إلا أن مصر لم توقع أو تصادق على هذه الاتفاقية حتى الآن، وتتضمن الاتفاقية أربعة أبواب: الباب الأول استخدام المصطلحات، الباب الثانى التدابير الواجب اتخاذها على الصعيد الوطنى – الباب الثالث الولاية القضائية والتعاون الدولى، الباب الرابع الأحكام الختامية (أحمد، ٢٠١١،ص ١٢) .

وفيما يلى نلقى الضوء بشكل موجز على الاتفاقية.

الغصن الأول
التعريفات والمصطلحات المستخدمة فى الاتفاقية

أوردت المادة الأولى من الاتفاقية التعريفات الأساسية لكل من النظام المعلوماتى ومقدم الخدمة والبيانات المعلوماتية والبيانات المتعلقة بالمرور وذلك على النحو التالى:

أ –النظام المعلوماتى يعنى كل آلة بمفردها أو مع غيرها من الآلات المتصلة أو المرتبطة، والتى يمكن أن تقوم سواء بمفردها أو مع مجموعة عناصر أخرى تنفيذًا لبرنامج معين، بأداء معالجة آلية للبيانات.

ب –البيانات المعلوماتية تعنى كل تمثيل للوقائع، أو المعلومات أو المفاهيم تحت أى شكل، وتكون مهيأة للمعالجة الآلية بما فى ذلك برنامج معد من ذات الطبيعة، يجعل الحاسب يؤدى المهمة.

ج –مقدم الخدمة يشير إلى:

– كل جهة عامة أو خاصة تقدم لمستخدمى خدماتها إمكانية الاتصال عن طريق النظام المعلوماتى.

– كل جهة أخرى تعالج أو تخزن البيانات المعلوماتية بدلاً من خدمة الاتصال أو نيابة عن مستخدمى هذه الخدمة.

د –البيانات المتعلقة بالمرور تعنى كل البيانات التى تتعامل مع الاتصال، والتى تمر من خلال النظام المعلوماتى، أو يتم إعدادها بواسطة هذا الأخير، والذى يعد عنصرًا فى سلسلة الاتصال بالإشارة إلى مصدر الاتصال، مكان الوصول، خط السير، الساعة التاريخ، الحجم، مدة الاتصال، أو نوع الخدمة المؤداة.

الغصن الثاني
التدابير الواجب اتخاذها على الصعيد الوطني

تناولت الاتفاقية فى الباب الثانى التدابير الواجب اتخاذها على الصعيد الوطنى، وقد انقسمت تلك التدابير إلى قسمين، يتناول القسم الأول القانون الجنائى الموضوعى، بينما يتناول القسم

الثانى القانون الإجرائى، وسوف نتناول فى هذا الجزء من الدراسة الماثلة القسم الأول فقط وهو المتعلق بالجوانب الموضوعية للجرائم المعلوماتية والواردة فى المواد من (٢– ١٣) من الاتفاقية.

أولاً: الجرائم ضد سرية وسلامة وإتاحة البيانات والنظم المعلوماتية:

تشمل تلك الجرائم عدد خمس جرائم، نلقى فيما يلى الضوء عليها.

١– جريمة النفاذ (الولوج) غير المشروع:

تنص المادة الثانية من الاتفاقية على أنه يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من أجل اعتبارها جريمة جنائية، وفقا لقانونه الداخلى، للولوج العمدى لكل أو لجزء من جهاز الحاسب بدون حق، كما يمكن له أن يشترط أن ترتكب الجريمة من خلال انتهاك إجراءات الأمن، بنية الحصول على بيانات الحاسب أو أية نية إجرامية أخرى، أو أن ترتكب الجريمة فى حاسب آلى يكون متصلاً عن بعد بحاسب آخر.

وعلى ذلك، فإن مجرد التدخل غير المصرح به أو السطو بمعنى القرصنة أو الدخول غير المشروع فى النظام المعلوماتى كل أولئك يجب أن يعتبر غير قانونى فى حد ذاته كمبدأ عام.

٢– جريمة الاعتراض غير المشروع:

تنص المادة الثالثة من الاتفاقية على أنه يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يراها ضرورية لاعتبارها جريمة جنائية، وفقًا لقانونه الداخلى لواقعة الاعتراض العمدى وبدون حق، من خلال وسائل فنية للإرسال غير العلنى لبيانات الحاسب فى مكان الوصول، فى المنشأ، أو فى داخل النظام المعلوماتى، بما فى ذلك الانبعاثات الكهرومغناطيسية من جهاز حاسب يحمل هذه البيانات. كما يمكن لأى طرف أن يشترط أن ترتكب الجريمة بنية إجرامية بقصد الغش، أو أن ترتكب الجريمة فى حاسب آلى يكون متصلاً عن بعد بحاسب آخر.
(Final activity report", "Draft explanatory memorandum,2001)

٣– جريمة الاعتداء على سلامة البيانات:

تنص المادة الرابعة من الاتفاقية على تجريم الاعتداء على سلامة البيانات، إذا حدث ذلك عمدًا، ودون حق، وترتب عليه إلحاق أضرار، أو محو، أو تعطيل، أو إتلاف، أو طمس لبيانات الحاسب، كما يمكن لأى طرف أن يحتفظ بحق اشتراط أن يكون السلوك المنصوص عليه فى الفقرة الأولى يؤدى إلى أضرار جسيمة.

وتشير المذكرة التفسيرية إلى أن الهدف من تقرير هذا النص هو أن تكون بيانات وبرامج الحاسب مكفولة بحماية مماثلة ضد الأضرار التى تحدث عمدًا، والمصالح القانونية المحمية لتلك التى تتمتع بها الأشياء المادية وحسن تشغيل يقصد بها سلامة البيانات أو البرامج أو حسن استخدام بيانات الحاسب المسجلة.

٤– جريمة الاعتداء على سلامة النظام:

تنص المادة الخامسة من الاتفاقية على تجريم الإعاقة الخطيرة، إذا تمت عمدًا، ودون حق، لوظيفة نظام الحاسب عن طريق إدخال، أو نقل، أو إضرار، أو محو، أو تعطيل، أو إتلاف أو طمس البيانات المعلوماتية.

وتوضح المذكرة التفسيرية أن التوصية رقم (٨٩) قد أشارت إلى هذا العنوان تحت مسمى تخريب نظام الحاسب، ويهدف هذا النص إلى تجريم الإعاقة العمدية للاستخدام الشرعى للنظم المعلوماتية بما فى ذلك نظم الاتصالات باستخدام أو التأثير على بيانات الحاسب.

والمصالح القانونية المحمية هى مصلحة مشغلى ومستخدمى نظام الحاسب، أو نظام الاتصالات فى عمل هذه الأجهزة بدقة، وتتم صياغة النص بطريقة محايدة من أجل حماية كل أنواع الوظائف من خلاله، ومصطلح الإعاقة يرتبط بالأفعال التى تحمل اعتداء على حسن تشغيل نظام الحاسب، وهذه الإعاقة يجب أن تكون ناجمة عن الإدخال أو الإضرار أو النقل أو الإتلاف أو المحو أو طمس البيانات المعلوماتية.

٥- جريمة إساءة استخدام أجهزة الحاسب:

تنص المادة الثانية من الاتفاقية على أنه:

- يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية للتجريم وفقا لقانونه الداخلى، إذا وقع الفعل عمدًا، ودون حق بما يلى:
- إنتاج أو بيع أو الحصول من أجل الاستخدام أو استيراد أو نشر أو أى أشكال أخرى للوضع تحت التصرف.
- أى جهاز يحتوى على برنامج معلوماتى مصمم بشكل أساسى لغرض ارتكاب إحدى الجرائم المنصوص عليها وفقاً للمواد من ٢-٥ السابق الإشارة إليها.
- كلمة المرور أو شفرة الدخول أو أى بيانات مماثلة تسمح بالولوج إلى كل وجزء من نظام الحاسب بنية استخدامها لغرض ارتكاب جريمة من الجرائم المشار إليها فى المواد من ٢-٥
- حيازة أى عنصر من العناصر المشار إليها فى البندين أ - (١)، أ - (٢) من المادة السادسة من اتفاقية بودابست[٥]، وذلك بنية استخدامه فى ارتكاب أى جريمة من الجرائم الواردة فى المواد ٢-٥.
- ويمكن لأى طرف أن يشترط فى قانونه الداخلى وجود بعض هذه العناصر لتقرير المسئولية الجنائية.
- هذه المادة لا يجب أن تفسر على أنها تفرض مسئولية جنائية حينما يكون إنتاج أو بيع أو الحصول من أجل الاستخدام أو الاستيراد أو النشر أو أي أشكال أخرى للوضع تحت التصرف المشار إليه فى الفقرة الأولى من هذه المادة، ليس بهدف ارتكاب جريمة، وفقا للمواد ٢ – ٥ من هذه الاتفاقية، مثال ذلك حالة الاختبار المصرح به أو حماية نظام الحاسب.
- كل طرف يمكن أن يحتفظ بحقه فى تطبيق الفقرة الأولى من هذه المادة بشرط ألا يحمل هذا التحفظ بيعاً أو توزيعاً أو وضعاً تحت التصرف لأى عنصر من العناصر المشار إليها فى البندين ١ - (١)، ١ - (٢).

(٥) تنص المادة ٦ من اتفاقية بودابست علي الآتى «إساءة استخدام الأجهزة . ١- تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمداً وبغير حق: أ. عملية إنتاج، بيع، شراء بغرض الاستخدام، استيراد، توزيع أو إتاحة بأي طرق أخرى. ١ - جهاز، بما في ذلك برنامج كومبيوتر، تم تصميمه أو ملاءمته مبدئيا، بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من ٢ إلى ٥. ٢ - كلمة سر خاصة بكومبيوتر، أو رمز الولوج، أو بيانات مماثلة يمكن بواسطتها النفاذ بشكل كامل أو جزئي إلى نظام كومبيوتر، بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من ٢ إلى ٥» .

كما يتطلب ارتكاب هذه الجرائم غالبًا حيازة وسائل الولوج مثال ذلك أدوات القرصنة، أو أى أدوات أخرى، فإن هناك دافعًا قويًا للحصول عليها لأغراض إجرامية الأمر الذى يمكن أن يؤدى فى النهاية إلى خلق نوع من السوق السوداء لإنتاج وتوزيع مثل هذه الأدوات.

ثانيًا: الجرائم المعلوماتية المتصلة بالحاسب الآلى:

تشمل تلك الجرائم ما يلي:

١- جريمة التزوير المعلوماتى:

تنص المادة السابعة من الاتفاقية على تجريم الإدخال أو الإتلاف أو المحو أو الطمس العمدى وبدون حق للبيانات المعلوماتية الذى يتوالد عنه بيانات غير صحيحة، بقصد أخذها فى الحسبان، لو تم استخدامها لأغراض قانونية كما لو كانت صحيحة، بصرف النظر عما إذا كانت سهلة القراءة وواضحة أم لا، ويمكن لأى طرف أن يشترط فى قانونه الداخلى نية الغش أو أى نية إجرامية مشابهة من أجل تقرير المسئولية الجنائية.

وتحصر المذكرة التفسيرية الغرض من هذه المادة فى خلق جريمة موازية لجريمة تزوير المستندات الورقية، وتهدف هذه الجريمة إلى استكمال أوجه النقص التى تعترى قانون العقوبات بالنسبة للتزوير التقليدى الأمر الذى يتطلب سهولة القراءة المرئية للإقرارات المتضمنة فى المحرر والتى لا تنطبق على البيانات المسجلة على دعامة إليكترونية.

٢- جريمة الاحتيال المعلوماتى:

تنص المادة الثامنة من الاتفاقية على تجريم التسبب فى إحداث ضرر مالى للغير عن طريق:

أ - الإدخال، الإتلاف، المحو، أو الطمس لبيانات الحاسب.

ب - كل شكل للاعتداء على وظيفة الحاسب بنية الغش أو أى نية إجرامية مشابهة من أجل الحصول دون حق على منفعة اقتصادية له أو للغير.

وتشير المذكرة التفسيرية إلى أنه مع حدوث الثورة التكنولوجية تضاعفت إمكانيات ارتكاب جرائم اقتصادية وعلى الأخص النصب والغش ببطاقات الائتمان، كما أن الأصول الممثلة أو المتداولة عن طريق النظم المعلوماتية كالأموال الإليكترونية، أو الودائع أصبحت هدفاً للتلاعبات، بنفس الأشكال التقليدية للملكية.

وهذه الجرائم تتكون بشكل أساسى من خلال التلاعبات بمدخلات النظام بمعنى تغذية الحاسب ببيانات غير صحيحة أو من خلال تلاعبات فى البرامج أو من خلال تدخلات أخرى فى معالجة البيانات، والهدف من هذه المادة تقرير الجزاء الجنائى لكل تلاعب تعسفى فى سياق المعالجة الآلية للبيانات يكون من شأنه نقل غير شرعى للملكية.

ثالثًا: الجرائم المتصلة بالمحتوى:

يغطى هذا الفصل الجرائم المرتبطة بالمحتوى، بمعنى الإنتاج أو النشر غير المشروع للمواد الإباحية الطفولية عبر النظم المعلوماتية، والذى يمثل نماذج تنفيذ الجريمة الأكثر خطورة، والذى بدأ فى الظهور حديثًا.

ومما تجدر الإشارة إليه أنه أثناء قيام اللجنة بوضع مسودة الاتفاقية محل البحث –ناقشت مدى إمكانية إدراج جرائم أخرى تتعلق بالمحتوى– مثال ذلك نشر دعاية عنصرية عبر نظم الحاسب أو النظم المعلوماتية. بيد أن اللجنة لم تكن فى وضع يسمح لها بالوصول إلى موافقة جماعية أو توافق بخصوص تجريم مثل هذا السلوك.

بالرغم من أن فكرة إدراج هذا النشر بوصفه جريمة جنائية قد وجد دعماً على نطاق واسع، إلا أن بعض الوفود أبدت تحفظات حقيقية، بإثارتها لمبدأ حرية التعبير.

وبالنظر إلى تعقد هذه المسألة فقد قررت اللجنة أن تكلف اللجنة الأوروبية للمشكلات الجنائية باقتراح إعداد بروتوكول إضافى يدرج بهذه الاتفاقية الحالية.

وفيما يلى نبين أحكام المادة التاسعة المتعلقة بالجرائم المتصلة بالمواد الإباحية للأطفال، والتى نصت على:

١- أنه يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية، للتجريم وفقاً لقانونه الداخلى السلوكيات التالية إذا ارتكبت عمدًا، ودون حق :

أ- إنتاج مواد إباحية طفولية بغرض نشرها عبر نظام معلوماتى.

ب- تقديم أو إتاحة مادة إباحية طفولية عبر نظام معلوماتى.

ج- النشر أو النقل لمادة إباحية طفولية عبر نظام معلوماتى.

د- واقعة التزود أو تزويد الغير بمادة إباحية طفولية عبر نظام معلوماتى.

هـ- حيازة مادة إباحية طفولية فى نظام معلوماتى أو فى أى وسيلة لتخزين البيانات المعلوماتية.

٢- توخيًا لأغراض الفقرة الأولى بعاليه، فإن المادة الإباحية الطفولية تشمل كل مادة إباحية تمثل بطريقة مرئية :

أ- حدث يقوم بسلوك جنسى صريح.

ب – شخص يبدو كأنه حدث يقوم بسلوك جنسى.

ج – صور حقيقية تمثل حدثًا يقوم بسلوك جنسى صريح.

٣-توخيا لأغراض الفقرة الثانية عاليه، فإن مصطلح «حدث» يشمل كل شخص عمره أقل من ١٨ عاماً. ومع ذلك فإنه يمكن لأى طرف أن يستوجب حدًا عمريًا أقل بشرط ألا يقل عن ١٦ عاماً.

٤-كل طرف له الحق فى عدم التطبيق كلياً أو جزئياً، الفقرات[١-(د)] و[١ -(هـ)] و [٢-(ب) و(٢)-(ح).

رابعًا: الجرائم المتصلة بالاعتداءات الواقعة على الملكية الفكرية والحقوق المجاورة(٦):

يحدد الفصل الرابع الجرائم المتعلقة بالاعتداء على الملكية الفكرية والحقوق المجاورة المرتبطة به، فقد نصت الاتفاقية على هذه النوعية من الجرائم، وذلك لأن الانتهاكات الواقعة على الملكية الفكرية هى أحد أشكال الإجرام المعلوماتى الأكثر شيوعًا، وبازدياد نسبته يزداد قلق أو انشغال

(٦) الحقوق المرتبطة (Related rights): هى حقوق فئات معينة من الأفراد والكيانات الذين يساهمون في نشر الأعمال الإبداعية أو أداءها، مثل الفنانين المؤدين، ومنتجى التسجيلات الصوتية، وهيئات البث. وتعتبر هذه الحقوق «مجاورة» أو «موازية» لحقوق المؤلف، لأنها تتعلق بالأعمال الإبداعية لكنها ليست الحقوق الأساسية المتعلقة بإبداع العمل نفسه.

العالم بأسره. وفيما يلى نبين أحكام المادة العاشرة الخاصة بالجرائم المتصلة بالاعتداءات الواقعة على الملكية الفكرية والحقوق المجاورة.

إذ تنص المادة رقم (١٠) على الجرائم المتصلة بالاعتداءات الواقعة على الملكية الفكرية والحقوق المجاورة.

١-يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية لتجريم – وفقاً لقانونه الداخلى – انتهاكات الملكية الفكرية المعرفة فى قانون ذلك الطرف، وفقاً للالتزامات التى تم التوقيع عليها فى ظل الاتفاقية العالمية لحق المؤلف الموقعة فى باريس فى ٢٤ يوليو ١٩٧١، واتفاقية برن لحماية الأعمال الأدبية والفنية واتفاقية الجوانب التجارية لحقوق الملكية الفكرية، واتفاقية المنظمة العالمية للملكية الفكرية (OMPI)، باستثناء أى حق معنوى ممنوح بواسطة هذه الاتفاقية – إذا ما ارتكبت هذه الأفعال عمداً، وعلى نطاق تجارى، وبواسطة نظام معلوماتى.

٢-يجب على كل طرف أن يتبنى الإجراءات التشريعية، وأية إجراءات أخرى، يرى أنها ضرورية لتجريم –وفقاً لقانونه الداخلي– انتهاكات الحقوق المجاورة، المعرفة فى قانون هذا الطرف، وفقاً للالتزامات التى تم التوقيع عليها فى ظل الاتفاقية الدولية لحماية الفنانين المؤدين أو العازفين ومنتجى الصوتيات ومنظمات البث المبرمة فى روما (اتفاقية روما).

٣-يمكن لأى طرف فى ظل ظروف محدودة للغاية أن يحتفظ بالحق فى عدم تطبيق المسئولية الجنائية، بالنسبة للفقرتين الأولى والثانية من هذه المادة بشرط توافر طرق أخرى فعالة وجاهزة، وألا يكون فى هذا التحفظ ما يحمل اعتداء على الالتزامات الدولية المفروضة على هذا الطرف، فى تطبيق الاتفاقيات الدولية المشار إليها فى الفقرتين الأولى والثانية من هذه المادة.

وتنبه المذكرة التفسيرية إلى أن انتهاكات حقوق الملكية الفكرية، وخاصة حق المؤلف تعتبر من بين الجرائم الأكثر انتشاراً على الإنترنت، الأمر الذى يهم كلاً من أصحاب أو حائزى حق المؤلف ومتخصصى الشبكات المعلوماتية.

وجدير بالذكر أن السهولة التى من خلالها يمكن عمل نسخ غير مصرح بها عن طريق التكنولوجيا الرقمية، والنطاق الذى بمقتضاه يتم إعادة الإنتاج والتوزيع عبر الشبكات الإليكترونية، كل ذلك فرض ضرورة وضع نصوص تشتمل على جزاءات جنائية تعمل على تعزيز التعاون الدولى فى هذا المجال.

وبمقتضى الأصول المشار إليها فى هذه المادة، فإن كل طرف يكون ملزمًا بتجريم الانتهاكات العمدية على الملكية الفكرية، وعلى الحقوق المتصلة، والتى يشار إليها تحت عنوان الحقوق المجاورة إذا كانت هذه الانتهاكات قد تم ارتكابها عن طريق نظام معلوماتى وعلى نطاق تجارى.
(Explanatory Report to the Convention on Cybercrime Budapest,.2001)

خامسًا: مسئولية الأشخاص المعنوية:

تنص المادة الثانية عشرة من الاتفاقية على أنه:

١- يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من أجل اعتبار الأشخاص المعنوية مسئولة عن الجرائم المشار إليها فى الاتفاقية الحالية، إذا ارتكبت لمصلحتها، عن طريق أى شخص طبيعى يتصرف بشكل فردى، أو بوصفه عضوًا فى مؤسسة الشخص المعنوى، ويمارس سلطة القيادة فى داخله بناء على القواعد التالية:

أ- سلطة تمثيل الشخص المعنوى.

ب – سلطة اتخاذ القرارات باسم الشخص المعنوى.

ج – سلطة ممارسة الضبط داخل الشخص المعنوى.

٢- بالإضافة إلى الحالات التى سبق النص عليها فى الفقرة ١، فإنه يجب على كل طرف أن يتخذ الإجراءات الضرورية من أجل التأكد من أن الشخص المعنوى يمكن أن يكون مسئولاً إذا تخلفت المراقبة أو الضبط من جانب شخص طبيعى مشار إليه فى الفقرة ١ فقد جعلت الاتفاقية أنه من الممكن ارتكاب الجرائم المشار إليها فى الفقرة ١ لحساب الشخص المعنوى عن طريق شخص طبيعى يتصرف تحت سلطته.

٣- طبقاً للمبادئ القانونية للطرف، فإن مسئولية الشخص المعنوى يمكن أن تكون جنائية، أو مدنية، أو إدارية.

٤- هذه المسئولية يجب أن تكون دون مساس بالمسئولية الجنائية للأشخاص الطبيعيين الذين ارتكبوا الجريمة.

وإذ كانت الاتفاقية قد أقرت المسئولية الجنائية للشخص المعنوى، وهو ما يتماشى مع الاتجاه القانونى الحالى الذى يسلم بمسئولية الأشخاص المعنوية، فإنّه يجب توافر أربعة شروط لتقرير مسئولية الشخص المعنوى وهى أنه يجب أن تكون الجريمة المرتكبة إحدى الجرائم المذكورة فى الاتفاقية، وأنه يجب أن تكون الجريمة قد ارتكبت لمصلحة الشخص المعنوى، وأن يكون الشخص الذى ارتكب الجريمة يمارس سلطة القيادة بما فى ذلك الشريك، ومصطلح شخص يمارس سلطة قيادة تعنى شخصًا طبيعيًا يتبوأ مكانة عالية فى المؤسسة مثال ذلك المدير ، وأن يكون الشخص الذى يمارس سلطة القيادة يتصرف استنادًا إلى سلطة من سلطاته وكسلطة اتخاذ القرارات أو ممارسة الضبط والتى تبرهن على أن الشخص الطبيعى المذكور قد تصرف فى نطاق سلطاته التى تستوجب مسئولية الشخص المعنوى.

الفصل الثالث
الأحكام المتعلقة بالجرائم المعلوماتية العابرة للحدود

أولاً: التعاون الدولي

تقرر المادة الثالثة والعشرون من الاتفاقية الأحكام العامة المتعلقة بالتعاون الدولى والتى جاء نصها أنه يجب على الأطراف أن تتعاون مع بعضها البعض وفقًا لأحكام هذا الفصل فى

تطبيق الأصول الدولية المتصلة بالتعاون الدولى فى المواد الجنائية، والاتفاقيات المعتمدة على التشريعات المتماثلة أو النظيرة والقوانين المحلية، إلى أوسع نطاق ممكن، لأغراض التنقيب والبحث أو الإجراءات الجنائية المتعلقة بالجرائم الجنائية المرتبطة بنظم وبيانات معلوماتية أو لجمع أدلة ذات شكل إلكترونى للجريمة الجنائية (المرجع التقريرى، ص ٤٤، ٤٦).

وتشير المذكرة التفسيرية لهذه الاتفاقية إلى أن هذه المادة تقرر ثلاثة مبادئ عامة تحكم التعاون الدولي وهى:

- المبدأ الأول: أن هذه المادة توجب على الأطراف أن تتعاون مع بعضها البعض فى أوسع نطاق ممكن.

فهذا المبدأ يفرض التزامًا على الأطراف بأن يعاون بعضهم بعضًا على نطاق واسع، وأن يقللوا ما استطاعوا العقبات التى ربما تعوق التدفق السريع للمعلومات والأدلة على المستوى الدولى.

- المبدأ الثانى: تبين المادة مدى الالتزام بالتعاون، فتقرر أن التعاون يجب أن يمتد نطاقه ليشمل كل الجرائم الجنائية المرتبطة بنظم وبيانات معلوماتية بمعنى الجرائم المشار إليها فى المادة (١٤) الفقرة الثانية البندين أ، ب من الاتفاقية.
- المبدأ الثالث: هذا التعاون يجب أن يُنفذ وفقًا لأحكام هذا الفصل وتطبيقًا للأصول الدولية المتصلة بالتعاون الدولى فى المواد الجنائية والاتفاقيات المعتمدة على التشريعات المماثلة أو النظيرة والقانون المحلى.

هذا البند الأخير المتعلق بالقانون المحلى ينشئ مبدأ عامًا بمقتضاه فإن شروط الفصل الثالث لا تبطل شروط الوثائق الدولية المتعلقة بالمساعدة القضائية واتفاقيات تسليم المجرمين النظيرة بين الأطراف بالنسبة لهذه الوثائق والمبينة بتفصيل أكثر فى تحليل المادة (٢٧) فيما بعد، أو شروط القانون المحلى المتعلقة بالتعاون الدولى.

وهذا المبدأ يتم دعمه بوضوح فى المواد (٢٤) المتعلقة بتسليم المجرمين، و(٢٥) المتعلقة بالمبادئ العامة للمساعدة المتبادلة، و ٢٦ المتعلقة بالمعلومات التلقائية و(٢٧) المتعلقة بالإجراءات الخاصة بطلبات المساعدة المتبادلة فى ظل غياب اتفاقيات دولية مطبقة، و(٢٨) المتعلقة بسرية وقيد الاستخدام، و(٣١) المتعلقة بالمساعدة المتبادلة الخاصة بالوصول أو بالولوج إلى البيانات المعلوماتية المخزنة بالحاسب، و(٣٣) المتعلقة بالمساعدة المتبادلة والخاصة بالتجميع فى الوقت الفعلى لبيانات المرور، و(٣٤) المتعلقة بالمساعدة المتبادلة الخاصة باعتراض بيانات المحتوى.

ثانيًا: تسليم المجرمين

تنص المادة الرابعة والعشرون من الاتفاقية على أنه

١-تنطبق هذه المادة على تبادل المجرمين بين الأطراف بالنسبة للجرائم الجنائية المعرفة وفقًا للمواد ٢-١١ من الاتفاقية الحالية، شريطة أن يكون معاقبًا عليها فى قانون الطرفين بعقوبة سالبة للحرية لا تقل عن سنة، أو بعقوبة أشد.

إذا كان الأمر يستلزم تطبيق عقوبة دنيا مختلفة، على أساس اتفاق تسليم مجرمين مطبق بين طرفين أو أكثر، بما فى ذلك الاتفاقية الأوروبية لتسليم المجرمين، أو أى اتفاقية منصوص عليها فى تشريعات متماثلة أو متناظرة، فإن العقوبة المنصوص عليها فى هذه الاتفاقية هى التى تطبق.

٢- الجرائم الجنائية الموصوفة فى الفقرة الأولى من هذه المادة يجب أن تعتمد جرائم تستوجب تسليم المجرمين فى كل اتفاق يتم بين أو من خلال الأطراف. ويجب على الأطراف أن تلتزم بإدماج هذه الجرائم بوصفها جرائم تستوجب تسليم المجرمين فى كل اتفاق لتسليم المجرمين يعقد فيما بينهم أو من خلالهم.

٣- إذا اشترط أحد الأطراف أن يكون تسليم المجرمين متوقفًا على وجود اتفاق لتلقى طلب تسليم مجرمين من طرف آخر لا يرتبط معه باتفاقية تسليم مجرمين، فإنه يمكن أن تعتبر هذه الاتفاقية (اتفاقية بودابست) كأساس قانونى لتسليم المجرمين بالنسبة لكل جريمة جنائية مشار إليها فى الفقرة الأولى من هذه المادة.

٤-الأطراف التى لا تشترط أن يكون التسليم متوقفاً على وجود اتفاقية سوف تقر بأن الجرائم الجنائية المشار إليها فى الفقرة الأولى من هذه المادة بمثابة جرائم تستوجب تسليم المجرمين فيما بينها.

٥- تسليم المجرمين يخضع للشروط المنصوص عليها بواسطة القانون الداخلى للطرف المطلوب منه التسليم أو لاتفاقيات تسليم المجرمين المطبقة، بما فى ذلك الأسباب التى من أجلها الطرف المطلوب منه التسليم يمكن أن يرفض هذا التسليم.

٦- إذا رفض تسليم المجرم بالنسبة لجريمة جنائية مشار إليها فى الفقرة الأولى من هذه المادة فقط بناء على جنسية الشخص المطلوب تسليمه أو لأن الطرف المطلوب منه التسليم يرى أنه هو المختص بهذه الجريمة، فإن الطرف المطلوب منه التسليم يحيل القضية بناء على طلب الطرف الملتمس إلى سلطاته المختصة بهدف إجراء التحقيقات، مع الأخذ فى الاعتبار الوقت المناسب لإرسال النتيجة النهائية للقضية للطرف الملتمس. وهذه السلطات ينبغى أن تتخذ قرارها وتباشر تحقيقاتها وإجراءاتها الجنائية بنفس طريقة أى جريمة أخرى لها نفس الطبيعة فى تشريع هذا الطرف.

٧- يجب على كل طرف أن يبلغ السكرتير العام لمجلس أوروبا وقت التوقيع أو التصديق أو القبول أو الموافقة على الانضمام إلى هذه الاتفاقية، اسم وعنوان كل سلطة مسئولة عن إرسال أو استلام طلب تسليم المجرمين، أو القبض المؤقت فى ظل غياب اتفاقية خاصة بذلك.

٨- يجب على السكرتير العام لمجلس أوروبا أن ينشئ ويهيئ سجلاً للسلطات المعنية بواسطة الأطراف. ويجب على كل طرف أن يتأكد دومًا من صحة البيانات المدرجة فى هذا السجل.

والملاحظ من مطالعة الفقرة الأولى من المادة (٢٤) سالفة الذكر أن الالتزام بتسليم المجرمين لا ينطبق إلا على الجرائم المعرفة وفقًا للمواد من (٢) إلى(١١) من الاتفاقية، والتى تكون

معاقبًا عليها فى تشريع كلا الطرفين بعقوبة سالبة للحرية لفترة لا تقل عن سنة أو بعقوبة أشد.
ويجوز للدولة التي يقدم إليها طلب التسليم أن ترفضه وفق الأسس المنصوص عليها في قانون الدولة سواء كانت عضوا في الاتفاقية أو غير عضو ووفق الأسس والإجراءات المنصوص عليها فى الاتفاقية – شرط ازدواجية التجريم – بمذكرة موضح بها الأسباب والأسس التي بنى عليها الرفض.

ثالثًا: المساعدة القضائية المتبادلة:

سوف نتناول هنا مادتين من مواد الاتفاقية، وهما المادة (٢٥) المتعلقة بالأحكام العامة التى تحكم المساعدة القضائية المتبادلة والمادة (٢٦) الخاصة بالمعلومات التلقائية أى تلك التى تأتى عفواً أو بطريقة عفوية.

حيث تنص المادة الخامسة والعشرون من الاتفاقية على أنّه:

١-يجب على كل الأطراف أن توفر لبعضها البعض مساعدة قضائية متبادلة إلى أقصى مدى ممكن لأغراض التحقيقات أو الإجراءات بالنسبة للجرائم الجنائية المرتبطة بنظم وبيانات معلوماتية أو بغرض جمع الأدلة الإلكترونية للجريمة الجنائية.

٢- يجب على كل طرف أيضًا أن يتبنى الإجراءات التشريعية وأية إجراءات أخرى يرى أنها ضرورية للوفاء بالالتزامات المنصوص عليها فى المواد(٢٧ إلى ٣٥).

٣-يمكن لكل طرف فى حالة الاستعجال أن يقدم طلبًا للمساعدة المتبادلة أو الاتصالات عن طريق وسائل سريعة للاتصال كالفاكس أو البريد الإلكترونى، وذلك لما تقدمه هذه الوسائل من شروط كافية للأمن والتوثيق (بما فى ذلك التشفير لو كان ضروريا)، مع التأكيد الرسمى اللاحق حينما يكون ذلك مطلوبًا بواسطة الدولة الموجه إليها الطلب، ويجب على الدولة المقدم إليها الطلب أن توافق وأن ترد على الطلب المقدم إليها عن طريق أية وسيلة من الوسائل العاجلة للاتصال.

٤-باستثناء ما يرد مخالفاً ذلك صراحة فى مواد هذا الفصل، فإن المساعدة المتبادلة تخضع للشروط المحددة عن طريق القانون الداخلى للطرف الموجه إليه الطلب أو عن طريق الاتفاقات المطبقة للمساعدة المتبادلة، بما فى ذلك الأسباب التى بناء عليها يمكن للطرف الموجه إليه الطلب أن يرفض التعاون. يجب على الطرف الموجه إليه الطلب ألا يمارس حقه فى رفض المساعدة القضائية المتبادلة بالنسبة للجرائم المنصوص عليها فى المواد من (٢ إلى ١١) من الاتفاقية، فقط إذا كان الباعث على تقديم الطلب يتصل بجريمة ذات طبيعة مالية.

٥-عندما يسمح وفقًا لبنود هذا الفصل للطرف المقدم إليه الطلب أن يُخضع المساعدة المتبادلة لوجود تجريم مزدوج (مشترك)، فإن هذا الشرط يعتبر مستوفياً إذا كان السلوك المكون للجريمة فى الطلب المقدم للطرف المطلوب منه المساعدة، يوصف بأنه جريمة جنائية فى قانونه الداخلى، سواء أكان القانون الداخلى قد صنفه فى نفس طائفة الجرائم أم لا، وسواء تم تجريمه بنفس المصطلح الذى نص عليه قانون الطرف الملتمس أم لا.

والالتزام بالمساعدة يجب أن يتوافر لأقصى حد ممكن، لذا فإن المساعدة المتبادلة يجب أن تكون – من حيث المبدأ – شاملة أو ممتدة كما يجب تقليل المعوقات إلى أقصى حد ممكن. كذلك فإن الالتزام بالتعاون المنصوص عليه فى المادة (٢٣) ينطبق كمبدأ عام على كل من الجرائم الجنائية المرتبطة بنظم وبيانات معلوماتية وعلى تجميع الأدلة الإلكترونية المرتبطة بجريمة جنائية. لقد أصبح فرض الالتزام بالتعاون بالنسبة لهذه الطبقة العريضة من الجرائم، لوجود مسوغ لتوافر آليات التعاون الدولى فى هذين النطاقين. ومع ذلك فإن المادتين (٣٤) و(٣٥) تسمحان للأطراف بتعديل نطاق تطبيق هذه الإجراءات.

كما تنص المادة السادسة والعشرون فقرة (١) من الاتفاقية على أنّه يمكن لأي طرف، في حدود قانونه الداخلى، ودون طلب مسبق، أن يرسل لأي طرف آخر، معلومات يكون قد حصل عليها في نطاق التحريات الخاصة به، إذا كان يرى أن هذه المعلومات يمكن أن تساعد الطرف المرسل إليه في استجلاء أو إجراء تحريات أو تحقيقات تتعلق بموضوع جرائم جنائية مقامة وفقا لهذه المعاهدة، أو عندما تكون هذه الجرائم تؤدى إلى طلب للمساعدة بواسطة هذا الطرف وفقاً لهذا الفصل.

والملاحظ أنّ المادة (٢٥) تنبثق من شروط نصت عليها اتفاقيات سابقة لمجلس أوروبا مثال ذلك المادة (١٠) من الاتفاقية المتعلقة بغسيل الأموال حيث أنه كثيرًا ما يحدث أن يكون طرف لديه معلومات هامة، ويعتقد هذا الطرف أن تقديم هذه المعلومات يمكن أن يحقق فائدة من أجل التنقيب والتحري أو الإجراءات المفتوحة، والتى لا يعلم بوجودها الطرف صاحب الشأن، في مثل هذه الحالات، لا يتم تقديم أية طلبات للمساعدة، ولذا تجيز الفقرة الأولى من المادة (٢٦) للدولة التي تحوز معلومة أن تقوم بالاتصال بالدولة الأخرى المعنية دون انتظار كتقديم طلب مسبق.

إنه من المفيد إدراج هذا الشرط، لأنه وفقاً للتشريع الداخلي لبعض الدول، إذ أن مثل هذا التأهيل الإيجابي يكون ضرورياً من أجل إمكانية الموافقة على المساعدة المتبادلة في غياب وجود طلب طرف لا يكون مطالباً بتقديم المعلومات للطرف الآخر بشكل تلقائي، إنما يملك حرية التصرف على ضوء الظروف الخاصة بالقضية محل البحث. علاوة على ذلك فإن الإفشاء التلقائي للمعلومات لا يمنع الطرف الذي يرسلها من القيام بالتنقيب والتحري أو البدء في إجراءات التحقيق في الوقائع التي تم الافصاح عنها. وتنص الفقرة الثانية من المادة(٢٦) على واقعة أنه في بعض الحالات، قد لا يقوم الطرف الذي لديه معلومات حساسة بإرسالها تلقائياً، إلا باشتراط أن تظل سرية، أو أن تستخدم وفقا لشروط معينة. وهكذا تصبح السرية في مثل تلك الحالات عاملاً هاماً في القضايا التي تكون فيها مصالح الدولة المانحة للمعلومات معرضة للخطر من جراء البوح بتلك المعلومات.

رابعًا: إنشاء شبكة طوارئ دائمة لتفعيل المساعدة المتبادلة:

سوف نتناول هنا مادة وحيدة من مواد الاتفاقية وهى المادة ٣٥ بخصوص إنشاء شبكة طوارئ دائمة لتفعيل المساعدة المتبادلة، والتى يطلق عليها الشبكة ٢٤/٧ بمعنى تلك الشبكة التى تعمل على مدار ٢٤ ساعة يومياً وبمعدل ٧ أيام فى الأسبوع بغرض التأكد من توفير المساعدة الفورية لإجراء التحقيقات المتعلقة بالجرائم الجنائية المرتبطة بنظم وبيانات معلوماتية أو لتجميع أدلة

ذات شكل إلكترونى لجريمة جنائية، وهذه المساعدة يجب أن تكون مشتملة على تسهيل، أو التطبيق العملى المباشر للإجراءات التالية (المرجع التقريرى، ص ١٨٥):

- تقديم المشورات التقنية.
- التحفظ على البيانات وفقاً للمادتين (٢٩-٣٠)
- تجميع أدلة وتقديم معلومات ذات طابع قانونى، وتحديد أماكن المشتبه فيهم.

وفضلاً عن ذلك فقد أوجبت المادة السابقة الآتى:

١-يجب أن تكون نقطة الاتصال الخاصة بطرف ما لديها القدرة على إجراء الاتصالات مع نقطة اتصال لطرف آخر على وجه السرعة.

٢-إذا كانت نقطة الاتصال المحددة بواسطة طرف ما لا تعتمد على سلطة أو سلطات هذا الطرف المسئولة عن المساعدة الدولية، أو تبادل تسليم المجرمين، فإنه يجب عليها أن تكون قادرة على التعاون مع هذه السلطة أو السلطات على وجه السرعة.

٣-يجب على كل طرف أن يكون لديه طاقم مدرب ومزود بالأجهزة التى تسهل عملية تشغيل الشبكة.

ويعتبر إنشاء هذه الشبكة من أهم الطرق المنصوص عليها فى هذه الاتفاقية، لأنها ليست فقط تضمن أفضل الوسائل الناجحة فى مواجهة مشكلات الإجرام المعلوماتى. بل أيضاً التغلب على التحديات الكبيرة التى يفرضها عصر المعلوماتية على السلطات المناط بها تنفيذ القانون.

وتستهدف نقطة الاتصال إما تسهيل الممارسة السريعة لوظائف الشبكة وإما التطبيق المباشر لعدد من التدابير من بينها توفير الإرشادات التقنية، التحفظ على البيانات تجميع الأدلة تحديد أماكن المشتبه فيهم.

الفرع الثاني
الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

وتعد هذه الاتفاقية من أهم الاتفاقيات العربية فى مجال مكافحة الجريمة التقنية بهدف منعها والتحقيق فيها وملاحقة مرتكبيها (بطيخ، ص ٢٢).

صدرت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات والموقعة فى القاهرة بتاريخ ٢١ ديسمبر ٢٠١٠، ووافقت مصر على الانضمام إليها بموجب قرار رئيس الجمهورية رقم ٢٧٦ لسنة ٢٠١٤ بتاريخ ١٩ أغسطس ٢٠١٤ والمنشور بالجريدة الرسمية بالعدد ٤٦ في ١٣ نوفمبر ٢٠١٤، ص ٦٥، وتهدف هذه الاتفاقية إلى تعزيز التعاون بين الدول العربية فى مجال مكافحة جرائم تقنية المعلومات لدرء أخطار هذه الجرائم حفاظاً على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها. كما أقرت الاتفاقية التزام كل دولة طرف بتجريم الأفعال الواردة فى المواد التى تضمنها الفصل الثانى من هذه الاتفاقية والمسمى بالتجريم (عبدالعظيم، ٢٠١٦، ص ١٦٦) .

مثل الاعتداء على سلامة البيانات، وجرائم إساءة استخدام وسائل تقنية المعلوماتية، والتزوير والاحتيال والإباحية والاعتداء على حرمة الحياة الخاصة، والجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات مثل نشر أفكار جماعات إرهابية والدعوة لها، وتمويل العمليات الإرهابية ونشر طرق صناعة المتفجرات، وأيضا ما يتعلق بالجريمة المنظمة مثل غسل الأموال والترويج للمخدرات والاتجار بالبشر والأعضاء البشرية والأسلحة(عبد الصادق، ٢٠١٨، ص ٥).

وتتكوّن الاتفاقية العربية من ثلاثٍ وأربعين مادة تمثَّلت فى إلزام الدول الأطراف بإدخال بعض التعديلات لتجريم جرائم تقنية المعلومات وهى أفعال الاختراق والاعتراض غير المشروع والاعتداء على سلامة البيانات والاعتداء على حُرْمَة الحياة الخاصة والاعتداء على الملكية الفكرية وإساءة استخدام وسائل تقنية المعلومات والتزوير والاحتيال والجرائم المتعلِّقة بالإرهاب وغسل الأموال والمخدرات والاتجار فى الجنس البشرى والأعضاء البشرية والأسلحة والمساس بالقِيَم الدينية أو النظام العام والتهديد والابتزاز والاتجار فى الآثار والتحَف الفنية والاستخدام غير المشروع لأدوات الائتمان والوثائق الإلكترونية (القاضى، ٢٠١١، ص ٥٠ وص٧٠) .

وقد جاء الفصلان الثالث والرابع من الاتفاقية العربية بتوضيح نطاق تطبيق الأحكام الإجرائية والتعاون القانونى والقضائى المتصلة بتسليم المجرمين والمساعدة المتبادلة بين الدول والمساعدة ذات الصلة أيضًا بسلطات التحقيق، والتأكيد على ضرورة أن تلتزم كل دولة طرف بأن تتبنى فى قانونها الداخلى التشريعات والإجراءات الداخلية لمواجهة الجرائم المعلوماتية.

وقد شهدت الاتفاقية انعكاسًا على الجانب التشريعى العربى فهناك العديد من الدول العربية التى واكبت هذا التطور التقنى الحاصل فى مجال تكنولوجيا المعلومات وعملت على محاولة التصدى لمكافحة الجرائم الإلكترونية الناشئة عنه بإصدارها عدداً من التشريعات الخاصة والتى قامت بالاستناد والبناء على ما ورد بالاتفاقية المذكورة.

المبحث الثاني
الجهود المصرية فى مجال الأمن السيبراني

شهدت مصر حراكًا قويًا فى مجال أمن المعلومات والشبكات، وذلك تزامنًا مع الاهتمام الدولى المتزايد بشأن أمن المعلومات، فى ظل ما تشهده بعض دول المنطقة من اختراقات أمنية للبنية التحتية والشبكات والمعلومات نتيجة التطورات التكنولوجية المتسارعة.

حيث سعت مصر نحو بناء وتأسيس منظومة حديثة قادرة على حماية الفضاء السيبرانى المصرى (حكاية وطن: ٢٠٢٣، ص ٢٧٦،٢٧٥، ٢٧٧)..

فقد تم إنشاء المجلس الأعلى للأمن السيبرانى، كما قامت بإنشاء المركز المصرى للاستجابة لطوارئ الحاسب الآلى «سيرت»، كما تم إنشاء مركز الاستجابة لطوارئ الحاسب الآلى للقطاع المالى والتابع للبنك المركزى، ثم أصدرت الاستراتيجية الوطنية للأمن السيبرانى ٢٠١٧-٢٠٢١، وأعقبها صدور الاستراتيجية الوطنية للأمن السيبرانى ٢٠٢٣-٢٠٢٧ وهو ما سنتناوله فى الفقرات المقبلة.

سوف نتناول الجهود المصرية فى مجال الأمن السيبرانى فى خمسة مطالب وذلك على النحو التالى:
المطلب الأول: المجلس الأعلى للأمن السيبراني
المطلب الثانى: المركز المصرى للاستجابة لطوارئ الحاسب الآلى «سيرت»
المطلب الثالث: مركز الاستجابة لطوارئ الحاسب الآلى للقطاع المالي والمصرفى التابع للبنك المركزي
المطلب الرابع: الاستراتيجية الوطنية للأمن السيبرانى لجمهورية مصر العربية. ٢٠١٧-٢٠٢١.
المطلب الخامس: الاستراتيجية الوطنية للأمن السيبرانى لجمهورية مصر العربية ٢٠٢٣-٢٠٢٧
المطلب السادس: نتائج الجهود المصرية فى مجال الأمن السيبراني

المطلب الأول
المجلس الأعلى للأمن السيبراني

تم تشكيل المجلس الأعلى للأمن السيبرانى فى مصر، بقرار رئيس الوزراء رقم ٢٢٥٩ في ديسمبر ٢٠١٤، والمعدل بالقرار رقم ١٤٤٧ لسنة ٢٠١٥، ويهدف إلى حماية المعلومات والبيانات لدى الجهات مع الاهتمام بإدارات المعلومات والاتصالات فى الوزارات والجهات المختلفة، والتأكد من توافر التمويل اللازم لضمان تنفيذ منظومة الأمن السيبرانى، مع ضرورة وضوح الإطار التشريعى الخاص به(٧).

ويضم تشكيل المجلس وزير الاتصالات وتكنولوجيا المعلومات رئيسا للمجلس، وعضوية ممثلين عن وزارات: الدفاع، والخارجية، والداخلية، والبترول والثروة المعدنية، والكهرباء، والصحة، والموارد المائية والرى، والتموين، والاتصالات، وهيئة الرقابة الإدارية، وجهاز المخابرات العامة، والبنك المركزى، وثلاثة أعضاء من ذوى الخبرة، ثم صدر قرار رئيس مجلس الوزراء رقم ١٦٣٠ لسنة ٢٠١٦ والذى حدد اختصاصات المجلس ومهامه ومواعيد عمله، كما حدد قرار رئيس مجلس الوزراء رقم ٩٩٤ لسنة ٢٠١٧ تولى وزير الاتصالات وضع وتحديد قواعد الحماية ومتابعة المجلس فى تنفيذ قراراته.

ويختص المجلس الأعلى للأمن السيبرانى بوضع استراتيجية وطنية لمواجهة الأخطار والهجمات السيبرانية والإشراف على تنفيذها و تحديثها بالإضافة إلى المهام التالية:

- اعتماد تحديد البنى التحتية للاتصالات والمعلومات الحرجة فى كافه قطاعات الدولة ووضع أطر تقييم و متابعة تأمين لها فى القطاعات المختلفة.
- اعتماد أطر واستراتيجيات و سياسات تأمين البنى التحتية للاتصالات والمعلومات الحرجة لكافة قطاعات الدولة.
- وضع خطط وبرامج تنمية صناعة الأمن السيبرانى وإعداد الكوادر اللازمة لمواجهة التحديات والمخاطر السيبرانية ووضع إطار للبحث العلمى والتطوير فى مجال الأمن السيبرانى.

(7)- www.escc.gov.eg

- التعاون والتنسيق إقليمياً ودولياً مع الجهات ذات الصلة فى مجال الأمن السيبرانى وتأمين البنى التحتية الحرجة للاتصالات والمعلومات وإعداد توصيات بأية تدخلات تشريعية لازمة للتأمين.
- وضع المعايير الملزمة لكافة الجهات كحد أدنى لتأمين البنى التحتية الحرجة للاتصالات والمعلومات وإلزامها بإعداد خطط الطوارئ.
- وضع آليات رصد المخاطر والمتابعة الدورية للهجمات السيبرانية وتوزيع الأدوار على المستوى الوطنى.
- وضع وتفعيل معايير وآليات لتحديد اعتمادات البنية الموجودة بين عناصر البنية الأساسية الحرجة و القائمين عليها وما يقع خارجها بحيث يتم تجنب التأثيرات المتتالية.
- إقرار مواصفات الأمن السيبرانى القياسية للأنظمة فى مختلف القطاعات وإضافة معايير الجودة السيبرانية.
- اعتماد توصيف التقويم الأمنى للقائمين على تشغيل البنى التحتية الحرجة للاتصالات والمعلومات.
- وضع آلية لمتابعة تأمين وحماية المواقع الحكومية الرسمية على الإنترنت.

يهدف المجلس الأعلى للأمن السيبراني إلى تعزيز الأمن السيبراني في مصر وحماية البنى التحتية الحيوية الحكومية والخاصة من الهجمات السيبرانية المحتملة وقد اتخذ المجلس العديد من القرارات المنظمة لتحقيق هذا الهدف.

أ- إنشاء مركز للرصد والتحليل والاستجابة للحوادث السيبرانية، وتطوير القدرات الوطنية للأمن السيبراني، وتعزيز التعاون الدولي في هذا المجال

ب- إصدار الاستراتيجية الاولي الوطنية للأمن السيبراني ٢٠١٧-٢٠٢١ والتي تناولت المخاطر والتحديات السيبرانية ثم أهم القطاعات الحيوية المستهدفة والعناصر الأساسية لخطورة التهديدات ثم الهدف الاستراتيجي وركائز التوجه الاستراتيجي لمواجهة الاخطار وآلية التنفيذ

ج-إصدار الاستراتيجية الوطنية للأمن السيبراني ٢٠٢٣ – ٢٠٢٧ وتهدف هذه الاستراتيجية لتوفير البيئة الآمنة لمختلف القطاعات لتوحيد الرؤى الوطنية سعياً إلى تحقيق فضاء إلكترونى مصرى مؤمن وقادر على الصمود أمام التهديدات والهجمات السيبرانية وتعزيز النمو والازدهار الاقتصادى.

د- عمل ورعاية العديد من المؤتمرات الخاصة بمجال الأمن السيبراني والأمن المعلوماتي لاستحداث آلية فعالة لمواجهة التهديدات، آخرهم مؤتمر أمن المعلومات والأمن السيبرانى (Caisec24) في النسخة الثالثة منه .

المطلب الثاني
المركز المصرى للاستجابة لطوارئ الحاسب الآلى (سيرت)

تبنت وزارة الاتصالات وتكنولوجيا المعلومات الدعوة لتشكيل مجلس أعلى لحماية البنى التحتية للاتصالات وتكنولوجيا المعلومات، ويعمل به فريق من ستة عشر متخصصاً، ويقدم الفريق الدعم الفنى على مدار ٢٤ ساعة لحماية البنية التحتية الحيوية للمعلومات، يقدم المركز منذ عام ٢٠١٢ الدعم لمختلف الجهات عبر قطاعات تكنولوجيا المعلومات والاتصالات، والخدمات المصرفية والحكومية من أجل مساعدتهم على مواجهة تهديدات الأمن السيبرانى بما فى ذلك هجمات الحرمان من الخدمة.

وتتمحور مهمة المركز المصرى للاستجابة لطوارئ الإنترنت والحاسب حول توفير نظام للإنذار المبكر ضد البرمجيات الخبيثة والهجمات الإلكترونية التى تنتشر بنطاق واسع ضد البنية التحتية الحيوية للمعلومات المصرية، ويعمل المركز حالياً على التوسع فى تطوير مختبراته فى الإدارات التشغيلية الرئيسية الأربع، ويجرى التخطيط لمختبرات إضافية للأمن السيبرانى فى مجال الهاتف المحمول والأمن السيبرانى فى أنظمة التحكم الصناعية.

ومن أهداف المركز أيضًا وضع إطار تشريعى ملائم للأمن السيبرانى، ووضع إطار تنظيمى مناسب لإنشاء نظام وطنى للأمن السيبرانى ومراكز استجابة للطوارئ، وتأسيس البنية التحتية اللازمة لضمان الثقة فى المعاملات الإلكترونية وحماية الهوية الرقمية، مثل البنية التحتية للمفاتيح العامة ومكاتب الائتمان بمشاركة القطاع الخاص، وجمع المعلومات حول الحوادث الأمنية وتحليلها، والتنسيق والوساطة بين كافة الأطراف لحل مثل تلك الحوادث.

ويتكون المركز من خمس إدارات وهى التعامل مع الحوادث السيبرانية واستمرارية الأعمال، ومراقبة الهجمات الإلكترونية والإنذار المبكر، وفحص الثغرات واختبارات الاختراق بالإضافة إلى إدارة حماية البنية المعلوماتية الحرجة وخطط الطوارئ وإدارة التوعية السيبرانية وتطوير الأعمال.

تهتم إدارة حماية البنية المعلوماتية الحرجة وخطط الطوارئ بحماية المعلومات فى القطاعات الحرجة فى الدولة، ولذلك تقوم الإدارة بدراسة احتياجات قطاعات معينة ومستويات تطبيق معايير وإجراءات الأمن السيبرانى فيها.

وتختص إدارة التوعية السيبرانية ببناء وتعزيز الثقافة والوعى بالأمن السيبرانى وأمن المعلومات والتعرف أكثر على مخاطر الإنترنت والتهديدات والهجمات الإلكترونية. وتستهدف هذه الإدارة توعية كل من الوزارات والمؤسسات الحكومية ذات البنية التحتية الحرجة وتقوم حملات التوعية من خلال دورات توعية، دورات تدريبية وورش عمل، نشرات دورية، كتيبات إرشادية، مقاطع فيديو توعوية، والمشاركة بفعاليات ومناسبات المدارس والجامعات[٨].

(8)-https://egcert.eg/ar

المطلب الثالث

مركز الاستجابة لطوارئ الحاسب الآلى للقطاع المالى والمصرفى التابع للبنك المركزى

يختص مركز الاستجابة لطوارئ الحاسب الآلى للقطاع المالى بالتعامل مع الحوادث السيبرانية وطوارئ الإنترنت داخل القطاع المالى والمصرفى، وذلك من خلال التنبؤ المبكّر بالحوادث الأمنية ومواجهتها والتخفيف من آثارها ومنع تكرار حدوثها، بالاعتماد على منظومة تقنية غير تقليدية للمراقبة والرصد الأمنى، فضلاً عن تحليل الأدلة الرقمية والثغرات الأمنية الخاصة بالجرائم السيبرانية على مستوى القطاع المالى، للوقوف على أسبابها ومنع تكرار حدوثها فى المستقبل، وذلك بالإضافة إلى التعامل مع البرمجيات الخبيثة وإجراء الهندسة العكسية.

وتتلخص مهام واستراتيجية مركز الاستجابة لطوارئ الحاسب الآلى للقطاع المالى والمصرفى فى الآتى:

١-تأمين الاستجابة لطوارئ أمن تكنولوجيا المعلومات والاتصالات تشكل دعمًا للهيئات الحكومية، البنى التحتية الوطنية الحساسة والجمهور العام فى البلد عبر مبادرات معترف بها قانونًا، موثوقة ومرخص لها ومنسقة مركزياً على المستوى الوطنى.

٢-تحفيز الأمن والحماية عبر نشر المعلومات المهمة مثل الإنذارات المبكرة والتنبيهات والاستشارات الأمنية ودعم أفضل الممارسات الأمنية.

٣-دعم والحفاظ على هذه المبادرات مما يتطلب اعتماد تكنولوجيات وتقنيات متطورة، تأسيس مناهج والبحث فى تحليل التهديدات والتخفيف منها.

هذا وتعمل استراتيجية مركز الاستجابة لطوارئ الحاسب الآلى للقطاع المالي والمصرفى التابع للبنك المركزى وفق أولوية حماية تكنولوجيا الاتصالات والمعلومات فى الوطن وذلك عبر:

١- اعتماد جميع المبادرات الضرورية للمركز المصرى للاستجابة لحوادث الحاسب الآلى «سيرت» .

٢-تأمين المعلومات الحساسة عبر التعاون الإقليمى مع الشراكة الدولية متعددة الأطراف ضد التهديدات السيبرانية والمراكز الإقليمية للاستجابة لحوادث الحاسب الآلى والتعاون الدولى عبر الشراكة الدولية متعددة الأطراف ضد التهديدات السيبرانية.

٣-جمع المعلومات حول التهديدات ذات المصدر الدولى والعالمى الاستخباراتى عبر منشآته التكنولوجية الخاصة.

٤-التنسيق مع الاتحاد الدولى ومع مراكز الاستجابة لطوارئ الحاسب الآلى المرخص لها فى الدول الأخرى وأية هيئات أخرى تعنى بأمن تكنولوجيا الاتصالات والمعلومات.

وقد نجح مركز الاستجابة لطوارئ الحاسب الآلى للقطاع المالى بالبنك المركزى المصرى، فى الحصول على اعتماد وعضوية المنتدى العالمى لفرق الاستجابة والحوادث الأمنية (FIRST)، بعد استيفاء وتلبية جميع المتطلبات التقنية والتنظيمية فى فترة زمنية وجيزة، ليصبح أول مركز قطاعى من نوعه معترف به دوليًا فى جمهورية مصر العربية.

يأتى ذلك فى ضوء استراتيجية البنك المركزى لبناء إطار متكامل لتعزيز الأمن السيبرانى

بالقطاع المالى والمصرفى، وتتويجًا لجهود مركز الاستجابة لطوارئ الحاسب الآلى (خلال الأربع سنوات الماضية)، وحرصه على اتباع المعايير والمواصفات الأمنية الدولية والامتثال لها، وكذا التأكد من تطبيقها، مما ساعد على نحو كبير فى سرعة اجتياز جميع عمليات المراجعة والتدقيق المنفذة من قبل المختصين بمنظمة (FIRST) الدولية على مدار الأربعة أشهر الماضية.

ويتيح الاعتماد والانضمام لمنتدى (FIRST)، الذى يهدف إلى تعزيز التعاون والتنسيق فى منع والحد من حوادث الأمن السيبرانى والاستجابة السريعة لها وتعزيز تبادل المعلومات بين الأعضاء والمجتمع ككل، التعامل والاستجابة بشكل أكثر فاعلية للحوادث السيبرانية، ويساهم فى تعظيم وتطوير القدرات الفنية والتقنية لمراكز وفرق الاستجابة للأعضاء من خلال اطلاعهم على أحدث الممارسات المتبعة عالميًا فى هذا المجال، فضلاً عن إتاحة التبادل اللحظى للمعلومات الأمنية للحوادث السيبرانية بينهم، بما يعزز من قدرتهم على التعامل والحد من الهجمات والتهديدات الأمنية وتحفيز الاستجابة السريعة والإجراءات والتدابير الاستباقية.

ويساعد هذا المنتدى أيضًا على تيسير التعاون والشراكات الاستراتيجية بين الدول والمؤسسات العالمية وتعزيز التواصل بين فرق الاستجابة للحوادث من مختلف دول العالم فى ضوء تبادل الخبرات التكنولوجية والاستخبارات الأمنية، كما يتيح للأعضاء حضور ندوات متخصصة تجمع خبراء الأمن السيبرانى، وكذلك الدورات التدريبية والمحاضرات العملية والتطبيقية إلى جانب المشاركة فى المؤتمر السنوى العالمى للاستجابة لحوادث الأمن السيبرانى، بالإضافة إلى أنه يوفر إمكانية الاطلاع على أحدث المناهج والمنشورات الخاصة بالأمن السيبرانى وخدمات الويب، مع إتاحة الدخول على المنتديات وحلقات النقاش الإلكترونية بين الأعضاء.

ويتسق كل ما سبق، مع استراتيجية البنك المركزى المصرى التى تهدف إلى تعزيز مشاركة مركز الاستجابة لطوارئ الحاسب الآلى للقطاع المالى فى تنفيذ الاستراتيجية الوطنية للأمن السيبرانى بكفاءة وفعالية، إلى جانب تعزيز قدرة المؤسسات والجهات بالدولة على الاستجابة السريعة والتعاون والتنسيق فى منع الحوادث السيبرانية.

المطلب الرابع

الاستراتيجية الوطنية للأمن السيبرانى لجمهورية مصر العربية ٢٠١٧-٢٠٢١

اهتمت مصر بمجال الأمن السيبرانى فى وقت مبكر كما سعت للريادة وتصدر المشهد العربى والإفريقى فى المؤشرات الدولية، وكانت فى مقدمة الدول التى تسعى لاستمرارية التحسين وخلق تجربة رائدة فى الشرق الأوسط.

وفى ضوء حوكمة الأمن السيبرانى على الصعيد الوطنى قامت مصر بإصدار الاستراتيجية الوطنية للأمن السيبرانى ٢٠١٧ – ٢٠٢١ التزامًا بالاتجاهات العالمية الحديثة والتزامًا بالاستحقاقات الواردة بالدستور المصرى الصادر فى ٢٠١٤ فى المادة ٣١ من الدستور والتى تنص على أنّ أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومى، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه، على النحو الذى ينظمه القانون.

محاور الاستراتيجية الوطنية للأمن السيبرانى

١- هدف الاستراتيجية

تهدف الاستراتيجية الوطنية للأمن السيبرانى فى مصر إلى مواجهة المخاطر السيبرانية وتعزيز الثقة في البنية التحتية للاتصالات والمعلومات وتطبيقاتها وخدماتها فى شتى القطاعات الحيوية، وتأمينها من أجل تحقيق بيئة رقمية آمنة وموثوقة للمجتمع المصرى بمختلف أطيافه، والأساس حسبما يظهر من هذا الهدف هو رصد ومواجهة المخاطر، تعزيز الثقة والأمان فى القطاعات الحيوية وتعاملاتها، بيئة رقمية آمنة وموثوقة.

٢-القطاعات الحيوية المستهدفة

حددت الاستراتيجية عددًا من القطاعات المستهدفة والتى تعد أولى بالحماية ورفع الكفاءة والجاهزية لها وتحسينها وهى:

أ- قطاعات الاتصالات وتكنولوجيا المعلومات وتتضمن شبكات الاتصالات السلكية واللاسلكية، والكوابل البحرية والأرضية، وأبراج الاتصالات، والأقمار الصناعية للاتصالات، ومقدمى خدمات الاتصالات والإنترنت.

ب- قطاع الخدمات المالية ويتضمن شبكات ومواقع البنوك وتقديم المعاملات المصرفية، الدفع الإلكترونى، والبورصة، وشركات تداول الأوراق المالية، وشبكات الخدمات المالية البريدية.

ج- قطاع الطاقة ويتضمن نظم وشبكات ومحطات التحكم فى إنتاج وتوزيع الكهرباء والبترول والغاز، ومحطات السد العالى، ومحطات الطاقة النووية، وغيرها.

د- قطاع النقل والمواصلات النقل البرى والبحرى والجوى والنيلى، ويضم كافة نظم ومراكز وشبكات التحكم فى القطارات والمترو، وشبكات المرور، ونظم التحكم فى الملاحة الجوية والبحرية.

هـ- قطاع الصحة وخدمات الإسعاف العاجل شبكات الإغاثة والإسعاف، وبنوك الدم، ونظم وشبكات المستشفيات، وشبكات ومواقع تقديم الرعاية الصحية.

و- قطاع الخدمات الحكومية بوابة ومواقع الحكومة الإلكترونية، ومواقع الجهات والمؤسسات الحكومية، وقواعد البيانات والمعلومات القومية، وأهمها قاعدة بيانات الرقم القومى والشبكات والمواقع المتصلة بها.

٣- آليات مواجهة المخاطر

أ- الدعم السياسى والمؤسسى الاستراتيجى والتنفيذى: ويشمل ذلك الوعى بخطورة التهديدات السيبرانية وضرورة التعامل معها كأولوية وبأعلى قدر من الجدية، مع الاهتمام بالاستعداد المسبق بما يشمل الخطط الاستراتيجية والتنفيذية وخطط الطوارئ وآليات التنسيق العرضى وإعداد الكوادر والتجهيزات التقنية واللوجستية.

ب-الإطار التشريعى: وضع الإطار التشريعى الملائم لأمن الفضاء السيبرانى ومكافحة الجرائم السيبرانية وحماية الخصوصية وحماية الهوية الرقمية وأمن المعلومات، وذلك

بمشاركة من الأطراف المعنيين، وذوى الخبرة فى القطاع الخاص ومؤسسات المجتمع المدنى، مع الاسترشاد بالخبرات والتجارب والبرامج الدولية ذات الصلة، مع إعداد وتدريب المتخصصين فى إنفاذ القانون فى الجهات القضائية والشرطية.

ج-وضع إطار تنظيمى لحماية أمن الفضاء السيبرانى وإنشاء منظومة وطنية لتأمين البنية التحتية للاتصالات وتكنولوجيا المعلومات ونظم وقواعد البيانات والمعلومات القومية وبوابات الخدمات الحكومية والمواقع الحكومية على الإنترنت.

د- إعداد وتفعيل فرق الاستعداد والاستجابة لطوارئ الحواسيب والشبكات فى القطاعات الحيوية على المستوى الوطنى، حيث تتولى هذه الفرق مسئولية المتابعة الأمنية لشبكات الاتصالات والمعلومات الوطنية والحواسيب المتصلة بها، والتعامل مع أى أخطار سيبرانية تهددها أو هجمات سيبرانية توجه إليها، بالإضافة إلى التوعية والإعداد لمواجهة هذه الأخطار.

هـ- تشجيع ودعم وتنمية البحث العلمى والتطوير ودعم التعاون بين الجهات البحثية والشركات الوطنية فى مجالات مثل تحليل البرمجيات الخبيثة المتقدمة، وتحليل الأدلة الرقمية، وحماية وتأمين نظم التحكم الصناعية، وتطوير أجهزة وأنظمة تأمين النظم والشبكات، والتشفير والتوقيع الإلكترونى، وحماية البنية التحتية للاتصالات وتكنولوجيا المعلومات، وحماية الحواسيب السحابية وقواعد البيانات الكبيرة، وتقنيات الذكاء الاصطناعى وإنترنت الأشياء.

و- تنمية الكوادر البشرية والخبرات اللازمة لتفعيل منظومة الأمن السيبرانى فى مختلف القطاعات، بالتعاون والشراكة مع القطاع الخاص والجامعات ومؤسسات المجتمع المدنى.

ز- التعاون الدولى: مع الدول الصديقة والمنظمات الدولية والإقليمية ذات الصلة، وتبادل الخبرات وتنسيق المواقف فى مجال أمن الفضاء السيبرانى ومكافحة الجرائم السيبرانية، حيث تعتبر هذه الجرائم غير محدودة بالحدود الجغرافية أو السياسية.

ح-وضع وتنفيذ خطط وحملات للتوعية المجتمعية بأهمية أمن الفضاء السيبرانى وحماية الخدمات الإلكترونية للأفراد والمؤسسات من المخاطر والتحديات التى قد تواجهها، بالإضافة إلى حماية الخصوصية وإطلاق برامج حماية الأطفال والشباب على الإنترنت.

٤-أهم برامج الاستراتيجية فى مرحلة ٢٠١٧- ٢٠٢١

أ- برنامج لتطوير الإطار التشريعى المناسب لأمن الفضاء السيبرانى، ومكافحة الجرائم السيبرانية، وحماية الخصوصية والهوية الرقمية، بمشاركة من الأطراف المعنيين، وذوى الخبرة فى القطاع الحكومى والخاص والأكاديمى ومؤسسات المجتمع المدنى، حيث تم إصدار قانون مكافحة جرائم تقنية المعلومات ١٧٥ لسنة ٢٠١٨، وقانون حماية البيانات الشخصية ١٥١ لسنة ٢٠٢٠م وفى انتظار اكتمال المنظومة التشريعية.

ب-برنامج لتطوير منظومة وطنية متكاملة لحماية أمن الفضاء السيبرانى وتأمين البنية التحتية للاتصالات وتقنية المعلومات، وذلك بإعداد وتفعيل ما يعرف بفرق الاستجابة

للطوارئ فى القطاعات الحيوية على المستوى الوطنى (مصر والأمن السيبراني» صادر عن الهيئة العامة للاستعلامات).

ج- برنامج لحماية الهوية الرقمية وتفعيل برنامج المواطنة الرقمية وتفعيل البنى التحتية اللازمة لدعم الثقة فى التعاملات الإلكترونية بوجه عام وفى الخدمات الحكومية الإلكترونية خصوصًا وتفعيل التوقيع الإلكترونى.

د- برنامج للتوعية المجتمعية بالفرص والمزايا التى تقدمها الخدمات الإلكترونية للأفراد والمؤسسات والجهات الحكومية، وبأهمية الأمن السيبرانى لحماية تلك الخدمات من المخاطر والتحديات التى قد تواجهها، على أن تشمل حملات توعية سنوية موسعة على مستوى الجمهورية والمؤتمرات والندوات وورش العمل النوعية فى مختلف القطاعات.

هـ- برنامج لدعم البحث العلمى وتنمية صناعة الأمن السيبرانى من خلال دعم برامج ومشروعات التعاون بين الجهات البحثية والشركات الوطنية؛ وخاصة فى مجال تحليل البرمجيات الخبيثة المتقدمة ومجال تحليل الأدلة الرقمية، وفى مجال حماية وتأمين نظم التحكم الصناعية، ومجال تطوير أجهزة وأنظمة تأمين النظم والشبكات، ومجال التشفير والتوقيع الإلكترونى، ومجال حماية البنى التحتية للاتصالات وتكنولوجيا المعلومات، ومجال تأمين الحواسب السحابية وحماية قواعد البيانات الكبرى ومجال تقنيات الذكاء الاصطناعى وإنترنت الأشياء.

و- برنامج إعداد الكوادر البشرية والخبرات اللازمة لتفعيل منظومة الأمن السيبرانى فى مختلف القطاعات يجرى بالتعاون والشراكة بين الجهات الحكومية والقطاع الخاص والجامعات (على، ٢٠٢٠، ص ١٦٨).

المطلب الخامس

الاستراتيجية الوطنية للأمن السيبرانى لجمهورية مصر العربية ٢٠٢٣-٢٠٢٧

خلال الأسبوع الأول من شهر فبراير من عام ٢٠٢٤ أعلن المجلس الأعلى للأمن السيبرانى عن إطلاق الاستراتيجية الوطنية للأمن السيبرانى للأعوام ٢٠٢٣-٢٠٢٧، وتهدف هذه الاستراتيجية لتوفير البيئة الآمنة لمختلف القطاعات وتوحيد الرؤى الوطنية سعيًا إلى تحقيق فضاء إلكترونى مصرى مؤمن وقادر على الصمود أمام التهديدات والهجمات السيبرانية، وتعزيز النمو والازدهار الاقتصادى.

وتعد هذه الاستراتيجية بمثابة خارطة طريق شاملة تتضمن مشاريع قومية تهدف إلى وضع أطر عمل وضوابط للتصدى للحوادث والتهديدات السيبرانية المتزايدة، وكذلك خلق فرص سانحة فى السوق المصرية من خلال بناء كوادر بشرية مؤهلة، وإقامة صناعة وطنية فعالة ومؤثرة تسهم فى زيادة الناتج المحلى الإجمالى للدولة المصرية، وأخيرًا بناء ثقافة الأمن السيبرانى لتوعية جميع فئات المجتمع، مما يُقلّل من مخاطر الجرائم الإلكترونية.

وتشمل الاستراتيجية ستة مجالات رئيسية هى:

١- بناء إطار تشريعى متكامل.
٢- تغيير ثقافة المجتمع حول الأمن السيبرانى.
٣- تعزيز الشراكات الوطنية.
٤- بناء منظومة دفاعات سيبرانية قوية وقادرة على الصمود.
٥- تشجيع البحث العلمى وتعزيز الابتكار والنمو.
٦- تعزيز التعاون الدولى.

وقد جاءت الاستراتيجية مقسمة إلى تسعة أجزاء، نبرز فيما يلى أهم ما جاء بكل جزء منها:

أولاً: الأمن السيبرانى فى مصر:

يتناول هذا الجزء مدخلاً للاستراتيجية من حيث بيان أهميتها وبيان ما تم استخلاصه من تحليل نقاط القوة والضعف والفرص والتهديدات والمخاطر SWOT، ثم بيان ماهية المصادر التى تم الاستناد إليها لإعداد الاستراتيجية مثل الخبراء والأكاديميين المعنيين، وكذلك أفضل الممارسات العالمية وفقًا لتجارب الدول الرائدة فى مجال الأمن السيبرانى.

ثانيًا: أسس ومحاور الاستراتيجية:

يتناول هذا الجزء الرؤية والرسالة والسند التشريعى الدستورى للاستراتيجية، بالإضافة إلى بيان برامج ومحاور الاستراتيجية والمتمثلة فى بناء إطار تشريعى متكامل وتغيير ثقافة المجتمع حول الأمن السيبرانى، وتعزيز الشراكة الوطنية وبناء دفاعات سيبرانية قادرة على الصمود، وتشجيع البحث العلمى وتعزيز الابتكار، وتعزيز التعاون الدولى.

ثالثًا: بناء إطار تشريعى متكامل:

يتناول هذا الجزء استعراض الهيكل التشريعى الحالى، حيث يستهدف المشرع العمل على محورين أساسيين ومتوازيين؛ ويتمثل الأول فى تجريم الفعل ومرتكب الفعل (الجانى) وقد تم ذلك من خلال قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨، ويتمثل المحور الثانى فى فرض الضوابط والمعايير القياسية وقد تم ذلك بشكل جزئى من خلال إصدار قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠ ولائحته التنفيذية ويتبقى إصدار قانون الأمن السيبرانى الجارى العمل عليه والمتوقع إصداره قريبًا.

رابعًا: تعزيز الشراكة الوطنية:

يتناول هذا الجزء جهود حوكمة منظومة الأمن السيبرانى فى جمهورية مصر العربية من خلال تنسيق التعاون بين الجهات الحكومية والشركات الخاصة العاملة فى مجال الأمن السيبرانى والمؤسسات التعليمية، وذلك بالتزامن مع إنشاء قاعدة مركزية لبيانات سوق الأمن السيبرانى لتيسير تبادل المعلومات والخبرات فى مجال الأمن السيبرانى لدعم منظومة اتخاذ القرارات لدى الأطراف المتعددة، بالإضافة إلى تنظيم اتفاقيات التعاون الثنائى مع ملاك ومشغلى وحدات البنية التحتية الحرجة لضمان تحقيق أعلى مستويات الأمن السيبرانى للبنية التحتية المعلوماتية

الحرجة، وأخيرًا ينظم هذا الجزء عملية استحداث صندوق تطوير صناعة الأمن السيبرانى من أجل ضمان استمرارية تدفق التمويل اللازم لاستمرارية مشروعات الأمن السيبرانى.

خامسًا: بناء دفاعات سيبرانية قوية وقادرة على الصمود:

يتناول هذا الجزء خمسة أنواع من البرامج التى تستهدف قطاعات مختلفة، فهناك برامج تهدف إلى التكامل مع المشروعات القومية، وأخرى موجهة إلى البنية التحتية الحرجة، وأخرى تستهدف وحدات ومؤسسات القطاع الخاص، وأخرى تستهدف وضع المعايير والسياسات الأمنية والتنظيمية، وأخيرًا برامج تستهدف رفع مستوى الخدمة.

سادسًا: تعزيز التعاون الدولى:

للتعاون الدولى فى مجال الأمن السيبرانى أهمية بالغة، حيث إن الجريمة السيبرانية هى جريمة عابرة للحدود الجغرافية وتستلزم تكاتف الدول والمنظمات للتصدى لها، ويندرج تحت تعزيز التعاون الدولى تطوير استراتيجية الدولة المصرية للتعاون الدولى فى مجال الأمن السيبرانى ثم إرساء مبادئ واتجاهات الدبلوماسية السيبرانية المصرية، مع التركيز على محاور الريادة والابتكار وضمان منع واكتشاف والتصدى للتهديدات السيبرانية حال وقوعها ومقاضاة مرتكبيها.

سابعًا: تغيير ثقافة المجتمع فيما يخص الأمن السيبرانى:

يتناول هذا الجزء مختلف جهود تغيير ثقافة المجتمع فيما يخص الأمن السيبرانى، ولهذا أهمية بالغة إذ إن هناك قطاعات واسعة لا يتوافر لها العلم بأبسط مبادئ وأساسيات الأمن السيبرانى وهو ما يؤدى لوقوعهم فى حبال الهجمات السيبرانية، ولأغراض تغيير ثقافة المجتمع فمن المزمع القيام بعدة أنشطة تستهدف مختلف الفئات من خلال إنشاء منصة للتوعية بالأمن السيبرانى بطريقة مبسطة من خلال وسائل التواصل السمعى والبصرى، وكذلك استهداف الأطفال من خلال ابتكار ألعاب توعوية تساهم فى توصيل المعلومات المطلوب توصيلها بطريقة مبسطة ومحببة للطفل، وكذلك استهداف طلاب المدارس بمختلف درجاتهم من خلال إدراج مناهج تعليمية تتعلق بالأمن السيبرانى وكذلك حملات توعوية داخل المدارس، وكذلك القيام بحملات توعوية عامة لاستهداف مختلف فئات المجتمع، وأخيرًا برامج تدريبية متخصصة لإعداد كوادر مهنية قادرة على المنافسة فى مجال الأمن السيبرانى.

ثامنًا: تشجيع البحث العلمى وتعزيز الابتكار والنمو:

يتناول هذا الجزء جهود تشجيع البحث العلمى وتعزيز الابتكار والنمو، وهى جهود أساسية لا غنى عنها نظرًا للتطور المستمر فى التقنيات والوسائل والأساليب المستخدمة فى الهجمات السيبرانية ومن ثم ضرورة مواكبة ذلك بتطوير التقنيات الدفاعية وكذلك باستحداث التقنيات اللازمة لتعزيز تأمين الفضاء الإلكترونى، وتشمل الجهود فى مجال تشجيع البحث العلمى دعم حاضنات المشروعات الصغيرة وتشجيع الاستثمار بنوعيه المحلى والأجنبى لزيادة عدد مقدمى الخدمات فى مجال الأمن السيبرانى وتعزيز توفير الكوادر المؤهلة لتقديم خدمات الأمن السيبرانى وهو ما يؤدى بدوره إلى زيادة عدد الخدمات فى مجال الأمن السيبرانى، وأخيرًا تعزيز التعاون مع الجامعات والمراكز البحثية وشركات القطاعين العام والخاص من أجل دعم البحوث والتطوير.

تاسعًا: مؤشرات الأداء:

يعد هذا الجزء من أهم أجزاء الاستراتيجية، حيث إن مؤشرات الأداء الرئيسية هى العامل الرئيسى لمتابعة تنفيذ ما جاء بالاستراتيجية وقياس درجة التقدم فى تنفيذها، وتتكون المؤشرات من عدة مقاييس كمية ونوعية منها المؤشرات الكلية ومؤشرات المواهب الوطنية ومؤشرات النمو والابتكار ومؤشرات الشراكة الوطنية ومؤشرات التوعية.

المطلب السادس
نتائج الجهود المصرية فى مجال الأمن السيبراني

إنّ أى اتفاق فى المجتمع الدولى دائما يقابله التزام، الأمر الذى دعا المجتمع الدولى إلى إيجاد آليات لقياس الأداء ومدى الالتزام ومستوى التقدم خلال مدة معينة، فظهرت العديد من المؤشرات الدولية والعالمية ومنها مؤشر الأمن السيبرانى العالمى Global Cybersecurity Index (GCI)) وهو مؤشر يصدره مركز الأمن السيبرانى العالمى فى الاتحاد الدولى للاتصالات (ITU)، وذلك من خلال تحليل أداء الدول فى ٨٠ مؤشرًا فرعيًا وكذا مؤشر الأمن السيبرانى الوطنى National Cyber Security Index (NCSI) ويتم إصدار المؤشر من قبل مركز الأمن السيبرانى الوطنى فى استونيا (NCSC) وهو ما يدعونا إلى بيان التقييم الخاص بالجهود السيبرانية للدولة المصرية فى ضوء المؤشرين آنفى البيان، حيث احتلت مصر المركز الثالث والعشرين عالميًا فى مؤشر قياس استعدادات الدول فى مجال الأمن السيبرانى الذى أصدره الاتحاد الدولى للاتصالات، فى عام ٢٠٢٠، بينما احتلت مصر فى مؤشر الأمن السيبرانى الوطنى فى استونيا (NCSC) فى نوفمبر ٢٠٢١، المركز الستين عالميًا.

علمًا بأن الدولة المصرية قد حققت نجاحات فى مجال الأمن السيبرانى يمكن إيجازها على النحو التالى:

- المشاركة فى مؤتمر بودابست للفضاء الإلكترونى فى أكتوبر ٢٠١٢ فى المجر
- مشاركة مصر فى ورشة العمل الإقليمية العربية حول حماية الأطفال على الإنترنت بالاتحاد الدولى للاتصالات حول الجوانب القانونية لحماية الأطفال على الإنترنت فى المنطقة العربية» فى يونيو ٢٠١٢.
- تشكيل اللجنة الوطنية لحماية الطفل على الإنترنت فى مارس عام ٢٠١٣
- احتل المركز المصرى للاستجابة لطوارئ الحاسب الآلى «سيرت» المرتبة الثالثة حسب مؤشر الأمن السيبرانى العالمى للاتحاد الدولى للاتصالات فى أكتوبر عام ٢٠١٣.
- كما حصل المركز على عضوية اللجنة التوجيهية لفريق الاستجابة لطوارئ الحاسوب التابع لمنظمة المؤتمر الإسلامى فى نوفمبر عام ٢٠١٣.
- استضاف المركز والجهاز القومى لتنظيم الاتصالات فى نوفمبر ٢٠١٦ المؤتمر الإقليمى الخامس للأمن السيبرانى ومنتدى فرست الإقليمى للمنطقة العربية والإفريقية.
- شارك المركز المصرى للاستجابة لطوارئ الحاسب الآلى «سيرت» فى المنتدى الإقليمى

للاتحاد الدولى للاتصالات نوفمبر ٢٠١٧ وورشة عمل لتقييم الجاهزية للاستجابة للطوارئ المعلوماتية للمنطقة العربية والإفريقية.

- قامت مصر بإقامة وعقد معرض ومؤتمر أمن المعلومات والأمن السيبرانى «CAISEC'22» على مدار يومى ١٣و ١٤ يونيو ٢٠٢٢ تحت عنوان «الأمن السيبرانى وقت الأزمات» برعاية ودعم من وزارات مختلفة وتكرر إقامة الحدث عام ٢٠٢٤ وشارك به العديد من الجهات الحكومية والقطاع الخاص والعديد من الجهات الدولية.
- تم انتخاب مصر لرئاسة المجلس الأعلى للاتصالات وتكنولوجيا المعلومات بالاتحاد الإفريقى لمدة عامين، كما تم أيضا انتخاب مصر لرئاسة المكتب التنفيذى لمجلس الوزراء العرب للاتصالات وتكنولوجيا المعلومات لمدة عامين.
- ترأست مصر الدورة ٢٤ لمجلس الوزراء العرب للاتصالات والمعلومات.
- فازت مصر بعضوية المجلس الإدارى للاتحاد الدولى للاتصالات عن إفريقيا وعضوية لجنة لوائح الراديو التابعة للاتحاد٢٠٢٣.

■ النتائج والمقترحات

أولا: من الناحية المؤسسية

١-التوسع فى إصدار استراتيجيات قطاعية على مستوى كافة مؤسسات الدولة والالتزام بها لكون الأصول الرقمية من أصول الدولة الحساسة.

٢-تحديد خطة العمل والمسئوليات والمهام محددة التوقيت وتحديد الموارد والمصادر (الرقمية) وفق مبادئ الإتاحة والنزاهة والشفافية.

٣-توفير المزيد من الشفافية فى نشر الاستراتيجية ومراحل تنفيذها بما يحقق الغاية منها ووضع آلية لتفعيل دور المجلس الأعلى للأمن السيبرانى فى وضع الخطط القطاعية ومراقبة تنفيذ الاستراتيجية ومدى الالتزام بها.

٤-العمل على إصدار دليل إرشادى للأمن السيبرانى فى كل جهة ومؤسسة حكومية ونشره وتعميمه على أن يكون ذلك تحت إشراف ومتابعة المجلس الأعلى للأمن السيبرانى.

٥-أن يتماشى تنفيذ الاستراتيجية مع نهج الدولة فى كافة الاستراتيجيات الأخرى التى تتبناها الحكومة مثل « استراتيجية الذكاء الاصطناعى – استراتيجية مكافحة الفساد –استراتيجية المناخ – خطط التنمية المستدامة والخطة الاقتصادية.

٦-وضع ممثل عن السلطة التشريعية الوطنية وكذا لجان الإصلاح التشريعى التابعة لرئاسة مجلس الوزراء والجهات المعنية بالحوكمة التشريعية ضمن تشكيل المجلس الأعلى للأمن السيبرانى، لضمان التحديث المستمر والدائم للتشريعات الحاكمة لمواكبة التطور السريع الحاصل فى مجال حماية الفضاء السيبرانى والهجمات السيبرانية فى ضوء ما نصت عليه الاستراتيجية فى المحور الثالث منها « بناء إطار تشريعى متكامل».

٧-تمثيل جهات البحث العلمى المتعلقة بهذا الشأن فى عضوية المجلس الأعلى للأمن السيبرانى، وكذا ذوى الخبرة فى ضوء ما نصت عليه الاستراتيجية فى المحور التاسع منها «برامج تشجيع البحث العلمى وتعزيز الابتكار والنمو».

ثانيًا: من الناحية التشريعية والقضائية

١-العمل على اكتمال النموذج الأمثل للإطار التشريعى – فى ضوء ما نصت عليه الاستراتيجية فى المحور الثالث منها «بناء إطار تشريعى متكامل» – ومؤسسى وتنظيمى قادر على حماية المقدرات الرقمية وتحقيق الأمن السيبرانى، وذلك من خلال تعزيز التشريعات القائمة بصياغة قوانين وتشريعات فعالة وشاملة تعالج جرائم الأمن السيبرانى وتحمى الأفراد والمؤسسات.

٢-إجراء تعديل تشريعى بقانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ يتم فيه إلغاء التصالح في الجرائم الإلكترونية، وتشديد العقوبات إلى عقوبة الجناية إذا ما كان الفعل الاجرامى متصلاً بالأمن والاقتصاد القومى أو تنفيذا لغرض إرهابى على وجه العموم.

٣-إجراء تعديل تشريعى على قانون تنظيم الاتصالات يتم من خلاله إنشاء إدارة مستقلة من خبراء تقنية المعلومات تكون تابعة لإدارة خبراء وزارة العدل وجزء من تكوين مكتب خبراء وزارة العدل.

٤-إذا كان المشرع المصرى قد أحسن صنعًا حين أناط بالمحكمة الاقتصادية الفصل فى كافة منازعات وجرائم الأمن السيبرانى، إلا أننا نقترح أن تكون المحاكمات سرية فى بعض الحالات تشجيعًا لضحايا الجرائم السيبرانية على الإبلاغ عنها، دون الخشية من التشهير بهم.

ثالثاً : من الناحية التوعوية والتثقيفية وإعداد الكوادر

١-حث الإعلام بمختلف أشكاله المرئية والمسموعة والمقروءة والحديثة منها على الإنترنت ومواقع التواصل الاجتماعى بتبنى حملات توعية عن الأمن السيبرانى تتناسب ومختلف الثقافات والمراحل العمرية والتخصصات ومستوى التعليم والمعرفة.

٢-تعزيز الوعى الأمنى إذ يجب أن يتم توعية الأفراد والمؤسسات بأهمية الأمن السيبرانى وأساليب الوقاية والدفاع الأساسية، كما يجب أن يتم تنظيم حملات توعية وتدريبات لتعزيز المعرفة والمهارات فى مجال الأمن السيبرانى.

٣-نشر ثقافة الأمن السيبرانى فى التعليم الأساسى وقبل الجامعى والجامعى وذلك بتبنى مناهج تعليمية فى مراحل التعليم المختلفة لنشر الوعى بين الطلاب فى مختلف المراحل العمرية لخلق جيل واع يقدر أهمية الأمن السيبرانى ويستطيع مواجهة التحديات.

٤- التركيز على الابتكار والبحث والتطوير:

أ- يجب دعم الابتكار والبحث والتطوير فى مجال الأمن السيبرانى، وذلك لمواجهة التهديدات المتطورة والمستقبلية، كما ينبغى الاستثمار فى تطوير تقنيات وأدوات جديدة للكشف والوقاية والاستجابة للجرائم السيبرانية.

ب- الاستثمار فى العنصر البشرى القائم على هذا المجال بإعداد كوادر فعالة وصقلها بمهارات متجددة ومتطورة باستمرار فى مواجهة تلك التحديات والمخاطر وكيفية إدارة الأزمات ومعالجتها.

رابعًا: فى مجال التعاون الدولى ومتابعة مؤشرات الأداء

١- فى مجال التعاون الدولى والاتفاقيات الدولية مصدر الالتزام الوطنى:

أ- يجب أن يكون هناك تعاون فعال بين الدول فى مجال مكافحة الجرائم السيبرانية، كما يجب تبادل المعلومات والخبرات وتقاسم أفضل الممارسات والتعاون فى مجال التحقيقات الجنائية السيبرانية لمواجهة التهديدات المشتركة.

ب- تعزيز الشراكات سواء من المؤسسات العامة والخاصة المحلية والإقليمية الدولية، فيجب تشجيع التعاون بين القطاع العام والخاص والأكاديمى لمكافحة الجرائم السيبرانية. يمكن تبادل المعلومات والخبرات والتعاون فى تطوير حلول تكنولوجية واستراتيجيات فعالة فى إطار تنمية الابتكار والبحث العلمى.

٢- فى مجال متابعة مؤشرات الأداء:-

أ- اعتماد النتائج الدولية لخطط العمل والممارسات الفضلى فى وضع الاستراتيجية وذلك بتبنى نموذج أمثل والبناء عليه وتخصيصه وفقاً للرؤية المصرية والتحديات ذات الخصوصية خاصة أن دليل الاتحاد الدولى للاتصالات فى هذا الشأن دائم التحديث والتطور.

ب- متابعة المؤشرات العالمية وتبنى منهجيات التقييم الخاصة بها للوصول لمراكز متقدمة إن لم يكن الهدف الصدارة.

ج- العمل على وضع آليات للتدقيق والمراجعة فى تطبيق سياسات واستراتيجيات الأمن السيبرانى للوصول إلى إمكانية قياس الأداء ومن ثم تطبيق المعايير العالمية والمقاييس الدولية ذات الصلة.

■ المـراجــع:

أولاً: المراجع العربية:

- بطيخ، حاتم، (٢٠٢١)، تطور السياسة التشريعية فى مجال مكافحة جرائم تقنية المعلومات، دراسة تحليلية مقارنة، مجلة الدراسات القانونية والاقتصادية، جامعة السادات، مجلد (٥)، العدد (١) اغسطس ٢٠٢١.
- وزير، عبدالعظيم، (٢٠٠٩)، شرح قانون العقوبات القسم العام- الجزء الأول.. النظرية العامة للجريمة، دار النهضة العربية.
- العوادى، أوس، ٢٠١٦، (س.ن). الأمن المعلوماتى السيبرانى. مركز البيان للدراسات والتخطيط، ص٥.
- الهيئة العامة للاستعلامات. (س.ن). تقرير الهيئة العامة للاستعلامات جمهورية مصر العربية.
- جعفر، حاتم، القاضى، هيثم، ولبيب، محمد. (٢٠٢٣). الأطر الاستراتيجية والقانونية للأمن السيبرانى. الأكاديمية الوطنية لمكافحة الفساد.
- الحسين، حسن. (٢٠٢٢). أساسيات الأمن السيبرانى. سوريا.
- أكويس، خالد.(٢٠١٨) الأمن السيبرانى فى الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.ص٣٠٣-٣٠٦.
- رئاسة مجلس الوزراء المصرى. (٢٠٢٣). حكاية وطن. الكتاب الأول.
- عبد الصادق، عادل. (٢٠١٨). الهجمات السيبرانية: أنماط وتحديات جديدة للأمن العالمى. المركز العربى لأبحاث الفضاء الإلكترونى.
- العتيبى، عبد الرحمن، وميرغنى، المرشدى. (٢٠٢٠). دور الأمن السيبرانى فى تحقيق رؤية ٢٠٣٠. جامعة نايف العربية للعلوم الأمنية.
- العمارات، فارس، والحمامصة، إبراهيم. (٢٠٢٢). الأمن السيبرانى: المفهوم وتحديات العصر. الطبعة الأولى.
- سليمان، قطاف، وبوقرين، عبد الحليم، ٢٠٢٢، (س.ن). مواجهة الجرائم السيبرانية فى ضوء الاتفاقيات الدولية. كلية الحقوق والعلوم السياسية – جامعة عمار ثليجى الأغواط، الجزائر.
- الطيب، مصطفى. (س.ن)، ٨ أغسطس،٢٠١٩، مقدمة فى الأمن السيبرانى: مدخل إلى الأمن السيبرانى والشبكات وأنظمة التشغيل. مدونة علمية.
- السمحانى، منى. (٢٠٢٠). متطلبات تحقيق الأمن السيبرانى لأنظمة المعلومات الإدارية. مجلة كلية التربية جامعة المنصورة. العدد ١١.

- آل خليفة، مى. (٢٠٢٣). دور التحول الرقمى فى تحقيق الأمن السيبرانى: دراسة تطبيقية على وزارة العدل بدولة قطر. مجلة البحوث الإدارية. العدد ١.
- أحمد، هلالى. (٢٠١١). اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها. دار النهضة العربية.
- أحمد، هلالى. (١٩٩٧). تفتيش نظم الحاسب الآلى وضمانات المتهم المعلوماتى. دار النهضة العربية.

ثانيًا: المقالات والمواقع على الإنترنت:

- بوابة تخطيط التنمية الوطنية العربية التابعة للإسكو. (س.ن).
- جريدة اليوم السابع. (٢٠١٥، ١٤ يناير). محاربة الإرهاب الإلكترونى.
- وزارة الاتصالات وتكنولوجيا المعلومات المصرية. (س.ن). الموقع الرسمى.
- المركز الإعلامى للهيئة المصرية للاستعلامات. (س.ن).
- جريدة المصدر. (٢٠١٤، ١٨ ديسمبر).
- الريس، سوزى. (س.ن). تعريف الاستراتيجية. موقع المقال.
- مسح الحكومة الإلكترونية ٢٠٢٢: مستقبل الحكومة الرقمية. (س.ن).
- المعهد الأمريكى للمعايير والتكنولوجيا. (س.ن). إصدار إطار حوكمة استراتيجيات الأمن السيبرانى.
- المركز الوطنى الإرشادى للأمن السيبرانى السعودى. (س.ن). الموقع الرسمى.
- موقع اليوم السابع. (س.ن).
- تقرير حالة مصر وفق تقرير ٢٠٢١ للمؤشر الوطنى للأمن السيبرانى. (س.ن).
- تقرير المركز القومى للاستعلامات. (س.ن).

ثالثًا: المراجع والمواقع على الإنترنت باللغة الإنجليزية:

Draft Explanatory Memorandum to the Draft Convention on Cybercrime. (2001, February 14). Strasbourg.

Final Activity Report. (2001, May 25). Strasbourg.

Cambridge Dictionary. (Cyber. Retrieved from https://dictionary.cambridge.org/dictionary/english/cyber on 03/03/2024.

Recommendation X.1205 (04/08) Overview of cybersecurity. Retrieved from https://www.itu.int/rec/T-REC-X.1205-200804-I on 03/03/2024.

National Institute of Standards and Technology (NIST). Cybersecurity. Retrieved from https://csrc.nist.gov/glossary/term/cybersecurity on 03/03/2024.

Green, James. (2016). Cyber Warfare: A Multidisciplinary Analysis. Routledge.

Middleton, Bruce. (2017). A History of Cyber Security Attacks 1980 to Present. Routledge.

IBM. (2023). Cost of a Data Breach Report. Retrieved from https://www.ibm.com/reports/data-breach on 03/03/2024.

Statista. Estimated cost of cybercrime worldwide 2017-2028. Retrieved from https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide on 03/03/2024.

Benson, Vladlena, & McAlane, John. (2020). Emerging Cyber Threats and Cognitive Vulnerabilities. Academic Press.

Kala, Emiles. (2023). The Impact of Cyber Security on Business: How to Protect Your Business. Open Journal of Safety Science and Technology, 13(2). Retrieved from https://www.scirp.org/journalpaperinformation?paperid=126109 on 03/03/2024.

Maurer, Tim, & Nelson, Arthur. (2021). The Global Cyber Threat: Cyber threats to the financial system are growing, and the global community must cooperate to protect it. International Monetary Fund. Retrieved from https://www.imf.org/external/pubs/ft/fandd/2021/03/pdf/global-cyber-threat-to-financial-systems-maurer.pdf on 03/03/2024.

National Institute of Standards and Technology (NIST). About NIST. Retrieved from https://www.nist.gov/about-nist on 03/03/2024.

National Institute of Standards and Technology (NIST). Cyber Framework. Retrieved from https://www.nist.gov/cyberframework on 03/03/2024.

Council of Europe. (2001). Explanatory Report to the Convention on Cybercrime: Budapest. Retrieved from https://rm.coe.int/16800cce5b on 03/03/2024.

ESCC. الموقع الرسمى للمركز المصرى للاستجابة لطوارئ الحاسب الآلى. Retrieved from https://www.escc.gov.eg/ on 03/03/2024.

EG-CERT. Retrieved from https://egcert.eg/ar/ on 03/03/2024.

Gate.ahram. Retrieved from https://gate.ahram.org.eg/

News/3187514.aspx on 03/03/2024.

UN-ESCWA. Retrieved from https://andp.unescwa.org/sites/default/files/2021-11/AR_National_Cybersecurity_Strategy_2017_2021.pdf on 03/03/2024.

International Telecommunication Union (ITU). Global Cybersecurity Index. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx on 03/03/2024.

NCSI. (Retrieved from https://ncsi.ega.ee/ on 03/03/2024.

UN-ESCWA. (Retrieved from https://andp.unescwa.org/sites/default/files/2021-11/AR_National_Cybersecurity_Strategy_2017_2021.pdf on 03/03/2024.

International Telecommunication Union (ITU). Retrieved from http://www.itu.int/md/S06-PP-C-0024-en on 03/03/2024.

Bayan Center. etrieved from www.bayancenter.org on 03/03/2024.

Oolom. Retrieved from https://www.oolom.com/6124/ on 03/03/2024.

رابعًا: المراجع باللغة الفرنسية

Kowalski, Melanie. (2002). Cybercriminalité: enjeux, sources de données et faisabilité de recueillir des données auprès de la police. Centre canadien de la statistique juridique, 85-558-XIF.