الأمن السيبرانى:
الأبعاد الاجتماعية والقانونية
تحليل سوسيولوجى

إسلام فوزى *

تناول البحث الحالى موضوع الأمن السيبرانى بالتركيز على الأبعاد الاجتماعية التى هى: تهديدات الجرائم السيبرانية المستحدثة، وزيادة معدلاتها؛ ومظاهر استهداف الأمن القومى؛ وتهديد القيم والأخلاق؛ وتدمير البنية التحتية؛ وترسيخ أزمة عدم الثقة لدى المواطنين، وغيرها من المخاطر الاجتماعية. ثم يعرض البحث الأبعاد التشريعية والتنظيمية من خلال القوانين المتعلقة بحماية الأمن السيبرانى وأهمية التعاون والسياسات الدولية. وأخيرا يتطرق البحث لآليات الحماية وممارسات الأمن السيبرانى. ويختتم بعرض لأهم النتائج ودلالتها النظرية.

مقدمة

مما لاشك فيه أن العالم أصبح يعانى من مشكلات اجتماعية أفرزتها البيئة الرقمية، بيد أن هذه المشكلات أصبحت مسارًا للبحث والدراسة لا سيما فى مجال علم الاجتماع مثل الغزو الثقافى الرقمى، والجريمة السيبرانية، والابتزاز والتنمر الإلكترونيين إلخ.

وفى ضوء هذه البيئة المتغيرة، ثمة حاجة ملحة لاتخاذ إجراءات– على الصعيدين المحلى والدولى– لحماية الاستهلاك والخصوصية ومجابهة تقنية المعلومات ضد جميع أشكال الجريمة السيبرانية، وهذا ما دعا لإعداد البحث

* مدرس علم الاجتماع القانونى، قسم علم الاجتماع، كلية الآداب، جامعة دمنهور.

الراهن. ففى ظل ما يشهده العالم من تطور سريع ومتزايد فى النظم الذكية والأجهزة الإلكترونية وما صاحبهما من هجمات وجرائم سيبرانية غدت الضرورة ملحة لنشر دعائم الأمن السيبرانى وتأمين سلامة الممارسة الإلكترونية.

وفى ضوء ما سبق تتضح الأهمية (النظرية والتطبيقية) للبحث فيما يلى:

وفقاً لخطة التنميـة المستدامة لعام ٢٠٣٠ التى وافقت عليها حكومات العالم فى سبتمبر٢٠١٥، والتى جاء فيها "تبشير بانتشار تكنولوجيا المعلومات والاتصالات والترابط العالمى بإمكانات كبيرة بل بتعجيل التقدم البشرى وسد الفجوة الرقمية وإنشاء مجتمعات المعرفة"(١). وفى ضوء ذلك يُعد هذا البحث خطوة لرصد وتحليل واحد من الموضوعات التى لها دور مهم فى سد الفجوة الرقمية وإنشاء مجتمعات المعرفة. وهنا تتجسد الأهمية التطبيقية فى توفير معلومات وبيانات يمكن أن يستفاد منها فى وضع الخطط والبرامج التى قد تساعد فى مواجهة تحديات الأمن السيبرانى فى المجتمع، فبموجبها يُمكن تحقيق سلامة وأمن المجتمعات من خلال ضبط البنية الرقمية التى تنعكس على البنية الواقعية. فضلاً عن الأهمية النظرية للبحث كإحدى الدراسات التى يمكن أن تثرى فرعى علم الاجتماع الرقمى والقانونى.

المشكلة والمنهج

١- المشكلة

إننا نتمتع بفوائد مجتمع معلوماتى عالمى، ولكنها تأتى مقترنة بتهديد الهجمات السيبرانية. ويمكن أن تنشأ هذه التهديدات فى أى مكان وفى أى وقت وأن تسبب ضرراً هائلاً فى طرفة عين. وهذا الضرر المحتمل يتزايد بصورة مضطردة مع ربط تكنولوجيا المعلومات والاتصالات بالبنية التحتية القومية. ولذا، وجب أن يعمل المجتمع للقضاء على هذا التهديد المتزايد(٢). وفى هذا

الصدد نبه رئيس مركز المعلومات ودعم القرار بمجلس الوزراء فى كلمته خلال مؤتمر "قانون مكافحة تقنية المعلومات بين الواقع والتطبيق" ٢٠١٨ بأن حجم الإنفاق السنوى عالميًا على الأمن السيبرانى وصل لحوالى ١٤٤ مليار دولار فى حين بلغ حجم الإنفاق العسكرى ٧،١ تريليون دولار سنويًا، أى أنه يمثل ٨٪ من حجم الإنفاق العسكرى عالميًا نظرًا لأهميته.

ومن ثَم فالأمر جد خطير؛ إذ كشفت دراسة حديثة فى مجال تكنولوجيا المعلومات عن أن الجرائم السيبرانية ستكلف العالم ما يقارب من ٦ تريليونات دولار سنويا فى عام ٢٠٢١ وهذا ضعف المبلغ فى عام ٢٠١٥، فهذه التكاليف نابعة من الأضرار والآثار الكثيرة التى تُخلفها الجرائم السيبرانية ومنها سرقة البيانات أو تخريبها وسرقة الأموال، وفقد الإنتاجية، وسرقة الملكية الفكرية، والاختلاس. والاحتيال، والاختلالات التجارية، والتحقيق الجنائى، واختراق الأنظمة، والإضرار بالسمعة[٣]. أضف إلى ذلك أن بعض المجموعات السيبرانية قد تكون مدعومة ومكرسة من قبل جهات أو حتى دول لأغراض هجومية أو استخباراتية[٤].

وفى هذا السياق نجد العديد من الدراسات الاجتماعية[٥] التى تناولت رصد المخاطر الإلكترونية، حيث ركزت غالبيتها على قضايا مجتمعية خطيرة أهمها:

- توضيح أثر التغييرات التكنولوجية على انتشار الجرائم المعلوماتية.
- توضيح الاستخدام السلبى لشبكة الإنترنت.
- رصد حجم وطبيعة الجرائم الإلكترونية الجديدة.
- الوقوف على أكثر الجرائم الرقمية انتشارا.

اعتمدت معظم هذه الدراسات على منهج إعادة التحليل ودراسة الحالة والمقابلة وتحليل بيانات جاهزة والنظرية النقدية، وتوصلت إلى نتائج مهمة منها ما يلى:

- أن أشهر الجرائم انتشارًا هى جرائم الدخول غير المشروع إلى البريد الإلكترونى للآخرين، وإنشاء مواقع للتشهير، ثم جرائم اختراق المواقع على الشبكة، ثم جرائم انتهاك حقوق الملكية.
- سوء استخدام الإنترنت أدى إلى إدمان المواقع الإباحية للهروب من الملل والخلافات والمشكلات الزوجية.
- يؤثر استخدام الإنترنت على العلاقات الاجتماعية والأسرية ويسبب العزلة والانطواء.
- تنامى جرائم الإنترنت فى المجتمع المصرى ومن أشهرها (جرائم السب والقذف والتشهير).

وفى ضوء ما سبق فإن هذه الدراسة تثير قضية بحثية لم تتناولها الدراسات السابقة فى مجال علم الاجتماع وهى الأمن السيبرانى. ففى ضوء هذه المخاطر ينطلق البحث الراهن من حيث انتهت هذه الدراسات بمحاولة سوسيولوجية جديدة تسعى لرصد وتحليل ركائز الأمن السيبرانى وتوضيح مدى استعداد الدول لمواجهة التهديدات التى باتت تشكل مخاطر اجتماعية عالمية، يمكن تفاديها بالاهتمام بالبنى التحتية والإنجازات الاستراتيجية والتطلعات التشريعية التى تنُم عن الاستعداد والتهيئة لفاعلية الأمن السيبرانى، لاسيما بعد أن أبدت مصر استعدادها من خلال تقرير مؤشر قياس استعداد الدول فى مجال الأمن السيبرانى الذى أصدره الإتحاد الدولى للاتصالات ٢٠١٧، حيث جاءت فى المرتبة الرابعة عشرة من بين ١٩٣ دولة من دول أعضاء الاتحاد،

وفى المرتبة الثانية عربياً بعد سلطنة عمان التى جاءت فى المركز الرابع عالمياً والأول عربيًا.

ومن هنا تتبلور إشكالية البحث فى الوقوف على أهم ركائز وممارسات الأمن السيبرانى اجتماعيًا ومجتمعيًا من خلال تحليل بُعديه الاجتماعى والقانونى لكونهما أهم بعدين، فأولهما يبرز المخاطر والتهديدات الاجتماعية، وثانيهما يعكس آليات المواجهة وسبل الحماية التشريعية والتنظيمية.

وفى ضوء ذلك يتمحور الهدف الرئيس حول التحليل السوسيولوجى لأبعاد الأمن السيبرانى المصرى. ويثير هذا الهدف عدة تساؤلات يطمح البحث فى الإجابة عنها وهى:

- ما الأبعاد الاجتماعية التى دعت لوجود الأمن السيبرانى؟
- ما الأطر التشريعية والتنظيمية للأمن السيبرانى؟
- ما سُبل وآليات المكافحة؟
- ما مظاهر الاهتمام بالأمن السيبرانى المصرى فى ضوء الشواهد والبراهين؟
- ما مجهودات أبرز الفاعلين بمجال الأمن السيبرانى فى مصر؟

مفاهيم الدراسة

- **السيبرانية:** تكتب سبرانى وسيبرانى وسيبيرانى. وهى صفة لما هو مرتبط بتقنية المعلومات والحواسيب، وتعنى: فضاء الإنترنت أو العالم الافتراضى.
- **الأمن السيبرانى:** يعرفه الاتحاد الدولى للاتصالات بأنه:

مجموعة من المهمات، مثل تجميع وسائل، وسياسات، وإجراءات أمنية، ومبادئ توجيهية، ومقاربات لإدارة المخاطر، وتدريبات، وممارسات، وتقنيات، يمكن استخدامها لحماية البيئة السيبرانية والمؤسسات والمستخدمين[٦]. كما يُعرَّف بأنه مجموعة الأدوات والسياسات والمفاهيم الأمنية والضمانات الأمنية والمبادئ التوجيهية ونُهُـــج إدارة المخاطـر والإجـراءات والتدريب وأفضـل

الممارسات وسبل الضمان والتكنولوجيات التى يمكن استخدامها فى حماية البيئة السيبرانية(٧).

- **الأبعاد الاجتماعية:** تتجسد فى تأثير المخاطر الاجتماعية والتهديدات السيبرانية فى تشكيل بنية المجتمع ومنها زيادة الجرائم المستحدثة، تهديد البنية التحتية، تهديد القيم والأخلاق، استهداف الأمن القومى، تصدير أزمة ثقة فى الحكومة والأجهزة . (تعريف إجرائى).
- **الحماية القانونية:** تعنى ضمان وجود أُطر تشريعية وتدابير نظامية؛ للحماية من الخطورة الاجتماعية والقانونية وتتجسد فى وجود تشريعات للمكافحة والحماية، عدم تضارب القوانين، التعاون الدولى، الاتفاقيات الدولية، إنشاء وحدات مكافحة، استصدار سياسات واستراتيجيات. (تعريف إجرائى).

المنهج

تُعد هذه الدراسة دراسة وصفية تحليلية تعتمد على منهج التحليل الوصفى وطريقة التحليل الثانوى" البيانات الجاهزة" لركائز وممارسات الأمن السيبرانى خلال العشر سنوات السابقة بدءاً من ٢٠٠٩ مع إنشاء أول مركز طوارئ لتلقى الشكاوى (CERT) وحتى ٢٠١٩ مع تنظيم ماستر كارد لأول منتدى حول الأمن السيبرانى فى القاهرة.

مستويات التحليل

- التحليل على المستويات الكبرى "الماكرو Macro Levels Analysis" (تحليل أحدث تقرير ٢٠١٧ للاتحاد الدولى للاتصالات (ITU) حول استعدادات مصر فى الأمن السيبرانى عالمياً وإفريقياً وعربياً).
- التحليل على المستويات الوسطى"الميزو miso- levels analysis" (تحليل مظاهر الاهتمام بالأمن السيبرانى فى مصر– وجهود أبرز الفاعلين بمجال

الأمن السيبرانى من خلال البيانات الجاهزة على الموقع الدائم لوزارة الاتصالات وتكنولوجيا المعلومات).

- التحليل على المستويات الصغرى "الميكرو Micro Levels Analysis" (تحليل تشريعات الحماية المصرية وتتمثل فى قانون ١٧٥ لسنة ٢٠١٨، قانون مكافحة تقنية المعلومات).

المنظور السوسيولوجى لدراسة الأمن السيبرانى

١- نظرية مجتمع المخاطر: "Risk Society Theory": لرصد وتحليل المخاطر السيبرانية

يُعد أولريش بك "Uilrich Beck" أستاذ علم الاجتماع الألمانى أول من فجر قضية المخاطرة ووضعها على قائمة جدول أعمال العلم الاجتماعى المعاصر، بعد أن تأثر علم الاجتماع من القرن العشرين بفكرة أو مفهوم المخاطرة فى المجتمع(٨).

تتناول نظرية المخاطر الوجود المتزايد لانعدام اليقين المنتشر فى ظل التغيرات التى تحدث فى المجتمع، حيث اندثر المجتمع الصناعى مفسحاً المجال لمجتمع المخاطر التقنى والتكنولوجى أو المجتمع المعلوماتى، وهو ما يطلق عليه منظرو ما بعد الحداثة "عالم الفوضى" الذى تغيب معه أنماط الحياة المستقرة(٩).

وفى ضوء ذلك يرى "اولريش بك" فى كتابه (مجتمع المخاطرة، ١٩٨٦) أن "مجتمع المخاطر" ظهر فى منتصف القرن العشرين وهو مجتمع ساخط على تبعات الحداثة السلبية، يبحث فى كيفية إدارة المخاطر والأخطار بالوقاية والعلاج معاً من خلال ما أسماه "بعقد المخاطرة" أى القدرة على التحكم فى التهديدات والأخطار. ثم استطاع أن يفرق بعد عشرين سنة بين مجتمع المخاطرة ومجتمع المخاطر العالمى من خلال كتابه الجديد (مجتمع المخاطر

العالمى: بحثا عن الأمان المفقود، ٢٠٠٦)، حيث يرى أن انتشار الأخطار عبر مجتمع عالمى فى مختلف الأقطار يجعلها تنتشر وتتمدد دون القدرة على إخضاعها أو التحكم فيها والسيطرة عليها من خلال العولمة وانسيابية التدفق وتخطى الحدود القومية التى عملت على توسيع نطاق عدم الأمان المصطنع، ومع تفاقم المخاطر والأخطار مقابل الفرص فإن مجتمع المخاطر بات يعيش حالة من عدم الأمان والشك وفقدان اليقين بخصوص إمكانياته ومقدرته على مواجهة تلك المخاطر والأخطار والتحكم فيها مكانياً وزمنياً. ولذ يتفق علماء الاجتماع على أن العالم يعيش حالة من فقدان اليقين العالمى(١٠).

وهنا يفرق "نيكلاس لومان" بين المخاطرة والخطر فى كتابه (المخاطرة: نظرية سوسيولوجية)، إذ يعرف المخاطرة على أنها: أذى محتمل يخيف الفرد ويرتكز على قرار اتخذه بنفسه. أما الخطر فهو: الأذى المحتمل الذى يتعرض له الفرد بفعل مؤثرات خارجية دون اتخاذ قرار من الفرد. ويرى "انتونى جيدنز" من خلال كتابه (عالم منفلت: كيف تعيد العولمة صياغة حياتنا) أن المخاطر نوعان الأول: مخاطر خارجية مرتبطة بالتقاليد والطبيعة، والثانى مخاطر مصطنعة، يتدخل فيها الإنسان بإرادته، كما يرى أن هذا النوع من المخاطر أصبح أكثر خطرًا من المخاطر الخارجية، مما جعلنا فى مجتمع ما بعد الطبيعة أو ما بعد التقاليد، أى أن ملامح واقعنا أخذت تتلاشى مع التحول فى توازن الخطر والأخطار الناتج عن المخاطر التى نخلقها بأيدينا(١١). حيث يرى "أنتونى جيدنز" أننا وفقًا "لأولريش بك" نعيش عالم المخاطرة وعدم اليقين فى المستقبل نتيجة التحولات والتغيرات التى تحدث فى المجتمع، فقد عرف مجتمع المخاطر بأنه "المجتمع المتخم بالاستقطابات الاجتماعية"(١٢).

وفى ضوء القراءات السوسيولوجية السابقة لمجتمع المخاطر العالمى، والعالم المنفلت، وسوسيولوجية المخاطر وبإحالة ذلك على موضوع البحث نجد

أن العلاقات والأفعال الافتراضية ساعدت فى تشكيل مجتمع المخاطر لكونها تتذر بالخطر، فقد شكلت خطرا على العلاقات الاجتماعية الواقعية باتساع شبكة العلاقات الإلكترونية التى هددت بمخاطر شبكة العلاقات الإجرامية وانعدام الأمن الافتراضى. ويتبنى البحث هذه النظرية فى عرض وتفسير وتحليل الأبعاد الاجتماعية ثم الأبعاد القانونية والتنظيمية للأمن السيبرانى بالتركيز على ما تحتويه من أخطار ومخاطر اجتماعية كما سيتبين لاحقا.

٢- نظرية تشكيل البنية "Structuration Theory" لرصد وتحليل ركائز وممارسات الأمن السيبرانى

يعتمد البحث على نظرية "تشكيل البنية" عند أنتونى جيدنز "A.Giddens" الذى يشير إلى أن البناءات الاجتماعية تتأسس من خلال الفعل البشرى، وفى الوقت نفسه تعد الوسيط الذى يحدث بواسطته هذا الفعل، وهو ما يسمى بازدواجية البناء التى تؤكد عدم الفصل بين البناء"Structure" والفعل "Agency"، فالبناء يتأسس من خلال الفعل، وبالتبادل فإن الفعل يتأسس بنائياً إذ تجمعهما علاقة تبادلية(١٣). وبالنظر إلى موضوع البحث ينظر للأمن السيبرانى على أنه فعل بنائى يُشكله المجتمع وقد يؤثر سلبًا وإيجابًا على البناء الاجتماعى الواقعى والافتراضى، لما لهذا الفعل "الأمن السيبرانى" من تأثير قوى وفعال على الأمن الوطنى والضبط الاجتماعى والاستقرار المجتمعى.

ويؤكد جيدنز على أن الوظائف الأساسية للتحليل السوسيولوجى تتمثل فى اثنتين، أولاهما التحليل التأويلى والتوسط بين أشكال الحياة داخل ما وراء اللغات الوصفية للعالم الاجتماعى. وثانيتهما تحليل عمليتى إنتاج وإعادة إنتاج المجتمع باعتبارهما الثمرة التى يحققها الفعل الإنسانى(١٤). أى أن النظرية تتبنى دراسة الممارسات "الأفعال" التى تتشكل من خلالها البنية الاجتماعية، وأن تستوعب دلالة وأهمية اللغة بوصفها الوسيط العملى الذى يجعل الفعل

ممكنًا[١٥]. وبذلك تعدت نظرية جيدنز حدود الأطر الجاهزة والمسلمات الإبستمولوجية إلى دراسة الممارسات التى تشكل البنية الاجتماعية. وتُعد ممارسات الأمن السيبرانى فى ضوء هذه النظرية من أهم مظاهر تشكيل البنية الاجتماعية وذلك فى ضوء **القضايا الرئيسة** التى دعا إليها جيدنز وهى كالآتى[١٦]:

أ- تنطوى عملية تشكيل البنية على المشاركة النشطة للذوات الفاعلة والممارسات اليومية الناجحة.

ب- يفرض البناء حدوداً على الفعل الإنسانى كما يُيسر تحقيق هذا الفعل "ازدواجية البناء".

ج- تتشكل البنية فى ضوء تفاعل بين المعانى والمعايير والقوة.

د- تتشكل البنية من خلال الأداء المهارى للأعضاء عبر مفهوم المكان والزمان.

الأبعاد الاجتماعية للأمن السيبرانى (المخاطر الاجتماعية)

لقد جاء فى تقرير الاتحاد الدولى للاتصالات (ITU) ٢٠١٠ بشأن الأبعاد الاجتماعية للأمن السيبرانى أن الثورة الرقمية غيرت كيفية التعامل التجارى، وكيفية عمل الحكومات. وأدت العولمة والتقدم التكنولوجى إلى إضعاف البنية التحتية وبالتالى جعلتها هدفاً محتملاً لهجمات إرهابية، حيث تُواجه البلدان مخاطر حقيقية؛ للأعداء أن يستغلوا مواطن الضعف التى تعانى منها أنظمة المعلومات الدقيقة. فهم يسعون إلى تعطيل البنية التحتية والموارد الأساسية من أجل تهديد الأمن القومى[١٧]. وهنا تكمن المخاطر الاجتماعية التى يمكن تفسيرها فى ضوء الآتى:

١- استحداث الجرائم السيبرانية وزيادة معدلاتها

مع الاعتماد المتزايد، في الحياة اليومية، على الأنظمة المعلوماتية، والأجهزة المتصلة بالشبكة الدولية للمعلومات، وتشعب طبيعة هذه الأجهزة من هواتف خلوية، وأجهزة حوسبة شخصية، يزداد عدد المتصلين بالفضاء السيبرانى، وتزداد احتمالات الاعتداءات والجريمة[١٨]. وتسهل سبل التجسس الاقتصادى وتؤثر على عمليات الحكومة مثل الفيروسات وهجمات منع الخدمة وسرقة البيانات والرسائل الاقتحامية والتدليس، وكلها تقوض مصداقية تكنولوجيا المعلومات والاتصالات وقدرة المجتمعات على العمل[١٩]. وقد أشار تقرير صادر عن مؤسسة ماكينزى، إلى توقع زيادة المعلومات الرقمية، بمعدل ٤٤٪، خلال الأعوام الممتدة من ٢٠٠٩ إلى ٢٠٢٠[٢٠].

وكذلك من أبـرز التهديـدات السيبرانيـة المحتمـل تزايـدها فى السنوات القادمة، هجوم الفدية (Ransom war)، الذى وصفته وزارة العدل الأمريكية بأنه نموذج عمل جديد للجريمة السيبرانية. ويُقدر مكتب التحقيقات الفيدرالى الأمريكى أن المبلغ الإجمالى من مدفوعات الفدية يقترب من مليار دولار سنويًا، حيث كان من المتوقع أن الشركات التجارية سوف تقع ضحية لهجوم الفدية كل ١٤ ثانية بحلول ٢٠١٩[٢١]. وتشير التقارير الدولية إلى أن فيروس الفدية تسبب فى خسائر مالية تفوق الخمسة مليارات دولار أثناء عام ٢٠١٧، وهو معدل مرتفع جداً خلال عام واحد. ومن أمثلة الهجوم الإلكترونى ما أصاب شبكة الكهرباء الأوكرانية والذى تسبب فى بقاء أُوكرانيا لساعات فى الظلام. وبذا، تخطت الحروب الإلكترونية والهجمات السيبرانية حاجز البيانات والمعلومـات والمواقـع الإلكترونية لتصل للبنيـة التحتيـة والأنظمـة الحيويـة مثل المفاعـلات النووية وأنظمـة الكهرباء والأنظمـة الطبيـة والنقل وغيرها من القطاعات التى تُعد ركائز أساسية للدول، مما يرفع مستوى الخطورة على

الدول[٢٢]. ومن المتوقع أن ترتفع التحديات والمخاطر فى الفترة القادمة لاسيما بعد أن أوضح تقرير "Overscan Security Advisory Council" عام ٢٠١٦، أن الهجوم السيبرانى على شركة أرامكو السعودية قد كلفها تغيير ٥٠ ألف قرص صلب لأجهزتها الحاسوبية، ولم تستطع استخدام الإنترنت لمدة خمسة أشهر تقريبا. كما أشار تقرير شركة نورتون الأمريكية (سمنتك) خلال شهر أغسطس ٢٠١٦ إلى أن هناك ٢٦٢،٥٣٨،٦ فردًا فى المملكة كانوا ضحايا هجمات سيبرانية أو تأثروا بجرائم سيبرانية. كذلك ذكر التقرير أن نسبة ٨٥٪ من السكان تعرضوا لهجمات سيبرانية وهذه النسبة تعد أعلى من النسبة العالمية بما يعادل ١٠٪[٢٣].

ومن أشهر الاختراقات، ما حدث من سرقة حسابات شركة ياهو (Yahoo) حيث بلغ عدد الحسابات المسروقة ثلاثة مليارات حساب، وكذلك اختراق إكيفاكس (Equifax) فى عام ٢٠١٧، حيث تأثر ٥،١٤٥ مليون عميل[٢٤]. وذلك يتطلب بشكل ملح إفساح المجال وبشدة للأمن السيبرانى تقنياً وتشريعياً وتنظيمياً ونشر ثقافة المواطنة الرقمية لزيادة سلامة التعامل السيبرانى.

ولذا، حذر القائمون على مؤتمر أمن المعلومات السنوى بمنطقة الشرق الأوسط وشمال أفريقيا ٢٠١٧ من أن المنطقة تواجه تحديات شديدة الأهمية تتعلق بتأمين المعلومات والبنية التحتية من الهجمات الإلكترونية التى يرتكبها القراصنة كالتخريب أو الابتزاز أو الاحتيال على ضحاياهم[٢٥]. وتشير التقارير إلى توالى حوادث اختراق الأنظمة وسرقة البيانات وتسربها، كاختراق أنظمة معلومات سونى، التى نتج عنها تسرب بيانات مليون مستخدم[٢٦].

ومما يزيد الأمر تعقيداً، ظهور ما يسمى بالويب العميق (Deep Web) والمعروف باسم الويب المظلم (Dark Web)، وهى شبكة خفية تستخدم فى

تعزيز الأنشطة الإجرامية الشنيعة[٢٧]. فمع تزايد أعداد المشتركين والمستخدمين للتقنية فى الوطن العربى، ارتفعت معدلات الجريمة الإلكترونية، وظهرت مجموعة من الظواهر السلبية الإلكترونية من قبيل التنمر والاحتيال والابتزاز الإلكترونى وغيرها من ممارسات تتسبب فى العديد من المشكلات الاجتماعية[٢٨]، فقد تطورت المعارك فى الفضاء الإلكترونى، حتى باتت أخطر على أمن الدول من المعارك المباشرة. كما كشفت دراسة حديثة أن أكثر من ٦٥٪ من خبراء تكنولوجيا المعلومات فى دول مجلس التعاون الخليجى يعتقدون أن المنطقة تشكل هدفاً رئيساً للجرائم الإلكترونية[٢٩].

وفى ضوء ما سبق يلاحظ أن الفضاء الإلكترونى أصبح يشكل خطرًا فى ظل انعدام الرقابة المهنية كعمليات الابتزاز من خلال طلب المال أو تنازلات تؤدى إلى إغراق الضحية. ولمحاربة كل أشكال الجريمة الإلكترونية من الابتزاز والفدية والتجسس والهجوم وغيرها يجب تطبيق سياسة الأمن السيبرانى وأنظمة الحماية البرمجية والمادية.

٢- استهداف الأمن القومى

يلاحظ أن التهديدات الأمنية قد ازدادت بطرق متسارعة لم يشهدها العالم من قبل حتى شملت السياحة والتجارة والاقتصاد، وطالت أمن الدول والمجتمعات. وفى هذا الخصوص، أشار تقرير صادر عن وكالة الأمن القومى الأمريكى إلى أن هناك ٢٣٢ جهاز حاسب آلى تتعرض لاختراقات وهجمات سيبرانية فى كل دقيقة على امتداد العالم مما أضاف صعوبة عالية فى المقدرة على اللحاق بمجرمى السيبر تقنياً وفنياً. كما أكدت الدراسات التى أصدرها الاتحاد الدولى للاتصالات (ITU) فى يوليو ٢٠١٧ أن هناك ضرورة ملحة فى مجالات التعليم والتدريب والدراسات لرفع مستوى المهارات والمعرفة فى الأمن[٣٠]. هذا إلى جانب إن هناك أربع فئات رئيسة للتهديدات السيبرانية للأمن القومى هى:

الحرب السيبرانية والتجسس الاقتصادى، وهما يرتبطان الى حد كبير بالدول، وفئة الجريمة السيبرانية، والإرهاب السيبرانى، اللذين يرتبطان فى الأغلب بجهات فاعلة غير تابعة لدولة معينة[٣١].

٣- تهديد القيم والأخلاق

ومـــن الأبعاد الاجتماعيـة الحمايـــة من تدنـــى المستويين القيمى والأخلاقى، فالمحتويات غير المشروعة وغير المرغوب بها ذات تأثير سلبى على أخلاقيات المجتمع وعلى ارتفاع نسبة الممارسات الإجرامية كالإباحية، والترويج للإتجار بالممنوعات، والدعارة، والإرهاب، والتجنيد لقضايا تمس الأمن والسلام الدوليين. وعليه، لا بد من بناء مجتمع مسئول، ومدرك لمخاطر الفضاء السيبيرانى، قادر على التعامل مع قواعد السلامة ومدرك للعواقب القانونية، التي يُمكن أن تترتب على التعرض لسلامة الأفراد والمؤسسات ورؤوس الأموال[٣٢].

٤- تدمير البنية التحتية

لا يشمل مفهـــوم الحـــرب السيبرانية استهـداف المقـدرات والأنظمة العسكرية وحسب، ولكن أيضًا استهداف البنية التحتية الحيوية للمجتمع- بما فى ذلك الشبكات الذكية وشبكات المراقبة الإشرافية وحيازة البيانات (SCADA)- التى تسمح لها بالعمل والدفاع عن نفسها[٣٣]. ومن ثَم يتمخض النزاع السيبرانى عن عواقب تُهدد الحياة إذا تم إفساد البنية التحتية للمعلومات.

ولذلك ورد فى تقرير(ITU ٢٠١٧) بالمؤتمر العالمى لتنمية الاتصالات فى مشروع الخطـة الاستراتيجية للاتحـاد "ضرورة وجود بنية تحتية حديثة وآمنة للاتصالات وتكنولوجيا المعلومات وضرورة تعزيز تنمية البنية التحتية والخدمات بما فى ذلك بناء الثقة والأمن فى استخدام الاتصالات و تكنولوجيا المعلومات. وضرورة وجود بيئة تمكينية وتعزيز بيئة تنظيمية وسياسات مؤاتية للتنمية المستدامة للاتصالات وتكنولوجيا المعلومات[٣٤]. وقد تواجه المجتمعات

خسائر اقتصادية واجتماعية فادحة إذا تعرضت شبكات اتصالاتها أو بنيتها التحتية الأخرى للهجوم والأعطال. وسوف يزيد التطور التكنولوجى من هذه الخسائر فى حالة عدم إيلاء اهتمام كافٍ بالأمن والبنية التحتية[٣٥]؛ إذ أن تنامى الاستغلال السيئ والمنحرف للشبكات الإلكترونية لتحقيق أهداف إجرامية، يُؤثر سلبًا على سلامة البنى التحتية للمعلومات، وهذا الخطر لا يقتصر فقط على المؤسسات، بل يطول أيضًا الأفراد على حساباتهم الخاصة للنيل منهم[٣٦].

٥- تصدير أزمة ثقة

إن المخاطر طويلة الأجل للمجتمع تُمثل عنصرًا جوهريًا يجب دراسته. فقد تستمر الهجمات لبضع ثوانٍ، ولكنها تُحدث آثاراً واسعة. وقد تتطلب الخسارة المجتمعية للثقة فى هذه الثوانى سنوات لإعادة بنائها. وتقويض الثقة بين المواطنين والشركات وبين الدول نفسها يمكن أن يولد آثاراً مدمرة على المجتمعات وعلى الاستقرار العالمى فى الأجل الطويل. ووقتها لا نستطيع أن نتحمل تكلفة الركود فى هذا المجال بسبب ضياع الثقة[٣٧]. ويرجع ذلك لأسباب من أهمها نقص الخبرة فى التعامل مع مثل هذه القضايا وقلة الوعى من قبل المستهدفين، مما يزيد فرص وجود الجرائم الإلكترونية بشكل كبير، ولمحاربتها يجب تطبيق سياسة الأمن السيبرانى[٣٨].

الأبعاد القانونية للأمن السيبرانى

١- الإطار التشريعى والإطار التنظيمى

تتمثل المخاطر القانونية، بشكل أساسى، فى غياب الإطارين التشريعى والتنظيمى المناسبين للتعامل مع نتائج الأعمال القانونية وغير القانونية منها، والتى تتم فى الفضاء السيبرانى. ويتطلب النشاط الاقتصادى والتجارى وغيرهما تحديدًا واضحًا، للواجبات والحقوق، فمستخدمو هذه التقنيات، عبر الفضاء

السيبرانى، بحاجة إلى إطـار يؤمّن حمايـة استخدامهم[٣٩]. ففى حالة غياب الأطر التشريعية تؤثر الجرائم السيبرانية على عمليات معلوماتية تخص حقوق الإنسان الدولية وتدفع على العنف وتُسبب ضرراً اقتصادياً خطيراً. فضمان إدارة مخاطر الأمن السيبرانى على نحو ممنهج يهدف إلى حماية الأصـول المعلوماتية والتقنية وفقًا للسياسات والإجـراءات التنظيمية والمتطلبات التشريعية.

٢- الأمن القانونى (عدم تناقض الأحكام والقوانين)

من هذا المنطلق، تتمثل المخاطر القانونية، فى غياب الأمن القانونى، أو حتى فى تناقض الأحكام والقوانين، وتنازع الأنظمة القانونية، فيؤدى إلى ارتفاع منسوب المخاطر، مع انعدام ملاحقة فاعلة، تتلاءم وطبيعة الأعمال والجرائم والاعتداءات السيبرانية، العابرة للحدود، وللأنظمة القانونية، بحيث تطال أى مواطن فى أية بقعة من الأرض، بما يطال الدول وأمنها واستقرارها[٤٠]. وتعد المخاطر التى يتعرض لها الأفراد والدول مخاطر هائلة وغير مقيدة بالأطر القانونية الجارية التى لا تستوعب العصر السيبرانى بالقدر الكافى. وهناك حاجة عاجلة إلى الخطى السريعة التى تُقيم بها البلدان القيادات السيبرانية وتوسع قدراتها العسكرية لتشمل النزاع السيبرانى، ويجب أن تتوازن بعدم تعارض للقوانين والتشريعات[٤١].

٣- التعاون الدولى

ونظراً لطبيعة مجتمع الفضاء السيبرانى العابرة للحدود، يعترف قطاع تنمية الاتصالات بأهمية التعاون الدولى فى تعزيز الموثوقية فى استخدام تكنولوجيات المعلومات والاتصالات وتوافر هذه التكنولوجيات وأمن استخدامها. وعليه، يعترف قطاع تنمية الاتـصـالات بالحـاجـة الملحـة لدعـم الـدول لوضـع تدابيـر محددة لتنفيذ أطرها الوطنية المتعلقة بالأمن السيبرانى من أجل معالجة شواغل أصحاب المصلحة المختلفين بهذا الشأن، ومن أجل إفساح المجال أمام

تبادل أفضل الممارسات على المستوى العالمى[٤٢]. ويمكن أن تصدر الهجمات السيبرانية من أى مكان، مما يجعل هذه التهديدات دولية بطبيعتها، وتتطلب التعاون الدولى والمساعدة فى التحقيق والأحكام الإجرائية والموضوعية المشتركة لمعالجتها على نحو ملائم. وإضافة إلى ذلك، من المعترف به على نطاق واسع أن التعاون الدولى يمثل أحد المتطلبات الرئيسة لضمان الأمن السيبرانى على الصعيد العالمى. وفى عامىَ ٢٠٠٣ و٢٠٠٥، اتفقت الدول فى القمة العالمية لمجتمع المعلومات (WSIS) على ضرورة وضع أدوات تتسم بالفعالية والكفاءة على المستويين الداخلى والخارجى للنهوض بالتعاون الدولى بشأن الأمن السيبرانى[٤٣]. ولذلك ينبغى أن يكون هذا التعاون، بدافع الرغبة المشتركة فى السلام، وبدافع المصلحة الفردية المستنيرة لكل بلد. وكذلك دعا المؤتمر الإقليمى الخامس للأمن السيبرانى والذى أعده المركز العربى الإقليمى (ITU-ARCC) التابع للاتحاد الدولى للاتصال، لتوحيد التعاون فى المنطقة العربية وتعزيز دور الاتحاد الدولى للاتصالات فى بناء الثقة والأمن على مستوى تقنية المعلومات والاتصالات فى المنطقة العربية والشرق الأوسط.

٤- استحداث اتفاقيات للمكافحة

عمدت الاتفاقية الأوروبية لمكافحة الجريمة السيبرانية، إلى إيراد ما تعده أعمالاً غير مشروعة، تحت عناوين تناولت، الجرائم ضد سرية الأنظمة والبيانات وسلامتها وتوفرها، والجرائم المتصلة بالأجهزة، والجرائم الخاصة بالمحتوى، والجرائم الخاصة بالملكية الفكرية[٤٤].

٥- إقرار سياسات وقائية ودفاعية

تمثل ذلك فى بناء الثقة والاطمئنان والأمن فى استعمال الاتصالات وتكنولوجيا المعلومات فضلاً عن حماية البيانات الشخصية وهى من الأولويات التى تستدعى تعاونًا وتنسيقًا دوليين بين الحكومات والمنظمات ذوات الصلة

وشركات القطاع الخاص والكيانات المعنية فى مجال بناء القدرات وتبادل أفضل الممارسات من أجل وضع السياسات العامة والتدابير القانونية والتنظيمية والتقنية التى تتناول حماية البيانات الشخصية، لضمان موثوقية وأمن شبكات وخدمات تكنولوجيا المعلومات والاتصالات[٤٥]؛ ولذلك اتجهت معظم الدول المتقدمة، إلى إقرار سياسات وقائية ودفاعية، ضد الهجمات السيبرانية، وخصصت بعض الدول مثل الولايات المتحدة الأمريكية[٤٦]. وأستراليا وانجلترا، مبالغ طائلة، لمعالجة مسائل الأمن السيبرانى. وليست هذه الحقيقة، سوى مؤشر، إلى مدى الاهتمام الذى توليه هذه الدول، لإرساء الثقة والاستقرار، فالعلاقات الدولية، مهددة فى كل لحظة نتيجة الاختراقات والاعتداءات على الشبكة العالمية للمعلومات، وعلى الأنظمة المعلوماتية، وقواعد المعلومات. ولم تتأخر الإدارة الأمريكية، عن استحداث قيادة عسكرية جديدة، مختصة بأمن الفضاء السيبرانى[٤٧]. وقد اقترح الاتحاد الدولى للاتصالات بالفعل عملية كاملة لوضع خطة وطنية للأمن السيبرانى وتنفيذها [ICEGOV1]. ولكن هذه العملية تتطلب استراتيجية شاملة تتضمن استعراضًا أوليًا واسعًا لمدى ملاءمة الممارسات الوطنية[٤٨].

٦- إنشاء وحدات خاصة للمكافحة

كثُرت النشاطات العسكرية فى هذا المجال، والتى تشمل الحماية، والقيام بمناورات مكامن الضعف، والتدريب على آليات الرد. ويتم ذلك، فى إطار استراتيجية أعدتها وزارة الدفاع الإنجليزى فى عام ٢٠١١ حول كيفية العمل فى الفضاء السيبرانى[٤٩]. وكان رئيس الوزراء، "جوردن براون"، قد أعلن عن إنشاء وحدة خاصة، لمكافحة الجريمة السيبيرانية[٥٠]. وعلى نفس النهج أنشأت مصر وحدة لطوارئ الإنترنت والحاسب الآلى ٢٠١٢ وتسمى (CERT).

٧- تنفيذ القوانين وفاعلية التشريعات

يأتى فى هذا الإطار، تقاعس الإدارات أو عجزها، حتى عن تنفيذ القوانين التى وضعت آليات تنفيذها، كما هو الحال مثلا، مع قوانين حماية الملكية الفكرية والأدبية، حيث تنتشر ظاهرة قرصنة البرامج، بشكل كثيف، فى مختلف الدول العربية. ويعود ذلك، إما لغياب إدارة متخصصة بالملاحقة، وإما لعدم إمكانية الإدارة المعنية، متابعة الوضع بشكل فاعل، نتيجة عدم توافر الإمكانات التقنية، والمادية والبشرية. وغياب القدرة على الضبط والتحقيق، ورغم إنشاء عدد من مراكز الاستجابة لطوارئ الإنترنت، فى البلدان العربية، فإن بعضها مازال غير فاعل بشكل كاف(٥١). كما أن القوانين المنسقة بشأن الجريمة السيبرانية تنهض بالتحقيقات وتقديم المجرمين السيبرانيين إلى القضاء. ويتعين القيام بالكثير من العمل فى كل مجال من هذه المجالات(٥٢).

وفى ضوء عرض المخاطر والتهديدات التى يتعرض لها الأمن السيبرانى ببعديه الاجتماعى والتشريعى، يُمكن الاسترشاد بكيفية التغلب على هذه التهديدات من خلال نتائج المبادرة الأفريقية والتى جاء فيها "ضرورة مساعدة الدول الأعضاء على وضع وتنفيذ سياسات واستراتيجيات ومعايير وآليات لتحسين أمن نظم وشبكات المعلومات، وحماية البيانات والأشخاص وضمان الثقة الرقمية. وحماية البنية التحتية لتكنولوجيا المعلومات والاتصالات وبناء الثقة فى استعمال تكنولوجيا المعلومات والاتصالات وتطبيقاتها"، حيث كانت النتائج المتوقعة هى(٥٣): ضمان تحقيق هدف برنامج التوصيل ٢٠٢٠ لتحسين التأهب فى مجال الأمن السيبرانى بنسبة ٤٠٪ فى عام ٢٠٢٠، ومساعدة الدول الأعضاء على تقييم وتكييف الأطر التشريعية والتنظيمية على أساس الاستخدام الأفضل للتقرير الصادر عن الاتحاد بشأن الرقم القياسى العالمى للأمن السيبرانى (CGI). والتشجيع على وضع إطار عالمى للتعاون

والتوعية على الصعيدين الإقليمى والوطنى من أجل إرساء ثقافة عالمية للأمن السيبرانى ومساعدة المستهلكين على فهم المخاطر والوقاية منها بشكل أفضل. وكذلك المساعدة فى توعية المستهلكين فى مجال التجارة الإلكترونية والمعاملات المتنقلة وإطلاعهم على التشريعات المالية للمعاملات الإلكترونية ونظم الدفع المتنقلة. وتشجيع وضع آليات مؤسسية وتنظيمية على الصعيدين الوطنى والإقليمى لتيسير التنفيذ الفعّال لاستراتيجيات الأمن السيبرانى. ووضع تدابير لحماية المستهلكين والأطفال والأشخاص الضعفاء الآخرين لدى استعمالهم تكنولوجيات المعلومات والاتصالات. وإذكاء الوعى بالتهديدات السيبرانية وتدابير الأمن السيبرانى. واعتماد تدابير لحماية الخصوصية والبيانات الشخصية. ووضع استراتيجية منسقة لتحسين أمن المعلومات ومكافحة التهديدات السيبرانية. ونستدل مما سبق على سبل المواجهة.

٨- الحماية من المخاطر الاجتماعية والقانونية للأمن السيبرانى

إذا كانت أسباب التهديدات تنحصر فى جهل الأفراد وعدم إدراكهم أولاً، ثم غياب تدابير الحماية ثانياً فيمكننا تقديم سبل الحماية كالتالى:

نشر ثقافة الأمن السيبرانى: (**إذكاء الوعى بالأمن السيبرانى**)

تعترف حكومات عديدة بأن التعليم العام وتوعية الجمهور من الأساليب القوية للدفاع السيبرانى. وتساعد قواعد بيانات المعلومات وبرامج التوعية الوطنية التى تنفذها الحكومة أو الكيانات الخاصة على تعزيز الوعى على مستوى القاعدة الجماهيرية، فعلى سبيل المثال: تشرف لجنة الحاسوب الوطنى فى موريشيوس، تحت ولاية وزارة تكنولوجيا المعلومات والاتصالات، على بوابة لإذكاء الوعى بالأمن السيبرانى[٥٤]، **وكذلك** تنظم الولايات المتحدة شهرًا لتنمية الوعى بالأمن السيبرانى القومى فى أكتوبر من كل سنة. كما أن الشراكات بين القطاعين العام والخاص، مثل التحالف الأمريكى للأمن

السيبرانى القومى، تعلّم المستعملين والمديرين للبنية التحتية الرقمية كيفية إقامة أنظمة مرنة وآليات وقائية[٥٥]. فعلى سبيل المثال، تم التسلل إلى القيادة المركزية الأمريكية بواسطة مفتاح ذاكرة مصاب بفيروس ٢٠٠٨ "Fifth Domain". ومن ثَم توجد ضرورة لضمان التأكد على التوعية الأمنية اللازمة فى مجال الأمن السيبرانى.

البرامج والإعلانات العالمية

- **برنامج الأمن السيبرانى العالمى ٢٠٠٧**": وهو إطار للتعاون الدولى يهدف إلى تعزيز الثقة والأمن فى مجتمع المعلومات ويهدف لتحقيق خمس ركائز لتوجيه مجالات أنشطته وهى: التدابير القانونية- التدابير الإجرائية والتقنية- الهياكل التنظيمية- بناء القدرات- التعاون الدولى[٥٦].
- **إعلان إيريتشى لمبادئ الاستقرار والسلام السيبرانى ٢٠٠٩**[٥٧]: وهو إعلان يدعو إلى تضافر العمل والترويج لمفهوم السلام السيبرانى العالمى **ويدعو** لما يلى:

- فحص الطريقة التى تعمل بها تكنولوجيا المعلومات والاتصالات على دعم الحياة اليومية.
- تقييم التهديدات السيبرانية.
- تحليل آثار الجريمة السيبرانية والنزاع السيبرانى.
- تقييم صحة الأطر القانونية الجارية.
- تعريف مفهوم السلام السيبرانى.
- رسم مسار العمل فى المستقبل.

وبذا، يعد إعلان إريتشى إنجازًا علميًا؛ إذ يصبح بحوزة البشرية الوسائل اللازمة لبسط الموارد الاقتصادية للدول وتعزيز القدرات الفكرية لمواطنيها،

وتطوير ثقافتهم وبناء ثقتهم فى مجتمعات أخرى بفضل تكنولوجيا المعلومات والاتصالات.

البعد التحليلى لركائز وممارسات الأمن السيبرانى فى مصر

التحليل فى ضوء المستويات الكبرى : تحليل مؤشر الاستعداد للأمن السيبرانى فى تقرير (ITU) ٢٠١٧ ووضع مصر عالميًا وإقليميًا.

وحسب هذا التقرير جاء ترتيب مصر عالميًا وعربيًا كالآتى:

الدولة	عربيًا	عالميًا
عُمان	١	٤
مصر	٢	١٤
قطر	٣	٢٥
تونس	٤	٤٠
السعودية	٥	٤٦
الإمارات	٦	٤٧
المغرب	٧	٤٩
البحرين	٨	٦٥
الجزائر	٩	٦٨
الأردن	١٠	٩٣
السودان	١١	٩٦
سوريا	١٢	١٠٢
فلسطين	١٣	١٠٤
ليبيا	١٤	١٠٥
لبنان	١٥	١١٩
موريتانيا	١٦	١٢٥
الكويت	١٧	١٣٩
جيبوتى	١٨	١٤٠
العراق	١٩	١٥٩
جزر القمر	٢٠	١٦١
الصومال	٢١	١٦٥
اليمن	٢٢	١٦٤

لقد أبدت مصر استعدادها فى مجال الأمن السيبرانى عام ٢٠١٧، حيث أصدر الاتحاد الدولى للاتصالات تقرير مؤشر قياس استعداد الدول فى هذا المجال من أجل دفع المزيد من الجهود فى مجال اعتماد الأمن السيبرانى وتكامله على نطاق عالمى، وقد تقدمت سنغافورة والولايات المتحدة الأمريكية وماليزيا وعمان وأستونيا وموريشيوس واستراليا وجورجيا وفرنسا وكندا وروسيا.

كما جاءت مصر فى المرتبة الرابعة عشرة من بين ١٩٣ دولة من دول أعضاء الاتحاد. وكذلك جاءت فى المرتبة الثانية عربيًا فيما يتعلق بمستويات الالتزام بالأمن السيبرانى بعد سلطنة عمان التى جاءت فى المركز الرابع عالمياً والأول عربياً.

أكد التقرير على أن مصر لديها استعداد قوى فى مجال الأمن السيبرانى من خلال هيكلة بنية تحتية وتبنيها استراتيجيات وطنية فى هذا المجال، كما عقدت اتفاقيات عديدة دعت من خلالها لتبادل الخبرات ونشر ثقافة الوعى بالأمن السيبرانى من خلال تبنيها سياسات وطنية، كما أن لديها الكثير من المبادرات والملتقيات والمنتديات وتدشين مؤتمرات واتفاقيات فى مجال الأمن السيبرانى، وقد تغلبت مصر بذلك على أزمات الثقة التى تهدد انتشار ثقافة الأمن السيبرانى محليًا وعالميًا من خلال خمسة معايير حددها مؤشر قياس ITU هى: الإمكانات (التقنية – التنظيمية– القانونية– التعاون– إمكانات النمو).

١- التحليل فى ضوء المستويات الوسطى: مظاهر اهتمامات مصر بقضايا الأمن السيبرانى خلال العشر سنوات الأخيرة

التاريخ	نوع الاهتمام والمشاركة
أبريل ٢٠٠٩	تأسس المركز المصرى للاستجابة لطوارئ الإنترنت والحاسب الآلى (سيرت).
يوليو ٢٠٠٩	إتاحة خدمة الرصد والاستجابة للحوادث على مدار ٢٤ ساعة يومياً طوال الأسبوع.
٢٠١٢	المشاركة فى التدريبات السيبرانية العملية التى نظمها فريق الاستجابة لطوارئ الحاسوب بآسيا والمحيط الهادى (APCERT)، وفريق الاستجابة لطوارئ الحاسوب التابع لمنظمة المؤتمر الإسلامى (OICCERT)، والاتحاد الدولى للاتصالات (ITU). كما عقدت مصر اتفاقيات تعاون مع فريق الطوارئ للحاسوب بالولايات المتحدة (US-CERT)، ووكالة أمن الإنترنت الكورية (KISA) فى مدينة سيول، والهيئة الماليزية للأمن السيبرانى.
٢٠١٢	تنظيم البعثات الخاصة إلى فنلندا وأستونيا لاستكشاف فرص التعاون فى مجال الأمن السيبرانى من خلال فرق الاستجابة لطوارئ الحاسوب وفى مجال التوقيع الإلكترونى.
٢٠١٢	عرض إطار الأمن السيبرانى المصرى فى واحدة من الجلسات الرئيسية لمنتدى حوكمة الإنترنت ٢٠١٢ فى أذربيجان
أكتوبر ٢٠١٢	المشاركة فى مؤتمر بودابيست للفضاء الإلكترونى فى المجر ٢٠١٢.
ديسمبر ٢٠١٢	بدء تشغيل خدمة اختبار الاختراق.
مارس ٢٠١٣	تم تدشين المركز العربى الإقليمى للأمن السيبرانى (ITU-ARCC) حيث أسهمت مصر بدور حيوى فى أعمال المركز.
مايو ٢٠١٣	تنظيم ورشة العمل الأولى للأمن السيبرانى فى القرية الذكية تحت رعاية الجهاز القومى لتنظيم الاتصالات لمناقشة قضايا الأمن السيبرانى.
أكتوبر ٢٠١٣	احتل المركز المصرى للاستجابة لطوارئ الإنترنت المرتبة الثالثة حسب مؤشر الأمن السيبرانى العالمى للإتحاد الدولى للاتصالات.
ديسمبر ٢٠١٣	افتتاح مبنى المركز المصرى للاستجابة للطوارئ المعلوماتية الجديد (CERT).
٢٠١٤	انضمت مصر إلى اتفاقية الاتحاد الأفريقى بشأن أمن الفضاء الإلكترونى وحماية البيانات ذات الطابع الشخصى.

ديسمبر ٢٠١٤	احتلت مصر المركز ٢٧ من بين ١٩٣ دولة وفقاً لما جاء فى مؤشر قياس استعدادات الدول فى مجال الأمن السيبرانى الذى أصدره الاتحاد الدولى للاتصالات وشركة (API).
ديسمبر ٢٠١٤	تم تشكيل المجلس الأعلى للأمن السيبرانى فى مصر.
يونيو ٢٠١٥	أعلنت غرفة صناعة تكنولوجيا المعلومات والاتصالات عن ٤ محاور لبحث مستقبل تطوير وتنمية أمن المعلومات فى مصر لتكون أول استراتيجية موحدة فى مجال الأمن السيبرانى.
نوفمبر ٢٠١٦	استضاف الجهاز القومى لتنظيم الاتصالات المؤتمر الإقليمى الخامس للأمن السيبرانى ومنتدى (FIRST) فرست الإقليمى للمنطقة العربية والإفريقية لتأكيد تبادل الخبرات والتعاون.
نوفمبر ٢٠١٦	النسخة– الدورة – السابعة من مؤتمر القاهرة للأمن الإلكترونى بمشاركة خبراء من جميع أنحاء العالم.
٢٠١٦	توقيع اتفاقية تعاون بين المعهد القومى للاتصالات التابع لوزارة الاتصالات وتكنولوجيا المعلومات وشركة سيسكو العالمية.
أبريل ٢٠١٧	نظمت سايبر تالنش مسابقة أمن المعلومات الوطنية المصرية بالقاهرة برعاية شركة (TREND MICRO).
أبريل ٢٠١٧	شاركت مصر فى مؤتمر المنطقة المركزية للاتصالات الذى استضافته القياده المركزية الأمريكية فى واشنطن لتبادل وجهات النظر فى استراتيجيات الأمن السيبرانى الوطنية ومبادرات تكنولوجية المعلومات.
يونيه ٢٠١٧	احتلت مصر المركز ١٤ عالمياً والثانى إفريقياً وعربياً فى مؤشر قياس استعدادات الدول فى مجال الأمن السيبرانى الذى أصدره الاتحاد الدولى للاتصالات (ITU).
نوفمبر ٢٠١٧	فاز الفريق المصرى بالمركز الأول فى المسابقة الدولية TREND MICRO CTF COMPETITION فى اليابان والتى تنافس فيها مع فرق من اليابان وكوريا الجنوبية وبولندا وإسرائيل ورومانيا وتايوان وروسيا.
نوفمبر ٢٠١٧	شاركت مصر فى المنتدى الإقليمى للاتحاد الدولى للاتصالات ومنظمة فرست، وورشة عمل لتقييم الجاهزية للاستجابة للطوارئ المعلوماتية للمنطقة العربية والإفريقية.

نوفمبر ٢٠١٧	شاركت مصر فى المؤتمر الإقليمى السادس للأمن السيبرانى بعمان والذى نظمه الاتحاد الدولى للاتصالات (ITU).
ديسمبر ٢٠١٧	اطلاق أول أكاديمية للأمن السيبرانى فى مصر لتثقيف وتطبيق مهارات التعامل مع تحديات الأمن السيبرانى.
أبريل ٢٠١٨	شاركت مصر فى مؤتمر اختراقات الأمن السيبرانى (HITB).
يوليو ٢٠١٨	شاركت مصر فى مؤتمر قمة إفريقيا للدفاع السيبرانى.
أغسطس ٢٠١٨	شاركت مصر فى مؤتمر فى اجتماع لجنة الدراسات ١٧ التابعة للاتحاد الدولى للاتصالات (ITU).
أكتوبر ٢٠١٨	شاركت مصر فى المؤتمر الإقليمى السابع للأمن السيبرانى ٢٠١٨.
سبتمبر ٢٠١٨	نظم مركز المعلومات ودعم القرار بمجلس الوزراء جلسة نقاشية بعنوان:الأمن السيبرانى وحماية الهوية المصرية فى البيئة الرقمية الحديثة.
ديسمبر ٢٠١٨	المجلس الأعلى للأمن السيبرانى يطلق الاستراتيجية الوطنية للأمن السيبرانى (٢٠١٧-٢٠٢١).
فبراير ٢٠١٩	ماستر كارد تنظم أول منتدى حول الأمن السيبرانى فى القاهرة.
مارس ٢٠١٩	غرفة تكنولوجيا المعلومات والاتصالات تنظم المؤتمر السنوى الخامس للأمن السيبرانى.

مما سبق يتضح أن مجال الأمن السيبرانى فى مصر **جاء محتويًا على بنية تحتية** تضمن استقرار وسلام الأمن السيبرانى والتى تمثلت فى تأسيس المركز المصرى للاستجابة لطوارئ الإنترنت والحاسب ٢٠٠٩، ثم افتتاح مبنى المركز المصرى للاستجابة للطوارئ المعلوماتية الجديد (CERT) ٢٠١٣، ثم إنشاء المجلس الأعلى للأمن السيبرانى ٢٠١٤، كما تم إطلاق أول أكاديمية للأمن السيبرانى فى مصر لتثقيف وتطبيق مهارات التعامل مع تحديات الأمن السيبرانى ٢٠١٧.

كما اتضح أيضًا مؤشرات تضمن سلامة **واستقرار الأمن القومى** مثل إتاحة خدمة الرصد والاستجابة للحوادث على مدار ٢٤ ساعة يوميًا طوال الأسبوع وتشغيل خدمة اختبار الاختراق.

أيضًا توجد مؤشرات **للتعاون الدولى والإقليمى** ومنها أن مصر شاركت فى مؤتمر بودابيست للفضاء الإلكترونى فى المجر ٢٠١٢، وشاركت أيضاً فى التدريبات السيبرانية العملية التى نظمها فريق الاستجابة لطوارئ الحاسوب بآسيا والمحيط الهادى (APCERT)، وفريق الاستجابة لطوارئ الحاسوب التابع لمنظمة المؤتمر الإسلامى (OICCERT)، والاتحاد الدولى للاتصالات (ITU) كما عقدت مصر اتفاقيات تعاون مع فريق الطوارئ للحاسوب بالولايات المتحدة (US-CERT)، ووكالة أمن الإنترنت الكورية (KISA) فى مدينة سيول، والهيئة الماليزية للأمن السيبرانى ٢٠١٢، وقد تم تدشين المركز العربى الإقليمى للأمن السيبرانى (ITU-ARCC) حيث أسهمت مصر بدور حيوى فى أعمال المركز ٢٠١٣، وفى ٢٠١٤ انضمت مصر إلى اتفاقية الاتحاد الإفريقى بشأن أمن الفضاء الإلكترونى وحماية البيانات ذات الطابع الشخصى. أما فى عام ٢٠١٦، فقد تم توقيع اتفاقية تعاون بين المعهد القومى للاتصالات التابع لوزارة الاتصالات وتكنولوجيا المعلومات وشركة سيسكو العالمية فضلاً عن مشاركتها فى المنتدى الإقليمى للاتحاد الدولى للاتصالات ومنظمة فرست، وورشة عمل لتقييم الجاهزية للاستجابة للطوارئ المعلوماتية للمنطقة العربية والإفريقية ٢٠١٧، وأيضًا شاركت مصر فى مؤتمر المنطقة المركزية للاتصالات الذى استضافته القيادة المركزية الأمريكية فى واشنطن لتبادل وجهات النظر فى استراتيجيات الأمن السيبرانى الوطنية ومبادرات تكنولوجية المعلومات ٢٠١٧، وكذلك شاركت مصر فى المؤتمر الإقليمى السادس للأمن السيبرانى بعمان والذى نظمه الاتحاد الدولى للاتصالات (ITU) ٢٠١٧، ثم شاركت فى مؤتمر اختراقات الأمن السيبرانى (HITB) ٢٠١٨، وبعدها شاركت فى مؤتمر قمة إفريقيا للدفاع السيبرانى فى اجتماع لجنة الدراسات التابعة للاتحاد الدولى

للاتصالات (ITU) ٢٠١٨، وتتبع ذلك مشاركتها فى المؤتمر الإقليمى السابع للأمن السيبرانى ٢٠١٨.

وفى مجال إذكاء الوعى السيبرانى نظمت مصر البعثات الخاصة إلى فنلندا وأستونيا لاستكشاف فرص التعاون فى مجال الأمن السيبرانى من خلال فرق الاستجابة لطوارئ الحاسوب وفى مجال التوقيع الإلكترونى، وكذلك عرضت إطار الأمن السيبرانى المصرى فى واحدة من الجلسات الرئيسة لمنتدى حوكمة الإنترنت ٢٠١٢ فى أذربيجان، وقد نظمت مصر ورشة العمل الأولى للأمن السيبرانى فى القرية الذكية تحت رعاية الجهاز القومى لتنظيم الاتصالات لمناقشة قضايا الأمن السيبرانى ٢٠١٣، كما استضاف الجهاز القومى لتنظيم الاتصالات المؤتمر الإقليمى الخامس للأمن السيبرانى ومنتدى (FIRST) فرست الإقليمى للمنطقة العربية والإفريقية ٢٠١٦، أيضًا أقامت مصر النسخة– الدورة– السابعة من مؤتمر القاهرة للأمن الإلكترونى بمشاركة خبراء من جميع أنحاء العالم ٢٠١٦، كما نظمت سايبر تالنش مسابقة أمن المعلومات الوطنية المصرية بالقاهرة برعاية شركة (TREND MICRO)، نظم مركز المعلومات ودعم القرار بمجلس الوزراء سبتمبر ٢٠١٨ جلسة نقاشية بعنوان: الأمن السيبرانى وحماية الهوية المصرية فى البيئة الرقمية الحديثة. وقد سمحت مصر لماستر كارد بتنظيم أول منتدى حول الأمن السيبرانى فى القاهرة ٢٠١٩، وكذلك نظمت غرفة تكنولوجيا المعلومات والاتصالات المؤتمر السنوى الخامس للأمن السيبرانى ٢٠١٩.

وفى مجال القضاء على أزمة الثقة احتلت مصر المركز ٢٧ من بين ١٩٣ دولة وفقاً لما جاء فى مؤشر قياس استعدادات الدول فى مجال الأمن السيبرانى الذى أصدره الاتحاد الدولى للاتصالات وشركة (API) ٢٠١٤، ثُم ازدادت الثقة عندما احتلت مصر المركز ١٤ عالمياً والثانى إفريقياً وعربياً فى

مؤشر قياس استعدادات الدول فى مجال الأمن السيبرانى الذى أصدره الاتحاد الدولى للاتصالات (ITU) ٢٠١٧. كما فاز الفريق المصرى بالمركز الأول فى المسابقة الدولية (TREND MICRO CTF COMPETITION) فى اليابان ٢٠١٧ والتى تنافس فيها مع فرق من اليابان وكوريا الجنوبية وبولندا وإسرائيل ورومانيا.

وفى مجال رسم سياسة استراتيجية للأمن السيبرانى أعلنت غرفة صناعة تكنولوجيا المعلومات والاتصالات ٢٠١٥ عن أربعة محاور لبحث مستقبل تطوير وتنمية أمن المعلومات فى مصر لتكون أول استراتيجية موحدة فى مجال الأمن السيبرانى، وفى ٢٠١٨ أطلق المجلس الأعلى للأمن السيبرانى الاستراتيجية الوطنية (٢٠١٧-٢٠٢١) وتهدف إلى تأمين البنى التحتية للاتصالات والمعلومات وتوفير بيئة آمنة لمختلف القطاعات لتقديم الخدمات الإلكترونية المتكاملة، وذلك فى إطار جهود الدولة لدعم الأمن القومى وتنمية المجتمع المصرى.

٢- التحليل فى ضوء المستويات الصغرى

القانون المصرى لتقنية المعلومات

بالنسبة للإطارين التشريعى والقانونى فى مجال الأمن السيبرانى المصرى: جدير بالذكر وجود إطار تشريعى فى مجال الأمن السيبرانى المصرى وإن كان ضعيفاً قبل إصدار قانون تقنية المعلومات ٢٠١٨، إلا أنه كان موجوداً متمثلاً فى قانون الاتصالات رقم ١٠ لسنة ٢٠٠٣، وقانون التوقيع الإلكترونى رقم ١٥ لسنة ٢٠٠٤، وقانون حماية المستهلك رقم ٦٧ لسنة ٢٠٠٦ وقرار جمهورى رقم ٢٧٦ لسنة ٢٠١٤ بشأن انضمام مصر للاتفاقية العربية لمكافحة الجرائم التقنية، وكذلك تم التأكيد على أن أمن الفضاء المعلوماتى جزء من الأمن

القومى فى المادة ٣١ من دستور ٢٠١٤، ثم جاء قانون تقنية المعلومات رقم ٢٠١٨ لتشهد مصر حراكًا قويًا فى مجال آمن المعلومات.

ب- تحليل قانون تقنية المعلومات[٥٨] فى ضوء الأبعاد الاجتماعية والتشريعية

فى مجال البنية التحتية جاء الباب الأول فى المادة الأولى بتعريف الجهاز (الجهاز القومى لتنظيم الاتصالات)، تحديد جهات الأمن القومى. **وفى مجال التعاون الدولى والاتفاقيات والسياسات،** جاءت المادة الرابعة لتحث على تيسير التعاون بالبلاد الأجنبية فى إطار الاتفاقيات الدولية والإقليمية. **أما فى مجال إذكاء الوعى السيبرانى،** فقد ورد فى الباب الثانى فى المادتين العاشرة والحادية عشرة أهمية الخبراء التقنيين والفنيين فى تقديم الأدلة الرقمية من الوسائط والدعامات الإلكترونية، والأخذ بحجية الأدلة التقنية والفنية فى المجال المعلوماتى بنفس قيمة حجية الأدلة الجنائية.

وفى مجال مجابهة الخطورة المجتمعية والتهديدات السيبرانية المستحدثة (الابتزاز- الغش- التنمر- الإرهاب- العنف... إلخ) عالج الباب الثالث أزمة الثقة التى يمكن أن تُهدد الأمن السيبرانى وتجلى ذلك فيما ورد بشأن الجرائم والعقوبات ويمكن تحليلها من خلال

- الجرائم المستحدثة.
- العقوبات.

أما عن الجرائم السيبرانية، فقد جاءت المواد (١٣ إلى ٢٦) على التوالى تخص جرائم مستحدثة، هى الانتفاع بدون وجه حق بخدمات الاتصال والمعلومات، تجاوز حدود الحق فى الدخول، الدخول غير المشروعة، الاعتراض غير المشروع، الاعتداء على سلامة البيانات والمعلومات والنظم، الاعتداء على البريد أو الموقع أو الحسابات الخاصة، الاعتداء على تصميم موقع، الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة، الاعتداء على

سلامة الشبكة المعلوماتية، تداول البرامج والأجهزة والمعدات المستخدمة فى تقنية المعلومات، الاحتيال والاعتداء على بطاقات البنوك وخدمات الدفع الإلكترونى، اصطناع مواقع وحسابات خاصة وبريد إلكترونى، الاعتداء على حرمة الحياة الخاصة والمحتوى المعلوماتى، تعمد استعمال برنامج أو تقنية معلوماتية فى معالجة معطيات شخصية للغير.

وأما عن العقوبات، فقد تنوعت بين الحبس أو الغرامة أو الحبس والغرامة معاً، وقد وردت فى باب الجرائم والعقوبات بحد أدنى للحبس مدة لا تقل عن شهر وبحد أقصى مدة لا تزيد على خمس سنوات، أما الغرامة فوردت بحد أدنى ١٠ آلاف جنيه وبحد أقصى ٥٠٠ ألف جنيه ولكن فى حالة إتلاف أو تدمير أو إلغاء أو تعديل أو نسخ البيانات أو المعلومات تكون الغرامة بحد أدنى مليون جنيه وبحد أقصى خمسة ملايين جنيه. ويمكن تضمين العقوبات الحبس والغرامة معًا أو إحداهما فقط.

جـ- تحليل جهود الفاعلين "المسئولين والقائمين" على الأمن السيبرانى

تضمن **خطاب الدكتور عمرو طلعت** وزير الاتصالات وتكنولوجيا المعلومات خلال المؤتمر العربى لأمن المعلومات ٢٠١٨[٥٩] "أن مصر تشهد حراكًا قويًا فى مجال الأمن السيبرانى والذى تمثل فى الاتفاقيات والتعاون الدولى وتخفيف سلبيات اختراق أمن المعلومات على الأمن القومى وميكنة الخدمة الإلكترونية والبنية السيبرانية" مما كان له أبلغ الأثر فى تحسين مؤشر جاهزية مصر فى مواجهة التهديدات الإلكترونية واستعدادها لإدارة الحوادث السيبرانية، حيث وصلت مصر للمرتبة ١٤ للعام ٢٠١٧ بين الدول البالغ عددها ١٩٤. وترتب على ذلك أن مصر شهدت انخفاضًا ملحوظًا فى معدل قرصنة البرمجيات بنسبة نقطتين مئويتين لتصل إلى ٥٩٪ وفقًا لما أفاد به الاتحاد العالمى لمنتجى البرمجيات التجارية (BSA) فى أحدث دراسة أصدرها ٢٠١٨[٦٠]. كما

يرى أن قانون تقنية المعلومات قد غطى مجموعة من الجرائم التى تستهدف المواطنين والاستثمار والجهات الحكومية والخاصة، حيث يضع حجية فى الأدلة الرقمية مما يضمن الوصول لمرتكبى الجرائم الإلكترونية وحماية المواطنين وتشجيع الاستثمار.

ولقد جاء فى **خطاب الدكتور محمد حجازى** "رئيس لجنة التشريعات والقوانين بوزارة الاتصالات وتكنولوجيا المعلومات "خلال جلسة نقاشية بعنوان: قانون مكافحة تقنية المعلومات بمركز المعلومات التابع لمجلس الوزراء سبتمبر ٢٠١٨": أن قانون مكافحة جرائم تقنية المعلومات لا يهدف إلى مراقبة المواطنين أو اختراق حسابات شخصية أو الحياة العامة، بل يهدف إلى حماية المواطنين والحسابات الشخصية على مواقع التواصل الاجتماعى، وقد استدل بأن هناك ١٤٥ دولة فى العالم لديها هذا القانون وأن مصر من أواخر الدول العربية إصدارًا لهذا القانون بعد السودان". وأن القانون ليس له علاقة بحرية التعبير والرأى، ولا يمكن حجب المواقع إلا بأمر قضائى.

كما جاء فى خطاب الدكتورولىد حماد الرئيس التنفيذى لشركة PROOXC فى تصريحه لجريدة "اليوم السابع" سبتمبر ٢٠١٨ خلال نفس الجلسة النقاشية، أن أمن المعلومات فى مصر جزء لا يتجزأ من الأمن القومى المصرى مشيرًا إلى أن مصر فى المرتبة رقم ٣٩ بين الدول الأكثر استهدافًا على مستوى العالم.

وفى خطاب المهندس زياد عبد التواب "رئيس مركز المعلومات ودعم اتخاذ القرار بمجلس الوزراء" خلال ندوة بعنوان: الحرية فى عصر المعلوماتية على هامش معرض القاهرة الدولى للكتاب ٢٠١٩. نجد أن حجم الجرائم الإلكترونية فى مصر ٢٠١٢: ٢٠١٧ زاد إلى ١٩٠٪. الأمر الذى استدعى ضرورة العمل بقانون مكافحة تقنية المعلومات الذى يضم ١٤٥ مادة.

النتائج والاستخلاصات

يتضح مما سبق أن ممارسات الأمن السيبرانى للتغلب على المخاطر الاجتماعية والقانونية فى مصر جاءت قوية ذات شواهد وبراهين ودلالات أدت إلى وجود تقارير عالمية وتصريحات محلية بهذا الشأن وتجسدت فى الآتى:

- ارتكز الأمن السيبرانى فى ضوء الأبعاد الاجتماعية على بنية تحتية تمثلت فى استحداث مركز الطوارئ (CERT) واستمرار الخدمة فيه ٢٤ ساعة، وكذلك إنشاء المجلس الأعلى للأمن السيبرانى الذى خضع لوزارة الاتصالات. ومن قبل وجود غرفة صناعة تكنولوجياالمعلومات والاتصالات، ومركز معلومات بمجلس الوزراء، وهذا قطعًا ينعكس على الأمن القومى.
- من مؤشرات الأمن السيبرانى فى مصر وجود استراتيجية وطنية قوية أطلقها المجلس الأعلى للأمن السيبرانى ٢٠١٨.
- نظمت مصر العديد من المؤتمرات والمنتديات وأطلقت كثيرًا من المبادرات بشأن الأمن السيبرانى.
- شاركت مصر فى اتفاقيات تعاون كثيرة مع العديد من الدول حول الأمن السيبرانى.
- احتلت مصر مراكز متقدمة ونالت جوائز متعددة ما جعلها تتغلب على أزمات الثقة.
- رغم الخطورة الاجتماعية فى الفضاء السيبرانى وتهديدات الجرائم المستحدثة، فإنه قد بات هناك إطار تشريعى للأمن السيبرانى فى غالبية الدول والتى تجسد فى مصر فى القانون رقم ١٧٥ /٢٠١٨ لمكافحة تقنية المعلومات.
- تضمن القانون ١٧٥لسنة ٢٠١٨ ٤٥ مادة لمكافحة جرائم تقنية المعلومات، وجاء متضمنًا العقوبات المستحقة للجرائم المستحدثة التى تعيق الأمن

السيبرانى، وتضمن مادة للتظلم من إجراءات الحجب حيث يتيح التظلم أمام دائرة قضائية أخرى. ومن ثَم ليس له علاقة بحرية الرأى والتعبير.

- جاء فى خطاب الفاعلين للأمن السيبرانى أن مصر فى مراحل متقدمة فى هذا المجال ما جعلها تحتل المركز ١٤ عالمياً والثانى عربيًا حسب ITU التقرير النهائى ٢٠١٧.
- مصر بصدد مناقشة قانون لحماية البيانات الشخصية بمجلس النواب ٢٠١٩ والذى حصل على موافقة مجلس الوزراء ويهدف إلى حماية بيانات المواطنين فى البنية الرقمية وتشجيع الاستثمار وتشجيع تكنولوجيا الذكاء الاصطناعى والحوسبة السحابية.

النتائج فى ضوء الدلالات النظرية

- يُفسر مجال الأمن السيبرانى أداء المسئولين والقائمين عليه بممارسات ومشاركات نشطة هى الفعل المنتج الذى له مردود قوى على تأمين البنية (الواقعية والرقمية) وحمايتها وإعادة تشكيلها.
- يتضح فى مجال الأمن السيبرانى فرض المجتمع لحدود فى التعامل السيبرانى بعيداً عن الإجرام والتطرف والعنف والتنمر والتدنى الأخلاقى والمساس بالأمن وفى نفس الوقت هيأ آليات لتيسير الفعل من خلال سُبل الحماية وتشريعات المكافحة.
- يتضمن الأمن السيبرانى معانى ودلالات من بينها الحماية والمكافحة، كما أنه يقوم على إرساء معايير من بينها مواجهة العنف والتمسك بالقيم والأخلاق ومحاربة الجريمة، فضلاً عن تفعيله لممارسة القوة من خلال العقاب التشريعى والتدبير التنظيمى فى الحماية والمواجهة والذى من شأنهما تشكيل بنية رقمية تتسم بالضبط والسيطرة لأنها تعتمد على التفاعل

بين المعانى والمعايير والقوة؛ مما يجعلها تنعكس إيجابًا على ضبط وأمن وسلامة البنية الواقعية.

- هيأت البنية المصرية للأمن السيبرانى من خلال الفعل السليم (الممارسات والأنشطة) والتفاعل القائم على أُطر تشريعية وتنظيمية وتقنية وتعاونية جيدة كما جاء فى مؤشر قياس ITU 2017، والذى أقر بأن هذا الفعل يُساعد فى تشكيل بنية منضبطة وآمنة ويزيد من إمكانات النمو والتنمية.

التوصيات

- الاهتمام بوضع آليات وسن تشريعات لمجابهة التدهور الأخلاقى والقيمى المستفحل فى الفضاء السيبرانى (كالتنمر الإلكترونى والبغاء الإلكترونى والتطرف الفكرى والدينى... إلخ).
- ضرورة إصدار قانون بشأن حماية الخصوصية يتيح آليات المراقبة من خلال استحداث تقنية لإنذار المسئولين بسوء الاستخدام مما يعطيها الحق فى التدخل والرقابة.
- زيادة التعمق فى الفضاء السيبرانى فى مجال علم الاجتماع الرقمى من خلال دراسة المواطنة الرقمية، الغزو الثقافى السيبرانى، العولمة الثقافية فى عصر المعلوماتية، مجتمع المخاطر المعلوماتى، مخاطر العالم الافتراضى، الشمول المالى والشمول الرقمى والتحول لمجتمع المعرفة، الحوسبة السحابية، قانون المعاملات الإلكترونية والتجارة الإلكترونية، التقاضى الإلكترونى... إلخ.

الهوامش

١- تقرير ITU، المؤتمر العالمى لتنمية الاتصالات (17-WTDC)، بوينس آيرس، الأرجنتين"، ٩-٢٠، أكتوبر ٢٠١٧، مكتب تنمية الاتصالات، الاتحاد الدولى للاتصالات، بجنيف، سويسرا، ٢٠١٨، ص٣٠.

٢- حمدون إ. تورية، البحث عن السلام السيبرانى، الاتحاد الدولى للاتصالات، فريق الرصد الدائم لأمن المعلومات، الاتحاد العالمى للعلماء، إيرتشه، صقلية، يناير ٢٠١١.

٣- عبد الله شرف الغامدى، الجرائم السيبرانية والتحديات المستقبلية، المجلة العربية: الأمن السيبرانى حروب الأرقام الصماء، ع ٤٩٨، ٢٠١٨، ص٦.

٤- أبو بكر شحرة، بناء القدرات فى الأمن السيبرانى، المجلة العربية: الأمن السيبرانى حروب الأرقام الصماء، ع ٤٩٨، الرياض، السعودية، ٢٠١٨، ص٩.

٥- هانى خميس، الأبعاد الاجتماعية للجرائم المعلوماتية فى المجتمع الحضرى، رسالة دكتوراه، قسم الاجتماع، كلية الآداب، جامعة الإسكندرية، ٢٠٠٦.

- نعمة محمد السيد عنانى، الاستخدام السلبى لشبكة الإنترنت وأثره على التفكك الأسرى، رسالة ماجستير، كلية الآداب، جامعة القاهرة، ٢٠١٣.
- عواطف سعود أبو تاكى، التحليل النقدى لجرائم الإنترنت الجديدة، رسالة ماجستير، قسم الاجتماع، كلية الآداب، جامعة الإسكندرية، ٢٠١٦.

٦ - Trends in Telecommunication Reform 2010-11- ITU-" The term "cyber security" refers to various activities such as the collection of tools ، risk management approaches، guidelines،security safeguards،policies andtechnologies that can be used to protect the cyber ، best practices،training environment and the assets of organizations and Users".

٧- الاتحاد الدولى للاتصالات ITU، "تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبرانى، قطاع تنمية الاتصالات، لجنة الدراسات ١، المسألة ٢٢/١، فترة الدراسة (٢٠٠٦-٢٠١٠)، ص١.

٨- السيد ياسين، تحولات الأمم والمستقبل العربى، نهضة مصر للطباعة، القاهرة، ط١، ٢٠١٠، ص٣٦٣.

٩- أولريش بك، مجتمع المخاطر العالمى بحثًا عن الأمان المفقود، ترجمة: علاء عادل وآخرون، القاهرة، المركز القومى للترجمة، ٢٠١٣، ص٢١٤.

١٠- المرجع السابق، ص ص ٢٣-٢٨.

١١- لبنى لطيف، علم اجتماع المخاطر: علم الاجتماع الجديد "العالم بين المخاطرة والخطر"، الجزائر، ١١ مارس، ٢٠١٧، ص ص ١٣-١٤.

١٢- أنتونى جيدنز، قواعد جديدة للمنهج فى علم الاجتماع، ترجمة محمد محى الدين، القاهرة، المجلس الأعلى للثقافة، ٢٠٠٠، ص١٤٠.

١٣- هانى خميس، التحليل السوسيولوجى لخطاب العنف فى المجتمع المصرى، المركز العربى للأبحاث ودراسة السياسات، مؤتمر السنوى الرابع، العنف والسياسة فى المجتمعات العربية المعاصرة، الدوحة، قطر، ٢٠١٥، ص٨.

١٤- أنتونى جيدنز، مرجع سابق، ص٢١٨.

١٥- المرجع السابق، ص٢٦.

١٦- أحمد زايد، آفاق جديدة فى نظرية علم الاجتماع نظرية تشكيل البنية، القاهرة، المجلة الاجتماعية القومية، مج٣٣، ع ١، ١٩٩٦، ص٦٦.

١٧- تقرير ITU، الوثيقة: RPM-ARB10/14-A، قطاع تنمية الاتصالات، الاجتماع الإقليمى التحضيرى للمؤتمر العالمى لتنمية الاتصالات ٢٠١٠ لمنطقة الدول العربية، دمشق، الجمهورية العربية السورية، ١٧-١٩ يناير ٢٠١٠.

متاح على:http://www.technologies.gov.ma/cmdt-pp10/RPM-ARB10X-E.pdf

١٨- منى الأشقر جبور، الأمن السيبرانى: التحديات ومستلزمات المواجهة، جامعة الدول العربية، المركز العربى للبحوث القانونية والقضائية، اللقاء السنوى الأول للمختصين فى أمن وسلامة الفضاء السيبرانى، بيروت ٢٧-٢٨ أغسطس (آب) ،٢٠١٢، ص٤.

١٩- حمدون إ. توريه، مرجع سابق، ص٢.

٢٠- Mckinsey noted in its july 2011 report.

٢١-عبد الله شرف الغامدى، مرجع سابق، ص٧.

٢٢- حسن بن على العجمى، الثورة الصناعية الرابعة وتغييرات الحياة الإنسانية، الرياض، السعودية، المجلة العربية: الأمن السيبرانى حروب الأرقام الصماء، ع ٤٩٨، ٢٠١٨، ص ١٦.

٢٣- محمد أسعد عالم، الهدم والتخريب تقنياً، الرياض، السعودية، المجلة العربية: الأمن السيبرانى حروب الأرقام الصماء، ع ٤٩٨، ٢٠١٨، ص١٣.

٢٤- عبد الله شرف الغامدى، مرجع سابق، ص٦.

٢٥- محمد سيد ريان، الأمن السيبرانى وثقافتنا الرقمية فى مصر، الرياض، السعودية، المجلة العربية: الأمن السيبرانى حروب الأرقام الصماء، ع ٤٩٨، ٢٠١٨: ص٢٨.

٢٦- Sony acknowledged a breach into its PlayStation network، in April 2011
انظر: بوابة إذكاء الوعى بالأمن السيبرانى، متاحة على:
www.gov.mu/portal/sites/ncbnew/main.jsp

٢٧- عبد الله شرف الغامدى، مرجع سابق، ص٧.

٢٨- حسن بن على العجمى، مرجع سابق، ص ١٧.

٢٩- محمد سيد ريان، مرجع سابق، ص٢٨.

٣٠- محمد أسعد عالم، مرجع سابق، ص١٣.

٣١- محمد أبو طه، فى الحاجة إلى الأمن السيبرانى، الرياض، السعودية، المجلة العربية: الأمن السيبرانى حروب الأرقام الصماء، ع ٤٩٨، ٢٠١٨، ص٢٢.

٣٢- منى الأشقر جبور، مرجع سابق، ص١٦.

٣٣- حمدون إ. توريه، مرجع سابق، ص ص ٨-١٠.

٣٤- تقرير ITU، ٢٠١٧، مرجع سابق، ص ص٦٤-٦٥.

٣٥- تقرير ITU، ٢٠١٠، مرجع سابق، ص ص ٨-١٠.

٣٦- خالد كاظم أبو دوح، الأمن السيبرانى للدول والأفراد الأمر الذى لا بد منه، المجلة العربية: الأمن السيبرانى حروب الأرقام الصماء، ع ٤٩٨، الرياض، السعودية، ٢٠١٨، ص٣٠.

٣٧- حمدون إ. توريه، مرجع سابق، ص ص ٨-١٠.

٣٨- محمد ابو طه، مرجع سابق، ص٢٢.

٣٩- منى الأشقر جبور، مرجع سابق، ص٦.

٤٠- المرجع السابق، ص٦.

٤١- حمدون إ. توريه، مرجع سابق، ص٥.

٤٢- تقرير ITU ٢٠١٧، مرجع سابق، ص٥٤.

٤٣- القمة العالمية لمجتمع المعلومات: برنامج عمل تونس بشأن مجتمع المعلومات، الفقرة ٤٠، القمة العالمية لمجتمع المعلومات، WSIS-05/TUNIS/DOC/6(Rev.1)-E، ١٨ نوفمبر ٢٠٠٥.

www.itu.int/wsis/docs2/tunis/off/6rev1.html

٤٤- Convention on cybercrime-Budapest-23XL، 2001.

٤٥- تقرير ITU، ٢٠١٧، مرجع سابق، ص٤٧.

٤٦- PricewaterhouseCoopers، Cyber Security M&A: Decoding Deals in the Global Cyber Security Industry (Nov. 2011)، p.76.

٤٧- le cyberspace anglais desormais protégé par d'anciens pirates informtiques، p3.http://techno.branchezvous.com/actualite/2009/06/le_cyberspace_anglais_desormais

٤٨- تقرير ITU، الوثيقة RPM-ARB10/14-A، ٢٠١٠: مرجع سابق، ص٣.

٤٩- منى الأشقر جبور، مرجع سابق، ص٨.

٥٠- le cyberspace anglais desormais:op.cit.، p.3

٥١- منى جبور الأشقر، مرجع سابق، ص١٤.

٥٢- حمدون إ. توريه، مرجع سابق، ص٤.

٥٣- تقرير ITU، ٢٠١٧: مرجع سابق، ص ص ١٦٦-١٦٧.

٥٤- موقع بوابة إذكاء الوعى بالأمن السيبرانى، موريشيوس.

٥٥- موقع التحالف الأمريكى للأمن السيبرانى الوطنى، متاح على:

www.staysafeonline.org/content/about-us

انظر: Understanding at 20 (يسرد الأهداف الشهيرة لهجمات القرصنة، بما فى ذلك وزارة الدفاع الأمريكية، والحكومة الألمانية، وGoogle وEbay وإدارة الولايات المتحدة الوطنية للملاحة الجوية والفضاء (ناسا).

٥٦- تقرير ITU، ٢٠١٠، مرجع سابق، ص ص٩٧-١٠٢.

٥٧- إعلان إريشتى، مبادئ الاستقرار السيبرانى والسلام السيبرانى، فريق الرصد الدائم لأمن المعلومات، الاتحاد العالمى للعلماء (WFS)، جنيف، الجلسة العامة للاتحاد، الدورة الثانية والأربعين، الحلقات الدراسية الدولية للطوارئ العالمية، إريتشى، صقلية، ٢٠ أغسطس ٢٠٠٩.

٥٨- قانون ١٧٥ لسنة ٢٠١٨، قانون مكافحة تقنية المعلومات، جريدة الجمهورية، ٢٠١٨/٨/١٤.

٥٩- كلمة وزير الاتصالات وتكنولوجيا المعلومات، المؤتمر العربى لأمن المعلومات، القاهرة، ٢٠١٨/١٢/٢٣.

الموقع الدائم لوزارة الاتصالات وتكنولوجيا المعلومات
www.mcit.gov.eg/Ar/media-center/pre -

٦٠- موقع وزارة الاتصالات وتكنولوجيا المعلومات -www.mcit.gov.eg/Ar/media center/pre -

Abstract

CYBER SECURITY: THE SOCIAL AND LEGAL DIMENSIONS، A SOCIOLOGICAL ANALYSIS

Islam Fawzi

The current research dealt with the issue of cyber security by focusing on the social dimensions that are: threats of cybercrime developed، and the increasing of their rates; Manifestations of targeting national security; Threatening of values and morals; Destroying of the infrastructure; entrenching the crisis of mistrust among citizens، and other social risks. The research then introduces the legislative and regulatory dimensions through laws related to protecting cyber security and the importance of international cooperation and policies. Finally، the research deals with protection mechanisms and cyber security practices. It concludes with presenting the most important results and their theoretical significance.