أ.م.د/ أسماء جابر مهران
أستاذ علم اجتماع الجريمة المساعد - كلية الآداب - جامعة أسيوط

الانعكاسات والمخاطر الاجتماعية للجرائم والهجمات السيبرانية على الأمن الرقمى وآليات المواجهة فى ضـــوء رؤيـــة مصـــر ٢٠٣٠

مقدمـة :

كشفت نتائج دراسة استقصائية أجرتها منظمة التعاون الاقتصادى والتنمية ، حول الاقتصاد الرقمى، أن الحكومات قد وضعت مجال الأمن فى المرتبة الثانية ، والخصوصية فى المرتبة الثالثة من بين ٣١ مجالاً مُمكنًا للسياسات ذات الأولوية. وفى الصدد نفسه يولى المستهلكون اهتمامًا متزايدًا بالخصوصية فى البيئة الرقمية؛ حيث أظهرت نتائج دراسة أجرتها (CIGI-IPSOS) عام ٢٠١٤م لمستخدمى الإنترنت فى ٢٤ دولة حول أمن الإنترنت والثقة إلى أن (٦٤٪) من المشاركين أصبحوا أكثر قلقًا بشأن الخصوصية مما كانوا عليه من قبل عام [١].

وعلى الرغم من صعوبة قياسها كميًا، يبدو أن الحوادث الأمنية تتزايد من حيث التعقيد والتكرار وحجم التأثير[٢]، فعلى مدى السنوات العشر الماضية تعرضت الأنشطة الحيوية بشكل متزايد لتهديدات الأمن الرقمى، وهو الاتجاه الذى يتسارع فيه التحول الرقمى الحالى، حيث تعمل الفوائد المتوقعة من المدن الذكية وشبكات الطاقة المعززة رقميًا والرعاية الصحية على توجيه الاعتماد والاستفادة من التقنيات التكنولوجية مثل البيانات الضخمة والذكاء الاصطناعى وأجهزة إنترنت الأشياء وشبكات الجيل الخامس. وعلى الرغم من أن هذه التقنيات تُعد تقنيات ناشئة، فإنها تزيد من تعقيد النظم البيئية الرقمية التى تدعم الأنشطة الحيوية؛ وذلك عن طريق نمو سطح الهجوم لمشغلى الأنشطة الحيوية بما يتناسب مع الكميات المتزايدة من البيانات والأجهزة والبرامج والبنى التحتية للشبكات التى يتعين عليهم إدارتها والتى لا يمكن اعتبارها آمنة تمامًا[٣].

ولم تعُد احتمالية أن تؤدى حوادث الأمن الرقمى إلى أضرار مادية أمرًا نظريًا، فقد دمرت هجمات الأمن الرقمى أجهزة الطرد المركزية النووية فى إيران، وولّدت أضرارًا مادية هائلة فى مصنع الصلب الألمانى عام ٢٠١٤م، فضلاً عن انقطاع التيار الكهربائى فى أوكرانيا فى عامى ٢٠١٥م، ٢٠١٧م، علاوة على ذلك أظهر حادث *Note petya* فى عام ٢٠١٧م أن الهجمات الأمنية الرقمية يمكن أن تُعطل بشكل كبير العمليات وسلاسل التوريد لعدة أيام فى مجالات مثل لوجستيات الحاويات العالمية (ميرسك) وإنتاج الأدوية (ميرك). وفى عام ٢٠٢١م أجبر هجوم إلكترونى شركة *(Colonia Pipeline Company)* على إغلاق أكبر خط أنابيب فى الولايات المتحدة لمدة ٦ أيام، مما أدى إلى نقص الوقود عبر الساحل الشرقى[٤].

إشكاليـة الدراسـة :

لقد انتقل الناس من العالم الواقعى إلى العالم الافتراضى، وكذلك انتقلت الجريمة. ولنا أن نتصوَّر حجم

التفاعلات التى تتم فى الواقع الافتراضى سواء كانت شخصية أو مؤسسية أو فى مجال الأعمال أو الخدمات أو الثقافة. ولابد من الإشارة إلى أن الفضاء الإلكترونى أنتج أنواعًا جديدة من الجريمة تسمى الجريمة الإلكترونية *(cyber crimes)* من خلال خلق فرص جديدة للمجرمين؛ فقد مَكَّنت مجرمى الفضاء الإلكترونى من تصفح الإنترنت وارتكاب جرائم فريدة من نوعها فى هذا الفضاء. إن هذه الميزات تشكل مفاتيح تحويلية *(keys transformative)* وتتمثل فى:

١- (العولمة *(globalization)* التى تُمكِّن الجناة مع وجود فرص جديدة من تجاوز الحدود التقليدية.

٢-(شبكات التوزيع *(networks distributed)* التى ولدت فرصًا لتكوين ضحايا.

٣- (الإجمالية والشمولية *(panopticism and synopticis)* التى تمكن الجناة من إذلال ضحاياهم عن بعد.

٤- (مسارات البيانات *(trails data)* التى خلقت فرصًا لارتكاب سرقة الهوية. ومن ناحية أخرى، فإن عدد ضحايا الجريمة الإلكترونية على ارتفاع، خاصة الذين يعانون خسارة مالية، أو المهددين أو المطاردين؛ وذلك نظرًا للزيادة فى عدد مستخدمى الإنترنت. هذا وتمثل الجريمة الإلكترونية المجال الجديد من الأبحاث فى مجال علم الجريمة(٥).

ومما سبق عرضه يتبين أن إشكالية الدراسة الحالية تكمن فى الإجابة عن التساؤل الرئيس:

ما الانعكاسات والمخاطر الاجتماعية للجرائم والهجمات والتهديدات السيبرانية على الأمن الرقمى؟ وما آليات المواجهة فى ظل رؤية مصر ٢٠٣٠؟

وينبثق عن هذا التساؤل الرئيس عدة أسئلة فرعية وهى:

أ- ما أجيال الهجمات السيبرانية؟

ب - ما طبيعة وأشكال الجرائم والهجمات السيبرانية؟

ج- ما جهات التهديد فى البيئة السيبرانية؟

د- ما المخاطر الاجتماعية للجرائم والهجمات السيبرانية على الأمن الرقمى؟

هـ - ما آليات وجهود الدولة المصرية فى التصدى للهجمات السيبرانية فى ضوء رؤية ٢٠٣٠؟

و - ما التصور المقترح لمجابهة المخاطر الاجتماعية للجرائم والهجمات السيبرانية على الأمن الرقمى فى مصر؟

أهمية الدراسة:

• الأهمية العلمية:

أ- تتمثل الأهمية العلمية للدراسة فى محاولة تسليط الضوء على حقل جديد فى العلوم الاجتماعية وبالأخص علم اجتماع الجريمة، حيث تُعد هذه الدراسة أول دراسة عربية - على حد علم الباحثة - تتناول الأمن الرقمى من منظور سوسيولوجى، والتى نأمل أن تُسهم فى فتح آفاق مستقبلية جديدة فى الدراسات السوسيولوجية.

ب- يُعد إضافة للتراث النظرى دراسة مفهوم جديد وهو الأمن الرقمى الذى يختلف عن الأمن المعلوماتى.

• الأهمية العملية:

إن رصد التاثيرات الاجتماعية للجرائم والهجمات السيبرانية على الأمن الرقمى مهم للأفراد من أجل رفع الوعى بمخاطرها وكيفية مواجهتها، كما أنه مهم للمسئولين وصُناع القرار من أجل تطوير استراتيجيات مجابهتها وتعزيز القدرات الدفاعية والهجومية لأنها تمثل تهديدًا خطيرًا على الفرد والدولة بأسرها.

أهداف الدراسة:

يتمثل الهدف الرئيس للدراسة الراهنة فى فحص الانعكاسات والمخاطر الاجتماعية للجرائم والهجمات والتهديدات السيبرانية على الأمن الرقمى، ورصد آليات المواجهة فى ظل رؤية مصر ٢٠٣٠، وينبثق من هذا الهدف العام، الأهداف الفرعية التالية:

أ- التعرف على أجيال الهجمات السيبرانية.

ب- الوقوف على طبيعة وأشكال الجرائم والهجمات السيبرانية.

ج - تبيان جهات التهديد فى البيئة السيبرانية.

د - الكشف عن المخاطر المجتمعية للجرائم والهجمات السيبرانية على الأمن الرقمى.

هـ - رصد آليات وجهود الدولة المصرية فى التصدى للجرائم والهجمات السيبرانية فى ضوء رؤية ٢٠٣٠.

و. التوصل إلى تصور مقترح لمجابهة المخاطر الاجتماعية للجرائم والهجمات السيبرانية على الأمن الرقمى فى مصر.

منهجية الدراسة:

ستعتمد الدراسة الراهنة على منهجية تحليل النظم التى وضعها (**ديفيد إيستون**-*David Easton*) فى تحليل

الظواهـر والنظم الاجتماعية من خـلال تحليل الظاهرة إلى عناصـرها كمُدخَلات، ومن ثم دراسة تأثير العوامل المتغيرة عليها كعمليات، وصولًا إلى المخرجات ومقارنتها بالمدخلات عبر ما يسـمى التغذية العكسـية وذلك لدراسـة العلاقة بين السبب والنتيجة (٦).

وعليه ستنقسـم موضوعات الدراسة فى ضوء هذه المنهجية وفـق الترتيـب التـالى:

أ- **المدخـلات :** التـى ستشـمل مفاهيـم الدراسـة مثـل (الجرائـم السـيبرانية – الهجوم السـيبرانى – الأمن الرقمى) .

ب- **العمليـات :** التـى ستشـمل دراسـة وتحليـل الأهـداف المتصلة بموضوع الدراسة، التى تتمثل فى الوقوف على أجيال الهجمات السـيبرانية، طبيعة وأشـكال الجرائم والهجمـات السـيبرانية، جهـات التهديـد فـى البيئـة السـيبرانية، المخاطر الاجتماعية للجرائم والهجمات السـيبرانية على الأمن الرقمى، وجهـود وآليات الدولة المصـرية فى التصدى للجرائم والهجمات السيبرانية فى ضوء رؤية ٢٠٣٠ .

ج- **المخرجـات :** ستشـمل المنهجية المُطـوَّرة التى تحاول الدراسـة التوصـل إليها كمقترح أو منهجية جديدة فى التصـدى لمخاطر الجرائم والهجمات السيبرانية على الأمن الرقمى .

المنظور السوسيولوجى لدراسة الأمن الرقمى:

١- نظريـة مجتمـع المخاطـر لرصـد انعكاسـات الجرائـم السيبرانية على الأمن الرقمى:

يعـد **أورليش بـك** عالـم الاجتمـاع الألمانى هو مؤسـس هـذه النظريـة، وأول مـن أشـار إلـى مصـطلح المخاطرة، ومجتمع المخاطر العالمـى، وتتناول نظرية المخاطر الوجود المتزايـد لانعـدام اليقين المنتشـر فـى ظل التغيـرات التى تحدث فى المجتمع، حيث اندثر المجتمع الصـناعى مُفْسِحًا المجـال لمجتمع المخاطـر التقنى والتكنولوجـى أو المجتَمع المعلوماتى، وهو ما يُطلق عليه مُنَظرو ما بعد الحداثة "**عالم الفوضى**» الذى تغيب معه أنماط الحياة المستقرة(٧).

إن مجتمع المخاطر العالمـى يمثل فترة فريدة للغاية من التاريخ قادرة على تدمير نفسها بنفسها تكنولوجيًا(٨).

وتأسيسًـا على ذلك نجد أن الأمن الرقمى يَشـهَد مخاطر عدة نتيجة الثورة الرقمية التى يشهدها المجتمع، وما تَمَخَّض عنهـا من تطور فـى أنماط الجرائـم والهجمات السـيبرانية التـى نتـج عنها عـدم الحفـاظ علـى الخصوصـية الثقافية للأفراد، والاسـتيلاء على بعض المعلومـات الرقمية للأفراد والمؤسسات والدول(٩).

٢- نظرية تشـكيل البنى لرصد مقومات الأمن الرقمى:

يمكـن النظر إلـى نظرية التشـكيل البنائـى (*Theory Structuration*) عند **أنتونى جيدنز** باعتبارها إسهامًا مُهمًا فـى طرح رؤية نظرية لحل إشـكالية اجتماعية، هى إشـكالية (البنية- الفاعلية *Agency - Structure*)

حيث تُعد ممارسـات الأمن الرقمى والسـيبرانى فى ضوء هـذه النظرية من أهـم مظاهر تشـكيل البنيـة الاجتماعية، وذلـك فى ضـوء القضـايا الرئيسـة التى دعـا إليهـا أنتونى جيدنز، وهى كالآتى (١٠):

أ- تنطـوى عملية تشـكيل البنية على المشـاركة النشـطة للذوات الفاعلة والممارسات اليومية الناجح.

ب- يفرض البنـاء حدودًا على الفعل الإنسـانى، كما ييُسر تحقيق هذا الفعل «ازدواجية البناء».

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

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

ومـن ثـم يتضـح أن الفاعلين، وهـم مُرتكبـى الجرائم والهجمات السـيبرانية، يقومون بالتأثير السلبى على البناء الاجتماعى، ويشـكلونه وفـق رؤيتهم المزدوجـة، وذلك من خلال الممارسـات الإجرامية المتكررة، فهم قوة فاعلة فى الفضاء الرقمى لأنهم يمتلكون القوة التخريبية، ويتصرفون وفـق معتقدات خاصـة، وعبـر أسـاليب مختلفة تـؤدى فى مجملها إلى جملة من المخاطـر الاجتماعية المؤذية للفرد والمجتمع بكامله.

تتضمن الدراسة العناصر التالية:

١- الإطار المفاهيمى للدراسة .

٢- أجيال الهجمات السيبرانية .

٣- أنماط الجرائم والهجمات السيبرانية.

٤- أنـواع جهـات التهديد فـى البيئة السـيبرانية (فئات المهاجمين السيبرانيين): .

٥- المخاطرالاجتماعيـة للجرائم والهجمات السـيبرانية على الأمن الرقمى .

٦- آليات وجهود الدولة المصـرية فى التصـدى للجرائم والهجمات السيبرانية فى ضوء رؤية مصر ٢٠٣٠ .

٧- المعايير والنموذج المقترح لمجابهة المخاطر الاجتماعية للجرائم والهجمات السيبرانية على الأمن الرقمى فى مصر.
٨- نتائج الدراسة ومقترحاتها.

أولاً : الإطار المفاهيمى للدراسة :

١- مفهوم الجريمة السيبرانية :

الجريمة السيبرانية تتمثل فى عدد محدود من الأعمال التى تمس سرِّية البيانات أو النظم الحاسوبية وسلامة توافرها، أما الأعمال المنفَّذة بواسطة الحواسيب الرامية إلى تحقيق مكاسب شخصية أو مالية أو إحداث أضرار بما فى ذلك أشكال الجريمة المتصلة بالهوية وبمحتوى الحواسيب، فهى تندرج كلها ضمن نطاق أوسع من مصطلح الجريمة السيبرانية، ولا يمكن تطويعها بسهولة لتنضوى ضمن تعاريف قانونية لمصطلح جامع. الأمر الذى يلزم تعريف وتحديد الأعمال الأساسية التى تشكل جريمة سيبرانية. وإن كان تعريف الجريمة السيبرانية لا يتسم بالقدر نفسه من الأهمية فيما يخص الأغراض الأخرى كتحديد نطاق صلاحيات الهيئات المختصة بالتحريات والتعاون الدولى، حيث يفضل التركيز على الأدلة الإلكترونية فيما يخص أى جريمة بدلًا من التركيز على تركيبة واسعة واصطناعية لـ «الجريمة السيبرانية»(١١).

بالمعنى الأوسع تشير الجرائم السيبرانية (الإلكترونية) إلى « أى سلوك غير قانونى يستخدم فيه الكمبيوتر أو الإنترنت كأداة أو هدف أو كليهما، فهذا السلوك غير القانونى يتم فيه استخدام أجهزة الحوسبة مثل الهواتف الذكية والأجهزة اللوحية والمساعدات الرقمية الشخصية (*PDAS*) وغيرها من أجهزة الحوسبة المستقلة أو المرتبطة كأداة أو هدف للسلوك الإجرامى يتم ارتكابها بشكل متكرر من قبل أشخاص ذوى سلوك مدمر وإجرامى لمجموعة متنوعة من الأسباب بما فى ذلك الانتقام أو المال أو المغامرة». ووفقًا (لقاموس أكسفورد) فإن مصطلح الجريمة السيبرانية يُقصد به: « الأنشطة الإجرامية التى يتم تنفيذها باستخدام أجهزة الكمبيوتر أو الإنترنت» . كما يتم تعريف الجريمة السيبرانية على أنها «نشاط إجرامى يحدث على أو باستخدام الأجهزة أو الويب أو أى تقنية أخرى معترَف بها». واستخلاصًا لما سبق فإن الجريمة السيبرانية هى: «تلك الأنواع التى يُعد جنسها جريمة تقليدية، ولكن يكون فيها الكمبيوتر شيئًا أو موضوع السلوك الذى يشكل جريمة» (١٢).

٢- مفهوم الهجوم السيبرانى :

تقع الهجمات السيبرانية فى سياق أوسع- ما يسمى تقليديًا- عمليات المعلومات أو العمليات المعلوماتية، التى تَستخدم بشكل متكامل القدرات الرئيسة للحرب الإلكترونية والشبكات النفسية والحاسوبية، الخداع العسكرى والعمليات الأمنية وذلك بالتنسيق مع الدعم الخاص والقدرات ذات الصلة. هذا، وقد تباينت تعريفات الهجوم السيبرانى من قِبَل متخصصين فى المجالين القانونى والفنى، ومن أهم هذه التعريفات أن الهجمات السيبرانية هى: «الإجراءات التى تتخذها الدول لاختراق أجهزة الكمبيوتر لدولة أو دول أخرى لإحداث ضررأو تعطيل» (١٣) .

كما تُعرَّف الهجمات السيبرانية على أنها: «فعل يُقَوِّض من قدرات وظائف الشبكة المعلوماتية من خلال استغلال نقاط الضعف، ما يمنح المهاجم القدرة على التلاعب بالنظام، وتُعرَّف كذلك بأنها الاستغلال المتعمد لأنظمة الكمبيوتر والشبكات المعتمدة على التكنولوجيا من خلال البرمجيات الضارة»(١٤).

ويمكننا التمييز وإظهار الفروق بين الجريمة السيبرانية والحرب السيبرانية والهجوم السيبرانى على النحو التالى:

الجريمة السيبرانية (الإلكترونية): هى إجراءات سيبرانية يتم اتخاذها فقط من قبل المهاجمين غير الحكوميين، ويتم تنفيذ الإجراء السيبرانى بواسطة نظام كمبيوتر، وهو ما يُعد انتهاكًا للقانون الجنائى.

الهجوم السيبرانى والحرب السيبرانية: الغرض من الهجوم السيبرانى هو تدمير وتعطيل تشغيل شبكة الكمبيوتر، وأن الهجوم يتم لأغراض سياسية أو أمنية، وأن آثار الهجوم السيبرانى هى آثار الهجوم المُسلح نفسه أو الفعل السيبرانى الذى حدث فى سياق هجوم مسلح(١٥).

٣- مفهوم الأمن الرقمى:

غالبًا ما تتضمن معايير الصناعة الدولية والوطنية الخاصة بأمن المعلومات تعريفًا للأمن الرقمى. مع الإشارة إلى إنه لا يوجد تعريف مقبول عالميًا أو إجماع عالمى حول ما يشمله المصطلح بدقة. وفى سياق الأمم المتحدة لاحظ المفتشون أنه لا توجد أى توجيهات على نطاق المنظومة من المنتديات المشتركة بين الوكالات ذات الصلة توصى بالإجماع بتعريف معين باعتباره موثوقًا للمنظومة، كما أن الأطر التنظيمية لدى المنظمات لا تحاول بشكل منهجى فرض تعريف للأمن الرقمى. ووفقًا للاتحاد الدولى

للاتصالات يُعرَّف الأمن الرقمى بأنه: «مجموعة من الأدوات والسياسات والمفاهيم الأمنية والضمانات الأمنية والمبادئ التوجيهية، ونهج إدارة المخاطر، والإجراءات، والتدريب، وأفضل الممارسات، والضمان، والتقنيات التى يمكن استخدامها لحماية البيئة السيبرانية وأصول المنظمة والمستخدمين. وتشمل أصول المنظمة والمستخدمين أجهزة الحوسبة المترابطة والموظفين، والبنية التحتية، والتطبيقات، والخدمات، وأنظمة الاتصالات ومجموع العمليات المنقولة أو المخزونة فى البيئة السيبرانية، ويسعى الأمن السيبرانى لضمان تحقيق وحفظ الخصائص الأمنية لأصول المنظمة والمستخدمين ضد المخاطر الأمنية ذات الصلة فى البيئة السيبرانية، وتتألف الأهداف الأمنية العامة من التوافر، والسلامة التى يمكن أن تشمل المصداقية وعدم التنصل، والسرية»[١٦].

أما وكالة الأمن الرقمى الأوروبية فى أول تشريع أصدرته عام ٢٠٠١م عَرَّفت الأمن الرقمى بأنه: «قدرة النظام المعلوماتى على مقاومة محاولات الاختراق، أو الحوادث غير المتوقعة التى تستهدف البيانات المتداولة أو المخزنة وفق إطار توافقى»[١٧].

كما يُعرِّفه **مركز هردو** لدعم التعبير الرقمى بأنه : «كيفية استخدام شبكة الإنترنت استخدامًا فعّالاً دون التعرض لأى تهديدات أو مخاطر أو مراقبة تهدد خصوصية وسرية المعلومات»[١٨].

وما يمكن الإشارة إليه بخصوص مفهوم الأمن الرقمى هو أنه يشكل أداة لتوحيد التعاون فى مجال مكافحة الجرائم الرقمية بمختلف أصنافها والوقوف فى وجه مخاطرها. والجدير بالذكر أنه من قبيل الدول التى اهتمت بمفهوم الأمن الرقمى كانت بريطانيا وتحتل المرتبة الأولى عالميًا وفقًا لتصنيف المؤشر العالمى للأمن السيبرانى (جى سى آى) الذى أصدره الاتحاد الدولى للاتصالات التابع للأمم المتحدة ثم الولايات المتحدة الأمريكية، ومن الدول العربية التى اهتمت بالأمن الرقمى وفقًا للتصنيف جاءت المملكة العربية السعودية فى المرتبة الأولى عربيًا ثم جمهورية مصر العربية وقطر.[١٩].

ثانياً : أجيال الهجمات السيبرانية :

ويمكن الإشارة إليها على النحو التالى[٢٠] :

الجيل الأول (١٩٨٩م-١٩٩٠م): حيث فى أواخر الثمانينيات شن المتسللون هجمات فيروسية على أجهزة الكمبيوتر المستعملة، الأمر الذى أسهم المستخدمون والشركات الخاصة المتضررة فى إنشاء منتجات مكافحة الفيروسات (*AV*) التى تركز على معلومات التوقيع .

ومن أمثلة الهجمات السيبرانية من الجيل الأول:

- (*ELK Cloner - 1982*) أول فيروس كمبيوتر فى العالم.

الجيل الثانى (١٩٩٥م): كان فى منتصف التسعينيات؛ حيث ظهرت هجمات الديدان السريعة التوسع مباشرة من شبكة الإنترنت المنتشرة فى كل مكان، مما أجبر الشركات على بناء جدار حماية على أطراف البنية التحتية لإبعاد الأشخاص المهاجمين .

ومن أمثلة الهجمات السيبرانية من الجيل الثانى:

- (وحدة موريس -١٩٨٨م) واحدة من أولى ديدان الكمبيوتر، مما أدى إلى إدانة جنائية فى الولايات المتحدة بموجب قانون الاحتيال وإساءة استخدام الكمبيوتر.
- (ميليسا - ١٩٩٩م) أول فيروس ماكرو بريدى جماعى.

الجيل الثالث(٢٠٠٥م): خلال السنوات الأولى من القرن الجديد بدأ المجرمون فى استغلال الأخطاء البرمجية التى يمكن أن تؤثر على الشركات التى تستغلها، ويتعلق ذلك أيضًا بالفترة التى يتحول فيها غرض الجانى من التقدير إلى المكافأة فى البداية بعد استخدام شبكة الروبوتات الخاصة لتوزيع البريد العشوائى.

ومن أمثلة الهجمات السيبرانية من الجيل الثالث :

- (*I Love you - 2000*) - دودة تصيب عشرات الملايين من أجهزة *Windows 2005 - SQL slammer*- رفض الخدمة لـ ٧٥٠٠٠ مُضيف.

الجيل الرابع (٢٠١٠م) : فى أثناء الربع الأول من العقد الماضى، لم تكن هناك أى علامات على ظهور الهجمات المستهدفة. وخلال محادثة حول عدم وجود أدلة واضحة فيما يتعلق بأسلحة الدمار الشامل تم حث المواطنين على اتباع كلمة المجهول الخفى التى اخترعها وزير الدفاع الأمريكى آنذاك **رونالد رامسفيلد.**

ومن أمثلة الهجمات السيبرانية من الجيل الرابع :

- (*Stux net 10 - 2005*) - تطوير ترعاه الدولة ويستهدف أنظمة *SCADA* فى البنية التحتية الحيوية بما فى ذلك البرنامج النووى الإيرانى.
- هجوم (*2016-DYN*) ليس فيروسًا مستقلاً ولكنه هجوم ضخم لرفض الخدمة الموزعة (*DDOS*) على مزود *DNS* الرئيسى.

الجيل الخامس (٢٠١٧م) : حيث بدأت هجمات ضخمة واسعة النطاق بتمويل من بعض الحكومات فى عام ٢٠١٧م حتى تتمكن العديد من الشركات من تنفيذها. فالجرائم السيبرانية لها شبكات الإنترنت والضمان الخاصة بها.

ومن أمثلة الاعتداءات من الموجة الخامسة :

- *(2017-Wannacry)* هجوم كبير ببرامج الفدية يؤثر على ٢٠٠٠٠٠ جهاز كمبيوتر فى ١٥٠ دولة.

ثالثاً : أنماط الجرائم والهجمات السيبرانية :

١ - أنماط الجرائم السيبرانية :

ظهرت الجرائم السيبرانية وتطورت لتصبح أحد أسرع التهديدات نموًا فى عالم الجريمة، ويبقى تحديد مدى انتشار هذه الأنشطة الإجرامية بغاية الصعوبة.

ومن الأفعال المُصنفة كجرائم سيبرانية مايلى(٢١):

- التعدى على البيانات المعلوماتية.
- التعدى على الأنظمة المعلوماتية.
- إساءة استعمال الأجهزة أو البرامج المعلوماتية.
- الجرائم على الأموال.
- الاستغلال الجنسى للقاصرين.
- التعدى على الملكية الفكرية للأعمال الرقمية.
- جرائم البطاقات المصرفية والنقود الإلكترونية.
- الجرائم التى تمسّ المعلومات الشخصية.
- جرائم العنصرية والجرائم ضد الإنسانية بوسائل معلوماتية.
- جرائم المقامرة وترويج المواد المخدرة بوسائل معلوماتية.
- جرائم المعلوماتية ضد الدولة والسلامة العامة.
- جرائم تشفير المعلومات.

٢ - أنماط الهجمات السيبرانية :

يمكن تصنيف الهجمات السيبرانية إلى الفئات التالية(٢٢):

أ - الهجمات على شبكة الإنترنت :

وهي الهجمات التى تحدث على مواقع الويب أو تطبيقات الويب، ومن أمثلتها :

- **هجمات الحقن** : وتشمل حقن *(SQL)*، وحقن *(XML)*، وحقن التعليمات البرمجية، وحقن السجل وهو الهجوم الذى يتم فيه حقن بعض البيانات فى تطبيق ويب لمعالجة التطبيق وجلب المعلومات المطلوبة .
- **انتحال***(DNS)*.
- **هجمات التصيد** ويشمل: (التصيد بالرمح – *Spear phishing*)، (تصيد الحيتان – *whaling*)، (التصيد الاحتيالى– *Smishing*)،(التصيد الصوتى –*Vishing*)، (التصيد بالبريد الإلكترونى –*Email Phishing*)، التصيد من خلال «تسميم محركات البحث» – *SEO Poising*).
- **هجمات حجب الخدمة** *(DRDOS/ DDOS/DOS)*
- **هجوم الوسيط** *(Man-In-The-Middle)*، ومن أنواع هجوم الوسيط (التنصت على الواى فاى – سرقة بريد إلكترونى أو *SSL* – انتحال *IP* أو *HTTPS* أو *DNS*).

ب - الهجمات القائمة على النظام :

والهجمات التى تهدف إلى اختراق جهاز الكمبيوتر أو شبكة كمبيوتر ومن أمثلتها :

- الفيروسات.
- الديدان.
- حصان طروادة.
- الأبواب الخلفية.
- الروبوتات.

وفضلاً عن ذلك فقد كشفت الاستراتيجية الوطنية للأمن السيبرانى (٢٠٢٣م-٢٠٢٧م) فى مصر عن تزايد أعداد الهجمات السيبرانية فى الأعوام السابقة بشكل كبير، كما تسببت الهجمات السيبرانية فى خسائر ضخمة للاقتصاد العالمى، مما يشكل عبئًا كبيرًا على ميزانيات الدول. هذا بالإضافة إلى الخسائر الأخرى مثل توقف بعض الخدمات الحيوية عن العمل، والإضرار بسمعة الشركات والأفراد.

كما كشفت الاستراتيجية إلى أن مصادر التهديدات السيبرانية قد تنوعت لتشمل الجريمة السيبرانية، الحرب السيبرانية، الإرهاب، التهديدات الداخلية وتهديدات الهواة ، ويمكن الإشارة إليهم على النحو التالى(٢٣) :

الجريمة السيبرانية *(Crime Cyber)* :

إن الجريمة السيبرانية هى المسئولة بصورة أساسية عن تطوير وترويج برامج ضارة من أجل الكسب المالى أو القرصنة بقصد سرقة البيانات و/أو الشبكات أو إتلافها أو تحريفها. وقد أصبحت تلك الهجمات شرسة وتنتشر فى العالم بشكل متزايد كما يوضحه الاستخدام المتزايد لبرامج طلب الفدية *(Ransom ware)* والتهديدات بهجوم حجب الخدمة *(Dodos)* لغرض تشويه الصورة أو الابتزاز

- الحرب السيبرانية *(War Cyber)* :

هى تهديدات تقوم بها دول وجماعات ترعاها دول، وذلك لاختراق القطاعات الحرجة فى دول أخرى مثل قطاعات الطاقة والاتصالات والبنوك وغيرها، وذلك

من أجل التجسس، أو مكاسب سياسية واستراتيجية، أو بغرض التخريب فقط. ومن الجدير بالذكر أن العديد من الدول قد أعلنت صراحة امتلاكها قدرات هجومية سيبرانية لغرض الدفاع عن النفس من هذه التهديدات.

ـ الإرهاب *(Terrorism)* :

على الرغم من القدرات السيبرانية المتواضعة للإرهابيين، فإنه من المتوقع خلال الأعوام القليلة المقبلة أن تزداد هذه القدرات على إحداث أضرار بالغة، مما يجعلها على خريطة التهديدات المحتملة.

ـ التهديدات الداخلية *(Insiders)* :

مع تزايد استخدام تكنولوجيا المعلومات داخل المؤسسات، تتزايد احتمالات المخاطر الناتجة، قصدًا أو دون قصد، من الموظفين المخوَّلين باستخدام أنظمة المعلومات. فقد يكون هؤلاء الموظفون مصدرًا لتهديد المؤسسات عن طريق سرقة بيانات حساسة تؤدى إلى خسائر مادية جسيمة أو إلى تهديد سمعة المؤسسة. وقد يعرّض الموظف بيانات المؤسسة الحساسة للخطر دون قصد عن طريق بعض الهجمات السيبرانية مثل التصّيد الإلكترونى *(Phishing)* أوالهندسة الاجتماعية *(Social Engineering)* .

ـ الهواة *(Kiddies Script)* :

هم مجموعة أشخاص أصحاب مهارات سيبرانية محدودة، ولكنهم يستخدمون برامج مجهَّزة ذات قدرات تخريبية عالية إذا صادفت نقاط ضعف فى أنظمة المعلومات الموجودة فى المؤسسات.

رابعاً : أنواع جهات التهديد فى البيئة السيبرانية (فئات المهاجمين السيبرانيين) :

وتتمثل الأنواع الرئيسية لجهات التهديد فى البيئة السيبرانية على النحو التالى(٢٤) :

- **القراصنة الحاسوبيون :**

أفراد أو جماعات يخترقون الشبكات لإحداث اضطراب أو أذى أو فوضى وذلك من أجل الشهرة أو التحدى.

- **نشطاء القرصنة الحاسوبية :**

لديهم دوافع محددة ويرون فى نشاطهم شكلًا من أشكال العصيان المدنى أو وسيلة للتعبير عن الذات سياسيًا أو أيديولوجيًا.

- **مجرمو الفضاء السيبرانى :**

جهات فاعلة تنخرط فى نشاط إجرامى مُمَكَّن سيبرانيًا (الجرائم الشائعة مثل الاحتيال والسرقة والابتزاز وما إلى ذلك) بمساعدة الوسائل الحاسوبية أو فى نشاط إجرامى معتمد على الفضاء السيبرانى، مثل نشر الفيروسات أو البرمجيات الخبيثة وغيرها من الأنشطة التى لا يمكن ارتكابها إلا من خلال الوسائل المُحَوْسبة.

- **جواسيس الصناعة :**

فئة فرعية من الجماعة الإجرامية وأهدافها محددة بالحصول على الأسرار التجارية، أو الابتزاز لأسباب تتعلق بالمصلحة الاقتصادية أو تخريب المنافسة.

- **الدول أو المجموعات التى ترعاها دولة :**

جهات فاعلة متطورة للغاية وذات موارد جيدة يصعُب عادة اكتشاف أنشطتها أو تعقبها أو تحديدها، يمكن أن تلتمس بطريقة خفية أهدافًا معقدة، غالبًا ما تكون غير مباشرة وغير واضحة، وتستخدم بشكل مباشر من قبل كيانات حكومية أو عسكرية أو بتمويل غير مباشر منها.

- **المطلعون :**

جهات فاعلة لا تُعد بحكم علاقاتها التعاقدية مع المنظمة المعنية جهات خارجية، ولكنها تعرضها للخطر من الداخل، ويمكن أن تشمل هذه الفئة الموظفين الساخطين والموظفين المدربين تدريبًا سيئًا، أو مقدمة الخدمة المتعاقد معهم والمدربين تدريبًا سيئًا، إلى جانب جهات أخرى.

خامساً : المخاطر الاجتماعية للجرائم والهجمات السيبرانية على الأمن الرقمى :

تسببت الجرائم السيبرانية (الإلكترونية) فى إلحاق الضرر بالمواطنين والشركات والحكومة بعدة طرق مثل فقدان معلومات الأعمال الحساسة وفقدان ثقة العملاء، وفقدان الملكية الفردية، والخسائر التجارية وما إلى ذلك. فقد ذكر مركز الدراسات الاستراتيجية والدولية أن التكلفة السنوية التى يتحملها الاقتصاد العالمى بسبب حوادث الجرائم الإلكترونية تزيد على (٤٠٠) مليار دولار، وإن تأثيرات الجرائم السيبرانية ستزداد تدريجيًا مع ازدهار وظائف الأعمال عبر الإنترنت، ومع اتصال المزيد من الشركات والعملاء فى العالم بالإنترنت. كما تتسبب الجريمة السيبرانية فى البلدان المتقدمة فى معدل التوظيف حيث كشفت نتائج الأبحاث أن الخسارة الناجمة عن الجريمة السيبرانية يمكن أن تلحق الضرر بـ (٢٠٠٠٠٠) وظيفة

أمريكيـة أى ما يقرب من ثلث الانخفاض فـى التوظيف، كما أن (٣٠٠٠) شـركة فى الولايات المتحدة تعرضـت للاختراق فـى عـام ٢٠١٤م، كما تكبـدت البرازيـل (١,٤) مليار دولار بسبب أضـرار الهجمات السيبرانية، لأن أكثر من (٤٥٪) من البرازيليين يسـتخدمون الإنترنت، وفى عام ٢٠١٣م خسـرت فرنسا (١٩,٥) مليون دولار بسبب الهجمات السيبرانية، كما أنها واجهت ١٩٠٠ هجوم سـيبرانى منذ الهجوم الإرهابى فى عام ٢٠١٤م، حيث إن نحو (٩١٪) من الشـركات فى المملكة المتحـدة و (٣١٪) مـن الأسـر لديهـا إمـكان الوصـول إلى الإنترنت، كما تقـدَّر التكلفة المحسـوبة للجرائم الإلكترونية فى المملكة المتحدة بنحو (٢٧) مليار دولار[٢٥].

وتأسيسًـا علـى ذلـك جـاء فى تقريـر الاتحـاد الدولى للاتصـالات *(TTU)* عام ٢٠١٠م بشـأن الأبعـاد الاجتماعية للأمن الرقمى أن الثورة الرقمية غيَّرت كيفية التعامل التجارى وكيفية عمـل الحكومات، وأدت العولمـة والتقدم التكنولوجى إلى إضـعاف البنيـة التحتية، وبالتالى جعلتهـا هدفًا محتملًا لهجمـات إرهابية، حيث تواجه البلـدان مخاطر حقيقية، وأن المجرميـن يقومون باسـتغلال مواطن الضـعف التى تعانيها أنظمـة المعلومـات الدقيقة من أجـل تعطيل البنيـة التحتية والموارد الأساسية ومن ثم تهديد الأمن القومى[٢٦].

وتتمثـل أهـم المخاطـر الاجتماعية للجرائـم والهجمات السيبرانية على الأمن الرقمى فى:

١- زيـادة معـدلات الجرائـم المستحدثـة والخسائـر الناجمـة عنهـا :

فى ٢٣ ديسـمبر ٢٠١٥م هاجم قراصـنة شبكة الكهرباء فى أوكرانيا وعطلوا أنظمة التحكم المستخدمة فى المحطات الكهربائيـة الفرعيـة عن بعد، وتركوا النـاس والجزء الغربى مـن البـلاد دون كهرباء لعـدة سـاعات، وقد ألقـت الخدمة الأوكرانيـة *(SBU)* اللوم على الحكومة الروسـية فى الهجوم السـيبرانى، وهـو الاتهام الذى وجـد دعمًا لاحقًـا فى تحليل البرامج الضارة من قبل شركات خاصة لأمن الكمبيوتر. كان الاختـراق الأوكرانى هـذا أول حالة مُعترَفًا بهـا علنًا لهجوم سيبرانى تسـبب بنجاح فى انقطاع التيار الكهربائى كما أنها مجرد واحدة من آلاف الأنشطة السيبرانية ومعظمها منتشرة تحدث جنبًا إلى جنب مع القتال الجسدى فى أوكرانيا[٢٧].

ونظـرًا لأن المسـتهلك أصـبح يعتمد بشـكل متزايد على أجهزة الكمبيوتر والشبكات والمعلومات التى يتم استخدامها لتخزينهـا وحفظها، فإن خطر التعرض للجرائم الإلكترونية مرتفـع، فقـد أظهـرت نتائج الدراسـات الاستقصـائية التى أجريـت إلـى أن مـا يصـل إلـى (٨٠٪) من الشـركات التى شـملتها الدراسـة اعترفـت بخسـائر مالية بسـبب انتهاكات أجهـزة الكمبيوتر تُقـدر قيمتها بمبلغ ٤٥٠ مليـون دولار، وما يقرب من (١٠٪) من الاحتيال المالى، حيث تتزايد الهجمات الجديـدة التـى تؤثر على سـرية أنظمة الكمبيوتر وسـلامتها وتوافرهـا يمكن أن تتـراوح ما بين سـرقة معلومات التعريف الشخصية وهجمات رفض الخدمة[٢٨].

وتماشـيًا مع ما تم ذكره فإنه فى السنوات الخمس عشرة الماضـية حدث العديد من المشكلات التى أثرت على التحول مـن أمن المعلومات إلى الأمن الرقمى: مثل زيادة التهديدات الداخليـة (كحـوادث تسـريبات الويكى الداخليـة وانتهاكات البيانـات والمهمات الخبيثة من الداخل، والتقنيات الناشـئة وتحديـدًا التقنيـات الرقميـة ذات التوجـه الخارجـى التـى تتيـح الاتصـال، التقنيـات المعرفيـة ، الذكاء الاصـطناعى وتكنولوجيا الهاتف المحمول، ووسـائل التواصـل الاجتماعى، وما إلى ذلـك)، وزيادة التهديـدات الخارجية مثل (البرامج الضارة وبرامج الفدية واختراق البيانات، الأجهزة المترابطة وأجهزة الإنترنت والحرب السيبرانية والهجمات التى ترعاها الدولة) . فعلى سـبيل المثال قدَّر **معهد بويتمون** أن التكاليف المباشرة لاختراق البيانات فى عام ٢٠١٧م قد بلغت (٣,٦٢) مليون دولار أمريكى [٢٩].

ليس هذا فحسـب، حيث إن أقسـام الشرطة فى جميع أنحـاء البلاد قد ذكرت أنها تلقت عددًا متزايدًا من جرائم الاحتيال والسـرقة الكبرى فى السـنوات الأخيرة، ويتزامن هذا مع الاتجاه الوطنى الناتج عن زيادة استخدام الكمبيوتر والأعمال التجاريـة عبر الإنترنت. وفى عام ٢٠٠٤م حققت الجريمة السـيبرانية عائدًا أعلى مـن الاتجار بالمخدرات، ومن المتوقع أن تنمو أكثر مع توسـع اسـتخدام التكنولوجيا فـى البلدان الناميـة. كما أظهرت النتائـج لعام ٢٠١١م أن أكثر من (٧٤) مليون شـخص فى الولايـات المتحدة كانوا ضـحايا للجرائـم الإلكترونية فى عـام ٢٠١٠م، وأدت هذه الأعمال الإجرامية إلى خسـائر ماليـة تقدَّر بقيمة ٣٢ مليار دولار، وأن (٦٩٪) مـن البالغيـن المتصـلين بالإنترنت قد وقعـوا ضـحايا لجرائم الإنترنـت مما أدى إلـى وقوع مليون ضـحية لجرائم الإنترنـت يوميًا. ويعتقد الكثيـر من الناس أن الجريمة السـيبرانية هى جرائم تتعلق بممارسة الأعمال التجارية عبر الإنترنت [٣٠].

٢- استهداف القطاعات الحيوية :

لقد أثر برنامج الفدية *(Wannacry)* على العديد من الخدمات فى جميع أنحاء العالم، مثل الخدمات الصحية الوطنية فى المملكة المتحدة، كما أوقفت شركة *(Renault)* الإنتاج فى المصانع فى جميع أنحاء فرنسا، وواجهت شركة *(Deutsche Bahn)* مشكلات فى عرض خطوط القطارات فى محطات القطار، وكانت حركة مرور الحاويات فى *(Maersk)* فى جميع أنحاء العالم صعبة للغاية، وما إلى ذلك (٣١).

وتشمل الأمثلة على الهجمات السيبرانية المدمرة الهجوم السيبرانى الشهير على خط الأنابيب الاستعمارى فى عام (٢٠٢١م) الذى أدى بشكل مباشر إلى منع تدفق الغاز فى جميع أنحاء الولايات المتحدة. وفى ليلة ٩ سبتمبر ٢٠٢٠م أصاب هجوم فدية الأنظمة فى مستشفى جامعة دوسلاوف وهو مستشفى كبير فى جنوب دوسلدوف، حيث تُعد برامج الفدية أحد أشكال البرامج الضارة التى تمنع المستخدمين من الوصول إلى ملفاتهم، وغالبًا ما يكون ذلك عن طريق تشفير البيانات حتى يتم دفع الفدية، ومع انتشار الهجوم عبر شبكة الكمبيوتر الخاصة بالمستشفى تم تشفير ثلاثين خادمًا وجعلها غير صالحة للعمل، وأصبح من الصعب الوصول إلى بيانات المرضى، وأصبح الكثير من المعدات الطبية المتصلة بشبكة *Wi Fi* غيرمتاحة واضطر المستشفى إلى وقف العمليات لعدة أسابيع فى أثناء إصلاح الأنظمة التالفة، وفى الوقت نفسه طالب المتسللون بفدية ضخمة لاستعادة الوصول إلى أنظمة الكمبيوتر المقفلة، وبعد إبلاغ الشرطة ذكر الجناة أن الهجوم امتد من غير قصد إلى المستشفى المحلى (٣٢).

يتضح مما سبق أن الجرائم والهجمات السيبرانية تستهدف بشكل مباشر الأنظمة والقطاعات الحيوية للدول من أجل ابتزازهم وتحقيق أغراض خاصة.

٣- تدمير البنية التحتية واستهداف الأمن القومى للدولة :

لا يشمل مفهوم الحرب السيبرانية استهداف المعدات والأنظمة العسكرية فحسب، 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، ومن ثم يتمخَّض النزاع السيبرانى عن عواقب تهدد الحياة إذا تم إفساد البنية التحتية للمعلومات. فقد ورد فى تقرير *(ITU-2017)* بالمؤتمر العالمى لتنمية الاتصالات فى مشروع الخطة الاستراتيجية للاتحاد ضرورة وجود بنية تحتية وآمنة للاتصال وتكنولوجيا المعلومات، وضرورة تعزيز تنمية البنية التحتية والخدمات بما فى ذلك بناء الثقة والأمن فى استخدام الاتصالات وتكنولوجيا المعلومات، وضرورة وجود بنية تمكينية وتعزيزية تنظيمية وسياسات مواتية للتنمية المستدامة للاتصالات وتكنولوجيا المعلومات. حيث 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 كاف بالأمن والبنية التحتية(٣٣).

ومن إحدى الوثائق الأساسية لفهم كيفية تأثير الهجمات على البنية التحتية على المجتمعات: مسح القصف الاستراتيجى الذى أجرته الولايات المتحدة فى أثناء الحرب العالمية الثانية وبعدها خلال الحرب؛ حيث أطلقت بريطانيا وأمريكا آلاف القاذفات الثقيلة التى ألقت ملايين الأطنان من المتفجرات الشديدة الانفجار على ألمانيا سعيًا إلى شل بنيتها التحتية وتدمير قاعدتها الصناعية وكسر إرادة السكان فى مواصلة الحرب، وقد توقع منظرو الحرب الجوية الأوائل أن مثل هذا الهجوم من شأنه أن يشل الهدف ومع تزايد وتيرة الهجوم الجوى لم يتمكن الألمان من منع تدهور اقتصادهم وانهياره (٣٤)

٤- سرقة الهُويّة الرقمية والبيانات الخاصة :

تُعد سرقة الهُويّة الرقمية من أخطر الجرائم التى تهدد مستخدمى الإنترنت ومستقبل الخدمات الإلكترونية، حيث قد تتعرض البيانات الشخصية للمستخدم إلى السرقة بهدف انتحال شخصيته والاستيلاء على ممتلكاته وأمواله أو للزج باسمه فى تعاملات مشبوهة أو غير قانونية. وعادة ما يستعين سارق الهُويّة بمعلومات موجودة بالفعل على الإنترنت وبخاصة على مواقع وشبكات التواصل الاجتماعية والمهنية المفتوحة أو قواعد البيانات والمعلومات القومية، والشبكات الخاصة بالخدمات الحكومية، وخدمات الضمان الاجتماعى وشبكات الرعاية الصحية، ومواقع التجارة الإلكترونية، والأسواق الافتراضية، وشبكات المدفوعات الإلكترونية، والصرافات الآلية، وبورصة الأوراق المالية. فضلًا على أنه قد تتعرض الأدوات والأنظمة المستخدمة فى إجراء المعاملات الإلكترونية للسرقة أو التخريب، مما يشكل خطرًا كبيرًا على مصالح المستخدمين ومستقبل الخدمات الإلكترونية، وقد

تؤثر الهجمات الموسعة على القطاع المالى الوطنى بوجه عام، كما تتعرض البيانات الخاصة بالمؤسسات العامة والشركات للسرقة مما يكبدها خسائر مادية وأدبية فادحة، فضلاً عن الإضرار بسمعتها وخسارتها عملاءها وأصولها الأدبية، مما قد يضر بالاقتصاد الوطنى بوجه عام(٣٥).

سادسًا: آليات وجهود الدولة المصرية فى التصدى للجرائم والهجمات السيبرانية فى ضوء رؤية مصر ٢٠٣٠:

كشف مؤشر الأمن السيبرانى *(GCI)* الصادر عن الاتحاد الدولى للاتصالات أن مصر قد احتلت المرتبة (٢٣) عالميًا من بين (١٩٣) دولة، كما جاءت فى المرتبة الأولى عالميًا فى تنافسية قطاعى الإنترنت والهاتف خلال عام ٢٠٢١م وفقًا لمؤشر المعرفة العالمى، كما تَقَدّم ترتيب مصر (٣) مراكز فى مؤشر جاهزية الحكومة للذكاء الاصطناعى الصادر من مجموعة أكسفورد لتصل إلى المركز (٦٢) مقارنة بالمركز (٦٥) عن عام ٢٠٢٢م(٣٦).

ويمكن الإشارة إلى آليات وجهود الدولة المصرية فى مجال الأمن السيبرانى وقوتها فى التصدى للجرائم والهجمات السيبرانية على النحو التالى:

(١) التشريعات الوطنية المصرية:

- الدستور المصرى:

نصَّت المادة (٣١) من الدستور المصرى - وفقًا للتعديلات الدستورية التى أدخلت عليه فى ٢٣ أبريل ٢٠١٩م- على أن: «الفضاء المعلوماتى جزء أساسى من منظومة الاقتصاد والأمن القومى، تلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه على النحو الذى ينظمه القانون»(٣٧).

- قانون مكافحة جرائم تقنية المعلومات (القانون رقم ١٧٥ لسنة ٢٠١٨م):

لأول مرة ينُص القانون على «تجريم الممارسات السيبرانية غير المشروعة» مثل إنشاء المواقع الإلكترونية التى تحث على الإرهاب، التزوير السيبرانى وغير ذلك. ووفقًا له تتحدد العقوبة وفقًا لحجم وطبيعة الجريمة، ففى حالة جرائم تقنية المعلومات، تُفرض عقوبات كبيرة؛ لما لتلك الجرائم من تداعيات جسيمة على الأمن القومى، علاوة على العقوبات الأخرى المتعلقة بجرائم الاختراق السيبرانى، والتزوير وغير ذلك(٣٨).

- القانون رقم ٩٤ لسنة ٢٠١٥م لمكافحة الإرهاب:

هو قانون شامل للتصدى لجرائم الإرهاب وتمويله من الناحيتين الموضوعية والإجرائية وقد تناول المحاور اللازمة للمجابهة القانونية للإرهاب بإجراءات ناجزة وعقوبات رادعة، حيث استمدت أحكام ذلك القانون من قرارات مجلس الأمن والصكوك والاتفاقيات الدولية والإقليمية فى مجال مكافحة الإرهاب، كما قرر المعاقبة على الشروع فى ارتكاب الجريمة الإرهابية أو التحريض عليها بذات العقوبة المقررة للجريمة التامة، ولم يترتب على التحريض أثر. ونظم المُشَرِّع فيه ضوابط تجميد الأموال والمنع من التصرف فيها، وأوجب القانون تخصيص دوائر لنظر الجنح والجنايات والاستئناف والطعون فى قضايا الجرائم الإرهابية(٣٩).

(٢) التدخل الاستراتيجى:

أ- الاستراتيجية الوطنية للذكاء الاصطناعى:

أطلقت مصر الاستراتيجية الوطنية للذكاء الاصطناعى بهدف استخدام هذه التكنولوجيا فى دعم تحقيق أهداف التنمية المستدامة، فضلًا عن القيام بدور رئيس فى تيسير التعاون الإقليمى فى المنطقتين الإفريقية والعربية، وترسيخ مكانة مصر بوصفها طرفًا دوليًا فاعلًا فى ذلك المجال. يأتى ذلك فى إطار حرص مصر على التفاعل مع معطيات العصر الرقمى الذى تتوالى فيه المُستجدات التكنولوجية كل يوم(٤٠).

ب ـ الاستراتيجية الوطنية للأمن السيبرانى (٢٠١٧م-٢٠٢١م):

أطلق المجلس الأعلى للأمن السيبرانى، التابع لرئاسة مجلس الوزراء، برئاسة وزير الاتصالات وتكنولوجيا المعلومات، الاستراتيجية الوطنية للأمن السيبرانى (٢٠١٧م-٢٠٢١م)، حيث تمثل الهدف الاستراتيجى فى مواجهة المخاطر السيبرانية، وتعزيز الثقة فى البنى التحتية للاتصالات والمعلومات وتطبيقاتها وخدماتها فى شتى القطاعات الحيوية وتأمينها من أجل تحقيق بيئة رقمية آمنة وموثوقة للمجتمع المصرى بمختلف أطيافه، وذلك فى إطار جهود الدولة لدعم الأمن القومى وتنمية المجتمع المصرى (٤١).

ج- استراتيجية الحوسبة السحابية الحكومية:

تسعى استراتيجية الحوسبة السحابية الحكومية لتحسين كفاءة الحكومة وأدائها، فهى تساعد فى تقديم القيمة المثلى من خلال زيادة الكفاءة التشغيلية والاستجابة بشكل أسرع للاحتياجات المتكاملة. ويدعم نموذج الحوسبة السحابية الوكالات الحكومية التى تعانى الحاجة لتوفير خدمات سريعة للغاية موثوقة ومبتكرة على الرغم من القيود المفروضة على الموارد(٤٢).

د ــ إطلاق الاستراتيجية الخمسية الوطنية للأمن السيبرانى (٢٠٢٣م – ٢٠٢٧م) :

أطلق المجلس الأعلى للأمن السيبرانى التابع لرئاسة مجلس الوزراء، برئاسة وزير الاتصالات وتكنولوجيا المعلومات، الاستراتيجية الخمسية الوطنية للأمن السيبرانى (٢٠٢٣م -٢٠٢٧م)، وتتمثل أهمية وجود استراتيجية وطنية للأمن السيبرانى فى نقطتين أساسيتين: **أولاهما**: التصدى للحوادث السيبرانية التى تزايدت من حيث عددها ومصادرها، **وثانيتهما**: صناعة فرص للسوق المصرية عن طريق بناء كوادر بشرية وتطوير صناعة وطنية تشارك فى زيادة إجمالى الناتج المحلى *(GDP)*[٤٣].

(٣) إنشاء المراكز الوطنية والمجالس المتخصصة :

أ ـ المركز الوطنى للاستعداد لطوارئ الحاسبات والشبكات:

أنشئ المركز فى عام ٢٠٠٩م من أجل مواجهة خطر الإرهاب السيبرانى وغيره من التهديدات السيبرانية، ويختص بتقديم الدعم للقطاعين الحكومى والمالى من خلال الدعم التقنى والميدانى، وتقديم التقارير الفنية للجهات المختصة لحماية البنية التحتية القومية للمعلومات المهمة وبخاصة فى قطاع تكنولوجيا المعلومات والاتصالات والقطاع المالى، وهناك فريق عمل متخصص على أعلى مستوى يقومون على مدار الساعة بمراقبة الأمن السيبرانى والاستجابة للحوادث، وتحليل معامل الطب الشرعى الرقمى، وتحليل البرمجيات الخبيثة والهندسة العكسية، ويتمثل هدفه الرئيس فى تعزيز أمن البنية التحتية المصرية للاتصالات والمعلومات من خلال اتخاذ إجراءات استباقية وجمع وتحليل المعلومات الخاصة بالحوادث الأمنية والتنسيق والوساطة بين الأطراف المعنية فى حل تلك الحوادث الأمنية والتعاون الدولى مع مختلف الفرق المعنية بالاستجابة لطوارئ الحاسبات والشبكات فى الدول الأخرى[٤٤].

ب ــ المركز المصرى للاستجابة لطوارئ الحاسب الآلى (سيرت):

لقد قام الجهاز القومى لتنظيم الاتصالات بتأسيس المركز المصرى لاستجابات طوارئ الحاسب الآلى (سيرت) فى إبريل ٢٠٠٩م حيث يعمل به فريق من ستة عشر متخصصًا، ويقدم الفريق الدعم الفنى على مدار ٢٤ ساعة لحماية البنى التحتية الحيوية للمعلومات. ويقدم المركز منذ عام ٢٠١٢م الدعم لمختلف الجهات عبر قطاعات تكنولوجيا المعلومات والاتصالات والخدمات المصرفية والحكومية من أجل مساعدتهم فى مواجهة تهديدات الأمن السيبرانى بما فى ذلك هجمات الحرمان من الخدمة. وتتركز المهمة الرئيسية للمركز المصرى للاستجابة للطوارئ المعلوماتية (سيرت) حول توفير نظام للإنذار المبكر ضد البرمجيات الخبيثة والهجمات الإلكترونية التى تنتشر بنطاق واسع ضد البنية التحتية الحيوية للمعلومات المصرية[٤٥].

جـ ــ إنشاء المجلس الأعلى لتأمين البنى التحتية للاتصالات والمعلومات (المجلس الأعلى للأمن السيبرانى) :

تم إنشاؤه فى ١٦ ديسمبر ٢٠١٤م، لحماية وتأمين البنى التحتية للاتصالات وتكنولوجيا المعلومات، ويهدف المجلس الأعلى للأمن السيبرانى إلى وضع خطط استراتيجية للتصدى للهجمات السيبرانية فضلاً عن الإشراف على كيفية تنفيذ الاستراتيجيات الوطنية لمواجهة التهديدات السيبرانية، ويتم تحديث تلك الاستراتيجية بشكل دورى، بالإضافة إلى ذلك أنشئ المكتب التنفيذى والأمانة الفنية للمجلس الأعلى للأمن السيبرانى الذى يختص بالإشراف على تنفيذ أعمال المجلس والخطط التى يُقرها فى ضوء الاستراتيجيات والسياسات المحددة، وتختص الأمانة الفنية للمجلس بالقيام بالأعمال والدراسات الفنية التى يطلبها المجلس ومكتبه التنفيذى، وبتنظيم وإطلاق حملات وطنية دورية للتوعية بمخاطر التهديدات السيبرانية فى مختلف القطاعات، وتنظيم ورش عمل ودورات للتوعية بالأمن السيبرانى على المستوى القطاعى وإعداد مواصفات نظم التبادل الآمن للمعلومات المتعلقة بتأمين البنى المعلوماتية للدولة[٤٦].

سابعاً : المعايير والنموذج المقترح لمجابهة المخاطر الاجتماعية للجرائم والهجمات السيبرانية على الأمن الرقمى فى مصر:

١ - المعايير المقترحة لمواجهة المخاطر الاجتماعية للجرائم والهجمات السيبرانية على الأمن الرقمى:

- المعيار الأول : وضع قوانين ولوائح الأمن السيبرانى:

تتطلب مواجهة الجرائم والتهديدات السيبرانية وضع القواعد القانونية التى تشمل جميع أنواع الجرائم السيبرانية والتهديدات المستمرة، إلى جانب وضع التشريعات واللوائح الضامنة لحماية حقوق الأفراد فى الفضاء الرقمى، وتأمين بياناتهم الشخصية والوعى بعدم مشاركة المعلومات الشخصية.

بالإضافة إلى تعزيز التعاون بين أجهزة إنفاذ القانون وأجهزة القضاء على المستويين الوطنى والدولى، وأن تعمل القوانين على حماية الأطفال والشباب فى الفضاء الرقمى.

- المعيار الثانى : التوعية المجتمعية:

حيث يتطلب مواجهة الجرائم والتهديدات السيبرانية كفاية برامج ومداخل توعية المواطنين من مختلف الفئات والأطياف ووجوب إشراك المجتمع المدنى فى ديناميكيتها.

- المعيار الثالث: تعزيز الشراكات:

مع القطاعات الحكومية والخاصة والمؤسسات والمنظمات الدولية وأصحاب المصلحة.

- المعيار الرابع : بناء القدرات:

وذلك عن طريق وضع واستحداث مناهج تدريبية معتمدة يتم تنفيذها من قبل الجامعات والمعاهد المعتمدة، وبناء قدرات المنظمات المختلفة من أجل القيام بوظائفها فى مجال الأمن السيبرانى والمعاملات الإلكترونية والتحول الرقمى.

- المعيار الخامس : بيئة حيوية للأمن السيبرانى:

تعتمد على تشجيع البحث العلمى والابتكار فى مجال الأمن السيبرانى وحماية الشبكات وأنظمة المعلومات، وتعزيز المهارات وتأهيل الكفاءات الوطنية فى مجال السلامة المعلوماتية والجرائم الإلكترونية.

- المعيارالسادس: استحداث طرائق لتأمين النظام الأمنى الرقمى:

والذى يجب أن يتركز على ثلاثة أركان أساسية :

- **الوقاية من الهجمات والتهديدات السيبرانية:** باستخدام جدار الحماية وبرنامج الأمان لمكافحة الفيروسات والديدان والبرامج الضارة.
- **الكشف والتعافى:** سرعة اكتشاف التهديدات والثغرات وتحديث الأنظمة.
- **سرعة رد الفعل:** إذا تم اكتشاف الهجمات ولم يتم التصدى لها يصبح الاكتشاف ليست له قيمة وأهمية فلابد من توافرجاهزية قدرات التصدى والدفاع والاستجابة للهجمات المختلفة.

المعيار السابع : الابتكار والاستثمار:

يتطلب مجابهة المخاطر الرقمية مثل الجريمة السيبرانية، والإرهاب، والهجمات الإلكترونية، واستقطاب الكوادر البشرية وتأهيلها التأهيل المناسب، وتعزيز الابتكار والاستثمار والتميز فى مجال الأمن السيبرانى التى ترتكز على تطوير البنية التحتية المرقمنة بما يُسهم فى تحقيق رؤية مصر ٢٠٣٠.

٢- نموذج مقترح لتطوير وتعزيز أنظمة الأمن الرقمى والسلامة المعلوماتية لمجابهة الجرائم والهجمات السيبرانية :

أ- مداخل مواجهة الجرائم والهجمات السيبرانية وتشمل:

الحوكمة - تنمية وعى أفراد المجتمع - إنفاذ القانون - التعاون الدولى - التدريب وبناء القدرات - دعم البحث والتطوير والابتكار .

ب- شركاء مواجهة الجرائم والهجمات السيبرانية (أصحاب المصلحة):

المنظمات الحكومية - القطاع الخاص - المنظمات الدولية - الأوساط الأكاديمية.

ج- أدوات مواجهة الجرائم والهجمات السيبرانية:

المؤتمرات - الندوات - الملتقيات - اللجان - ورش العمل - البرامج - الحملات - الاجتماعات - الاتفاقيات الدولية.

د- القضايا المستهدفة:

الجرائم الإلكترونية- الهجمات السيبرانية - البرمجيات الخبيثة - الإرهاب السيبرانى - الحرب السيبرانية - التجسس السيبرانى - التخريب السيبرانى - الذكاء الاصطناعى - إنترنت الأشياء - الهندسة الاجتماعية - البلوكتشين - المرونة السيبرانية - الحوسبة الكمومية - الاختراق الحيوى - الهويات المزيفة - هجمات الأجهزة - فقدان الخصوصية.

هـ - الفئات المستهدفة:

على مستوى الأفراد :

الأطفال — طلاب الجامعات — الموظفون — الشباب ضحايا الجرائم الإلكترونية — الشباب ضحايا الهجمات الإلكترونية — الشباب مُرتكب الجرائم الإلكترونية.

على مستوى الدول :

- الدول التى ترتفع فيها معدلات الجرائم الإلكترونية.
- الدول التى تعانى الهجمات السيبرانية.
- الدول التى تعانى الإرهاب السيبرانى.
- الدول التى تعانى جرائم الهندسة الاجتماعية.

و- المخرجات المستهدفة وتتمثل فى:

- إرساء أفضل الممارسات فى مجال الأمن الرقمى والمعلوماتى والسيبرانى وضوابطها الأمنية والتقنية.
- التقليل من وطأة المخاطر والهجمات والجرائم الإلكترونية.
- تحسين قدرات التعامل مع الحوادث الرقمية والأمنية.
- بناء إطار تنظيمي لحماية التقنيات الحالية والناشئة.
- اكتشاف الهجمات السيبرانية وتعزيز طرائق التعافى من الحوادث السيبرانية.

ثامناً : نتائج الدراسة ومقترحاتها :

١ - النتائـــج :

خلصت الدراسة إلى عدة نتائج وتوصيات يمكن الإشارة إليها على النحو التالى:

١-هناك عدد من التعريفات الوطنية والدولية لمصطلحات الأمن السيبرانى- الأمن الرقمى- الجرائم السيبرانية، وأن المفاهيم تتطور بشكل مستمر نتيجة التطورات التكنولوجية والتقنيات الناشئة والتغيرات فى أنظمة الاتصالات وتكنولوجيا المعلومات، وإنه من الصعوبة بمكان وضع تعريف جامع مانع للأمن الرقمى نظرًا لحداثته من جانب، ونتيجة لاختلاف المدلول بين الباحثين من جانب آخر.

٢- يُعد الأمن الرقمى ضرورة مُلحَّة فرضها التطور التكنولوجى ومنظومة التحول الرقمى لضمان سلامة وأمن المعلومات وتكنولوجيا الاتصالات.

٣- هناك صعوبة فى حصر أنماط الجرائم الإلكترونية والهجمات السيبرانية، نتيجة اعتماد مُرتكبيها من المجرمين على التقنيات والوسائل المرتبطة بالتقدم التكنولوجى الذى تزداد وتيرة تغيره يومًا بعد يوم.

٤-أظهرت نتائج الدراسة أن مرتكبى الهجمات السيبرانية يقومون باستغلال نقاط الضعف المعروفة لدى الأفراد، والمنظمات والدول، الأمر الذى يترتب عليه ضعف القدرة على تصنيف الأضرار وتعاظم المخاطر المترتبة على ذلك، إلى جانب صعوبة التحديد الدقيق للتكاليف المباشرة وغير المباشرة الناجمة عنها.

٥- أوضحت النتائج أن الجرائم الإلكترونية والهجمات السيبرانية تؤثر تأثيرًا بالغ الخطورة على البناء الاجتماعى للدول فهى جرائم عابرة للقارات؛ وتستهدف البنية التحتية والأنشطة الاجتماعية التى تتعلق بالأفراد والمجتمع ككل.

٦- تشكل الجرائم الإلكترونية والسيبرانية تهديدًا خطيرًا ومتزايدًا، وأن تكاليف مجابهة الآثار الناجمة عنها واكتشافها تُعد كثيرة جدًا بالنسبة للدول لأنها تعتمد كليًا على التكنولوجيا والتقنيات الحديثة والمتطورة.

٧- تؤدى الجرائم والهجمات السيبرانية إلى تقويض ثقة الأفراد فى الحكومات لأنها قادرة على إحداث ضرر هائل، الأمر الذى يتطلب من الحكومة حماية مواطنيها من جيل جديد من الهجمات السيبرانية.

٨- بينت النتائج أن معظم دول العالم تعرضت للعديد من الجرائم والهجمات السيبرانية التى استهدفت القطاعات الحيوية فى المجتمع، ومن ثم قامت بإصدار القوانين المختلفة من أجل التغلب على التهديدات والأخطار الناجمة عنها.

٩- أوضحت النتائج أن مصر من أوائل الدول التى قامت بسن التشريعات والقوانين وإنشاء المراكز والمجالس المتخصصة، ووضع الكثير من الاستراتيجيات التى تتضمن العديد من البرامج الاستراتيجية المختلفة، وعقد المؤتمرات من أجل حماية الدولة من مخاطر الجرائم والهجمات السيبرانية، ولتحقيق بيئة رقمية آمنة وموثوقة للمجتمع المصرى بمختلف أطيافه.

٢ - المقترحـــات :

فى ضوء ما كشفت عنه النتائج تقترح الدراسة مايلى:

١- أن مواجهة الجرائم والتهديدات السيبرانية تتطلب توفيرمزيد من المعرفة والوعى لدى مستخدمى الإنترنت والشبكات الاجتماعية لتفادى الحوادث والأضرار السيبرانية المباشرة وغير المباشرة التى من الممكن أن يتعرضوا أو يكونوا ضحايا لها، وتوفيرًا للتكاليف التى تتكبدها الدولة فى مواجهتها.

٢- وجوب تفعيل استراتيجيات وقوانين وسياسات الأمن الرقمى؛ لأنها من سُبل تحقيق الأمن القومى لمصر، ونشر ثقافة الأمن الرقمى بين مختلف فئات المجتمع وتضمينها فى مختلف الخطط والاستراتيجيات على جميع المستويات الإقليمية والدولية، حتى تتحقق السلامة السيبرانية والأمن المعلوماتى بما يتماشى مع التغيرات المتسارعة.

٣- يجب على الجامعات والمعاهد والمنظمات المختلفة الاهتمام بتطوير منهج الأمن السيبرانى وتدريسه، بحيث يصبح مطلبًا جامعيًا، حتى تتوافر الخبرة العلمية والتقنية اللازمة فى التصدى للهجمات والتهديدات الإلكترونية المتطورة والمتغيرة .

٤- يجب على صانعى السياسات والأكاديميين والمتخصصين التفكير فى أفضل السبل لتطبيق مفهوم إدارة المخاطرالمرتبطة بحماية الخصوصيات والبيانات والمعلومات من التهديدات المحتملة.

٥- يُعد بناء الثقة أمرًا ضروريًا فى البيئة الرقمية وفى تطويراستراتيجيات حماية الخصوصية والتصدى

لنقاط الضعف والتهديدات الجديدة الناشئة، ومواجهة المخاطر الأمنية وإشكالات الخصوصية، فيجب الاهتمام بأخلاقيات بناء الثقة لأنها تؤثر على البيئة الرقمية.

٦- يجب على صُناع القرار التعامل مع مخاطر الأمن الرقمى باعتباره خطرًا يهدد الأمن السياسى، والاقتصادى، والاجتماعى والتكنولوجى.

٧- يجب على الاستراتيجيات الوطنية التى تهدف إلى تحقيق الأمن الرقمى أن تعكس رؤية المجتمع وتعزز حماية الخصوصية فى الفضاء الرقمى الذى يعتمد على البيانات كركيزة أساسية.

٨- من شأن استراتيجيات الأمن الرقمى أن تُسهم فى تعزيز التعاون مع أصحاب المصلحة والاستفادة منهم وإرساء أفضل الطرق والوصول إلى الحلول الممكنة لإدارة مخاطر الفضاء الرقمى وتعزيز الممارسات الجيدة لإدارة المخاطر.

٩- يجب على المؤسسات والشركات الصغيرة والناشئة زيادة الوعى لدى القائمين على إدارة التكنولوجيا الرقمية بمخاطر الخصوصية.

١٠- تعزيز الوعى بمفهوم المواطنة الرقمية لدى جيل الشباب الذين تتراوح أعمارهم بين ١٨ و٤٠ عامًا بكيفية التعامل مع البيئة الرقمية ووسائل التكنولوجيا المختلفة لتحقيق الفوائد الشخصية والمجتمعية بطرق إيجابية.

١١- نشر الوعى حول الاستخدام الآمن للبطاقات الإلكترونية لتعزيز التصدى للاستخدامات غير المشروعة فى المعاملات الإلكترونية.

١٢- العمل على إصدار نشرات بصفة دورية حول الجرائم الإلكترونية والتهديدات السيبرانية وآليات التعامل معها.

١٣- تأهيل العاملين فى مختلف القطاعات وبالأخص قطاع أمن المعلومات بالمستجدات والتطورات فى مجال تكنولوجيا المعلومات والاتصالات للحد منها ومكافحتها.

١٤- يجب تسريع الجهود لتفعيل تشريعات الذكاء الاصطناعى بما يتماشى مع رؤية مصر ٢٠٣٠ والاستراتيجية الوطنية للأمن السيبرانى.

الهوامش :

(1) OECD Digital Economy Papers Managing Digital security and Privacy Risk, 2016 Ministerial Meeting on the Digital Economy, Back Growth Report the Digital Economy innovation, Growth and social prosperity, 2016, p, 5.

(2) Oced digital Economy papers ,Op cit p.5

(3) Bernat :Enhancing the digital security of critical activities, Going Digital Toolkit Note, 2021 No. 17. P.4.

(4) Op. Cit, P. 4.

(٥) ذياب البدانية : الجرائم الإلكترونية، المفهوم والأسباب، ورقة مقدمة فى الملتقى العلمى- الجرائم المستحدثة فى ظل التغيرات والتحولات الإقليمية والدولية ٢-٢٠١٤/٩/٤م عمان - الأردن.

(٦) فوزى حسين الزبيدى : منهجية تقييم مخاطر الأمن القومى : دراسة تحليلية لمنهجية تقييم مخاطر الأمن القومى NSRA، رؤى استراتيجية، مركز الإمارات للدراسات والبحوث الاستراتيجية، المجلد (٣) العدد (١١)، ٢٠١٥م، ص ١١ى.

(٧) أولريش بك، مجتمع المخاطر العالمى بحثًا عن الأمن المفقود، ترجمة علا عادل وآخرون، القاهرة، المركز القومى للترجمة، ٢٠١٣م، ص٢١٤.

(8) Jarvis, Darry I S "Theorizing Risk: Ulrich Beck, Globalization and Risk of the Risk society" Lee Kaun Yew School of public policy, National University of sing pore , p 3

(٩) نجوان أحمد عاصم عبد الجواد : الجريمة السيبرانية وتأثيرها على الأمن القومى المصرى، دراسة سوسيو تحليلية، جامعة الفيوم، مجلة كلية الآداب، الإنسانيات والعلوم الاجتماعية، المجلد (١٥)، العدد (١) يناير ٢٠٢٣م، ص ٢١٠٤.

(١٠) إسلام فوزى : الأمن السيبرانى، الأبعاد الاجتماعية والقانونية، تحليل سوسيولوجى، القاهرة، المجلة الاجتماعية القومية، المجلد السادس والخمسون، العدد الثانى، مايو ٢٠١٩م.

(١١) مكتب الأمم المتحدة المعنى بالمخدرات والجريمة : دراسة شاملة عن الجريمة السيبرانية، فيينا، ٢٠١٣م، ص ٧.

(12) Suhasini Verma, (et. al): Mounting Cases of Cyber- Attacks and Digital payment. India, 2023.P.61

(13) Yuchong Li, &, Qinghui Liu: A Comprehensive Review Study of Cyber- attacks and Cyber Security; Emerging trends and recent developments Energy reports,2021, P.8179.

(١٤) سامى محمد بونيف : دور الاستراتيجيات الاستباقية فى مواجهة الهجمات السيبرانية، الردع السيبرانى إنموذجًا.المجلة الجزائرية للحقوق والعلوم السياسية، المجلد (٤) العدد (٧)، ٢٠١٩م، ص ١٢

(15) Yuchong Li, & Qinghui, Liu, 2021 op. cit., P.8180

(١٦) خورجى فلوريس كابيخاس، عائشة عفيفى، نيكولاى لوزنيسكى : الأمن السيبرانى فى مؤسسات منظومة الأمم المتحدة تقرير وحدة التفتيش المشتركة، الأمم المتحدة ، ٢٠٢١م، ص٧.

(١٧) أمنية عبيشات: الأمن الرقمى – قراءة فى مفهومه واستراتيجية حمايته، مجلة المسار للدراسات القانونية والسياسية، المجلد (١) العدد (١) ٢٠٢٣م، ص ١٠٠ .

(١٨) مركز هردو لدعم التعبير الرقمى: الأمن الرقمى وحماية المعلومات، الحق فى استخدام شبكات آمنة، القاهرة ،٢٠١٧ ، ص ٦

(١٩) أمينة عبيشات (٢٠٢٣م): مرجع سابق ، ص ٩٩.

(20) Sakshi Singh&Suresh Kumar: THE TIMES OF CYBER ATTACKS: ACTA TECHNICA CORVINIENSIS – Bulletin of Engineering TOME XIII 2020 FASCICULE 3, July – September, P 134-135

(٢١) نشرة تكنولوجيا المعلومات والاتصالات للتنمية فى المنطقة العربية – اللجنة الاقتصادية والاجتماعية لغربى آسيا (الإسكوا): الأمم المتحدة نيويورك، العدد (١٨) ٢٠١٢م، ص ١٠ .

(22) Digital Notes on cyber security, Department of information technology, Malla Reddy College of Engineering & Technology India ,2021, pp7-9

(٢٣) الاستراتيجية الوطنية للأمن السيبرانى (٢٠٢٣م –٢٠٢٧م)، وزارة الاتصالات وتكنولوجيا المعلومات.

(٢٤) خورخى فلوريس كابيخاس، عائشة عفيفى، نيكولاى لوزنيسكى ٢٠٢١م. مرجع سابق ، ص ١٤

(25) Lynn Batten, & Gang Li, : Application and Techniques in information security international conference Atis 6 th . Osaka University, Osaka, Japan.2016 P, 60

(٢٦) تقرير (TTU) الوثيقة RPM-ARB 1044- A قطاع تنمية الاتصالات، الاجتماع الإقليمى التحضيرى للمؤتمر العالمى لتنمية الاتصالات ٢٠١٠م لمنظمة الدول العربية، دمشق، الجمهورية العربية السورية، ١٧–١٩ يناير ٢٠١٠م.

(27) Nadiya Kostyuk, & yuri M. Zhukov: Invisible Digital front can cyber Attacks Shape Battlefield Events. Journal of Conflict Resolution, Vol 63 (2), 2019, P. 318.

(28) Hemraj, Saini, & Yerra shanker Rao, & T.C Panda: cyber- crimes and their Impacts, A review. International Journal of Engineering research and Application (IJERA) no/2. 2012, P 209

(29) Mario Spremié, & Alen Simunic,: Cyber Security Challenges in Digital Economy,2018. P 979.

(30) Proceedings of the world congress on Engineering No/ 1 London

(31) Mario Spremié, &, Alen, Simunic ,Op. cit., p 979

(32) Ryan Shandler, &, Miguel Alberto Gomez: The hidden threat of cyber- attacks- undermining public confidence in government, Journal of information technology & politics .2022 p 363

(٣٣) إسلام فوزى : مرجع سابق ، ص ١١٢ – ١١٣.

(34) James A. Lewis: Op Cit.

(٣٥) الاستراتيجية الوطنية للأمن السيبرانى (٢٠١٧م - ٢٠٢١م).

(36) https://mcit.gov.eg/Ar/Media_Center/Press_Room/Press_Releases/67460

تاريخ الدخول ٢٤/٤/ ٢٠٢٤م الساعة ١١,٥٠ مساء

(٣٧) الدستور المصرى ٢٠١٤م.

(٣٨) القانون رقم ١٧٥ لسنة ٢٠١٨م قانون مكافحة جرائم تقنية المعلومات.

(٣٩) القانون رقم ٩٤ لسنة ٢٠١٥م لمكافحة الإرهاب.

(٤٠) الاستراتيجية الوطنية للذكاء الاصطناعى، يوليو ٢٠٢١م . وزارة الاتصالات وتكنولوجيا المعلومات .

(٤١) الاستراتيجية الوطنية للأمن السيبرانى (٢٠١٧م – ٢٠٢١م) .

(٤٢) استراتيجية الحوسبة السحابية الحكومية ، ٢٠١٤ م ، وزارة الاتصالات وتكنولوجيا المعلومات .

(٤٣) الاستراتيجية الوطنية للأمن السيبرانى (٢٠٢٣م – ٢٠٢٧م) .

(٤٤) مصر والأمن السيبرانى : الهيئة العامة للاستعلامات https://www.sis.gov.eg/Story/258293 تاريخ الدخول ٢٥/٤/٢٠٢٤م الساعة ١١:٤٧ مساء

(٤٥) المرجع السابق

(٤٦) المرجع السابق

الانعكاسات والمخاطر الاجتماعية للجرائم والهجمات السيبرانية على الأمن الرقمى وآليات المواجهة فى ضوء رؤية مصر ٢٠٣٠

أ.م.د/ أسماء جابر مهران
أستاذ علم اجتماع الجريمة المساعد - كلية الآداب - جامعة أسيوط

المستخلص :

هدفت الدراسة الراهنة إلى تقديم تحليل سوسيولوجى للمخاطر الاجتماعية للجرائم والهجمات السيبرانية على الأمن الرقمى ورصد آليات وجهود الدولة المصرية فى ضوء رؤية مصر ٢٠٣٠ .

لقد أظهرت النتائج أن الأمن الرقمى يعد ضرورة ملحة فرضها التطور التكنولوجى ومنظومة التحول الرقمى لضمان سلامة وأمن المعلومات وتكنولوجيا الاتصالات .

بيَّنت النتائج أن معظم دول العالم تعرَّضت للعديد من الجرائم والهجمات السيبرانية التى استهدفت القطاعات الحيوية فى المجتمع، ومن ثم قامت بإصدار القوانين المختلفة من أجل التغلب على التهديدات والأخطار الناجمة عنها. أوضحت النتائج أن مصر من أوائل الدول التى قامت بسن التشريعات والقوانين وإنشاء المراكز والمجالس المتخصصة، ووضع الكثير من الاستراتيجيات التى تتضمن العديد من البرامج الاستراتيجية المختلفة، وعقد المؤتمرات من أجل حماية الدولة من مخاطر الجرائم والهجمات السيبرانية، ولتحقيق بيئة رقمية آمنة وموثوقة للمجتمع المصرى بمختلف أطيافه.

الكلمات المفتاحية : الجرائم السيبرانية – الهجمات السيبرانية – الأمن الرقمى – رؤية مصر ٢٠٣٠

The social repercussions and risks of crimes and cyber-attacks on digital security and coping mechanisms in light of Egypt's Vision 2030

Prof / Asmaa Jaber Mahran
Assistant Professor of Sociology of Criminology
Faculty of Arts - Assiut University

Abstract:

The current study aimed to provide a sociological analysis of the social risks of crimes and cyber attacks on digital security and monitor the mechanisms and efforts of the Egyptian state in light of Vision 2030. The results showed that digital security is an urgent necessity imposed by technological development and the digital transformation system to ensure the safety and security of information and communications technology.

The results showed that most countries in the world were exposed to many crimes and cyber attacks that targeted vital sectors of society, and then issued various laws in order to overcome the threats and dangers resulting from them. The results showed that Egypt is one of the first countries to enact legislation and laws, establish specialized centers and councils, develop many strategies that include many different strategic programs, and hold conferences in order to protect the state from the dangers of crimes and cyberattacks, and to achieve a safe and reliable digital environment for Egyptian society of all walks of life.

Keywords: Cyber-crimes - cyber-attacks - digital security - Egypt Vision 2030