



■ أ.م.د/ أسماء جابر مهران

أستاذ علم اجتماع الجريمة المساعد - كلية الآداب - جامعة أسيوط

## الانعكاسات والمخاطر الاجتماعية للجرائم والهجمات السيبرانية على الأمن الرقمي وآليات المواجهة

في ضوء رؤية مصر ٢٠٣٠

### مقدمة :

كشفت نتائج دراسة استقصائية أجرتها منظمة التعاون الاقتصادي والتنمية ، حول الاقتصاد الرقمي، أن الحكومات قد وضعت مجال الأمن في المرتبة الثانية، والخصوصية في المرتبة الثالثة من بين ٣١ مجالاً ممكناً للسياسات ذات الأولوية. وفي الصدد نفسه يولى المستهلكون اهتماماً متزايداً بالخصوصية في البيئة الرقمية؛ حيث أظهرت نتائج دراسة أجرتها (CIGI-IPSOS) عام ٢٠١٤م لمستخدمي الإنترنت في ٢٤ دولة حول أمن الإنترنت والثقة إلى أن (٦٤%) من المشاركين أصبحوا أكثر قلقاً بشأن الخصوصية مما كانوا عليه من قبل عام (١).

ولم تُعد احتمالية أن تؤدي حوادث الأمن الرقمي إلى أضرار مادية أمراً نظرياً، فقد دمرت هجمات الأمن الرقمي أجهزة الطرد المركزية النووية في إيران، وولدت أضراراً مادية هائلة في مصنع الصلب الألماني عام ٢٠١٤م، فضلاً عن انقطاع التيار الكهربائي في أوكرانيا في عامي ٢٠١٥م، ٢٠١٧م، علاوة على ذلك أظهر حادث *Note petya* في عام ٢٠١٧م أن الهجمات الأمنية الرقمية يمكن أن تُعطل بشكل كبير العمليات وسلاسل التوريد لعدة أيام في مجالات مثل لوجستيات الحاويات العالمية (ميرسك) وإنتاج الأدوية (ميرك). وفي عام ٢٠٢١م أجبر هجوم إلكتروني شركة (Colonia Pipeline Company) على إغلاق أكبر خط أنابيب في الولايات المتحدة لمدة ٦ أيام، مما أدى إلى نقص الوقود عبر الساحل الشرقي (٤).

### إشكالية الدراسة :

لقد انتقل الناس من العالم الواقعي إلى العالم الافتراضي، وكذلك انتقلت الجريمة. ولنا أن نتصور حجم

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



### أهمية الدراسة:

#### • الأهمية العلمية:

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

ب- يُعد إضافة للتراث النظري دراسة مفهوم جديد وهو الأمن الرقمي الذي يختلف عن الأمن المعلوماتي.

#### • الأهمية العملية:

إن رصد التأثيرات الاجتماعية للجرائم والهجمات السيبرانية على الأمن الرقمي مهم للأفراد من أجل رفع الوعي بمخاطرها وكيفية مواجهتها، كما أنه مهم للمسؤولين 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 في فحص الانعكاسات والمخاطر الاجتماعية للجرائم والهجمات والتهديدات السيبرانية على الأمن الرقمي، ورصد آليات المواجهة في 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 في البيئة السيبرانية.

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

هـ - رصد آليات وجهود الدولة المصرية في التصدي للجرائم والهجمات السيبرانية في ضوء رؤية ٢٠٣٠.

و- التوصل إلى تصور مقترح لمجابهة المخاطر الاجتماعية للجرائم والهجمات السيبرانية على الأمن الرقمي في مصر .

### منهجية الدراسة:

ستعتمد الدراسة الراهنة على منهجية تحليل النظم التي وضعها (ديفيد إيستون-David Easton) في تحليل

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

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

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

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

٤- مسارات البيانات (*trails data*) التي خلقت فرصًا لارتكاب سرقة الهوية. ومن ناحية أخرى، فإن عدد ضحايا الجريمة الإلكترونية على ارتفاع، خاصة الذين يعانون خسارة مالية، أو المهنيين أو المطاردين؛ وذلك نظرًا للزيادة في عدد مستخدمي الإنترنت. هذا وتمثل

الجريمة الإلكترونية المجال الجديد من الأبحاث في مجال علم الجريمة<sup>(٥)</sup>.

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

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

وينبثق عن هذا التساؤل الرئيس عدة أسئلة فرعية وهي:

أ- ما أجيال الهجمات السيبرانية؟

ب- ما طبيعة وأشكال الجرائم والهجمات السيبرانية؟

ج- ما جهات التهديد في البيئة السيبرانية؟

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

هـ - ما آليات وجهود الدولة المصرية في التصدي للهجمات السيبرانية في ضوء رؤية ٢٠٣٠؟

و- ما التصور المقترح لمجابهة المخاطر الاجتماعية للجرائم والهجمات السيبرانية على الأمن الرقمي في مصر؟

التي نتج عنها عدم الحفاظ على الخصوصية الثقافية للأفراد، والاستيلاء على بعض المعلومات الرقمية للأفراد والمؤسسات والدول<sup>(٩)</sup>.

### ٢- نظرية تشكيل البنى لرصد مقومات الأمن الرقمي:

يمكن النظر إلى نظرية التشكيل البنائي (Theory of Structuration) عند أنتوني جيدنز باعتبارها إسهاماً مهماً في طرح رؤية نظرية لحل إشكالية اجتماعية، هي إشكالية (البنية- الفاعلية Agency - Structure) حيث تعد ممارسات الأمن الرقمي والسيبراني في ضوء هذه النظرية من أهم مظاهر تشكيل البنية الاجتماعية، وذلك في ضوء القضايا الرئيسية التي دعا إليها أنتوني جيدنز، وهي كالاتي<sup>(١٠)</sup>:

- أ- تتطوى عملية تشكيل البنية على المشاركة النشطة للذوات الفاعلة والممارسات اليومية الناجح.
  - ب- يفرض البناء حدوداً على الفعل الإنساني، كما يبسر تحقيق هذا الفعل «ازدواجية البناء».
  - ج- تشكل البنية في ضوء تفاعل بين المعاني والمعايير والقوة.
  - د- تتشكل البنية من خلال الأداء المهاري للأعضاء عبر مفهوم المكان والزمان.
- ومن ثم يتضح أن الفاعلين، وهم مُرتكبي الجرائم والهجمات السيبرانية، يقومون بالتأثير السلبي على البناء الاجتماعي، ويشكلونه وفق رؤيتهم المزدوجة، وذلك من خلال الممارسات الإجرامية المتكررة، فهم قوة فاعلة في الفضاء الرقمي لأنهم يمتلكون القوة التخريبية، ويتصرفون وفق معتقدات خاصة، وعبر أساليب مختلفة تؤدي في مجملها إلى جملة من المخاطر الاجتماعية المؤذية للفرد والمجتمع بكامله.

### تتضمن الدراسة العناصر التالية:

- ١- الإطار المفاهيمي للدراسة.
- ٢- أجيال الهجمات السيبرانية.
- ٣- أنماط الجرائم والهجمات السيبرانية.
- ٤- أنواع جهات التهديد في البيئة السيبرانية (فئات المهاجمين السيبرانيين): .
- ٥- المخاطر الاجتماعية للجرائم والهجمات السيبرانية على الأمن الرقمي .
- ٦- آليات وجهود الدولة المصرية في التصدي للجرائم والهجمات السيبرانية في ضوء رؤية مصر ٢٠٣٠ .

الظواهر والنظم الاجتماعية من خلال تحليل الظاهرة إلى عناصرها كمدخلات، ومن ثم دراسة تأثير العوامل المتغيرة عليها كعمليات، وصولاً إلى المخرجات ومقارنتها بالمدخلات عبر ما يسمى التغذية العكسية وذلك لدراسة العلاقة بين السبب والنتيجة<sup>(٦)</sup>.

وعليه ستنقسم موضوعات الدراسة في ضوء هذه المنهجية وفق الترتيب التالي:

أ- المدخلات : التي ستشمل مفاهيم الدراسة مثل (الجرائم السيبرانية - الهجوم السيبراني - الأمن الرقمي) .

ب- العمليات : التي ستشمل دراسة وتحليل الأهداف المتصلة بموضوع الدراسة، التي تتمثل في الوقوف على أجيال الهجمات السيبرانية، طبيعة وأشكال الجرائم والهجمات السيبرانية، جهات التهديد في البيئة السيبرانية، المخاطر الاجتماعية للجرائم والهجمات السيبرانية على الأمن الرقمي، وجهود وآليات الدولة المصرية في التصدي للجرائم والهجمات السيبرانية في ضوء رؤية ٢٠٣٠ .

ج- المخرجات : ستشمل المنهجية المُطوّرة التي تحاول الدراسة التوصل إليها كمقترح أو منهجية جديدة في التصدي لمخاطر الجرائم والهجمات السيبرانية على الأمن الرقمي .

### المنظور السوسيولوجي لدراسة الأمن الرقمي:

١- نظرية مجتمع المخاطر لرصد انعكاسات الجرائم

السيبرانية على الأمن الرقمي:

يعد أورليش بك عالم الاجتماع الألماني هو مؤسس هذه النظرية، وأول من أشار إلى مصطلح المخاطرة، ومجتمع المخاطر العالمي، وتتناول نظرية المخاطر الوجود المتزايد لانعدام اليقين المنتشر في ظل التغيرات التي تحدث في المجتمع، حيث اندثر المجتمع الصناعي مُفسحاً المجال لمجتمع المخاطر التقني والتكنولوجي أو المجتمع المعلوماتي، وهو ما يُطلق عليه مُنظرو ما بعد الحداثة "عالم الفوضى" الذي تغيب معه أنماط الحياة المستقرة<sup>(٧)</sup>.

إن مجتمع المخاطر العالمي يمثل فترة فريدة للغاية من التاريخ قادرة على تدمير نفسها بنفسها تكنولوجياً<sup>(٨)</sup>. وتأسسًا على ذلك نجد أن الأمن الرقمي يشهد مخاطر عدة نتيجة الثورة الرقمية التي يشهدها المجتمع، وما تمخض عنها من تطور في أنماط الجرائم والهجمات السيبرانية



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

## أولاً : الإطار المفاهيمي للدراسة : ١- مفهوم الجريمة السيبرانية :

الجريمة السيبرانية تتمثل في عدد محدود من الأعمال التي تمس سرية البيانات أو النظم الحاسوبية وسلامة توافرها، أما الأعمال المنفذة بواسطة الحواسيب الرامية إلى تحقيق مكاسب شخصية أو مالية أو إحداث أضرار بما في ذلك أشكال الجريمة المتصلة بالهوية وبمحتوى الحواسيب، فهي تدرج كلها ضمن نطاق أوسع من مصطلح الجريمة السيبرانية، ولا يمكن تطويعها بسهولة لتتضمن ضمن تعاريف قانونية لمصطلح جامع. الأمر الذي يلزم تعريف وتحديد الأعمال الأساسية التي 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 الدولي، حيث يفضل التركيز على الأدلة الإلكترونية فيما يخص أي جريمة بدلاً من التركيز على تركيبة واسعة واصطناعية لـ «الجريمة السيبرانية»<sup>(١١)</sup>.

بالمعنى الأوسع تشير الجرائم السيبرانية (الإلكترونية) إلى « أي سلوك غير قانوني يستخدم فيه الكمبيوتر أو الإنترنت كأداة أو هدف أو كليهما، فهذا السلوك غير القانوني 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 الإجرامي يتم ارتكابها بشكل متكرر من قبل أشخاص ذوي سلوك مدمر وإجرامي لمجموعة متنوعة من الأسباب بما في ذلك الانتقام أو المال أو المغامرة». ووفقاً (لقاموس أكسفورد) فإن مصطلح الجريمة السيبرانية يُقصد به: « الأنشطة الإجرامية التي يتم تنفيذها باستخدام أجهزة الكمبيوتر أو الإنترنت ». كما يتم تعريف الجريمة السيبرانية على أنها « نشاط إجرامي يحدث على أو باستخدام الأجهزة أو الويب أو أي تقنية أخرى معترف بها». واستخلاصاً لما سبق فإن الجريمة السيبرانية هي: « تلك الأنواع التي يُعد جنسها جريمة تقليدية، ولكن يكون فيها الكمبيوتر شيئاً أو موضوع السلوك الذي يشكل جريمة»<sup>(١٢)</sup>.

## ٢- مفهوم الهجوم السيبراني :

تقع الهجمات السيبرانية في سياق أوسع- ما يسمى تقليدياً- عمليات المعلومات أو العمليات المعلوماتية، التي تستخدم بشكل متكامل القدرات الرئيسة للحرب الإلكترونية والشبكات النفسية والحاسوبية، الخداع العسكري والعمليات الأمنية وذلك بالتنسيق مع الدعم الخاص والقدرات ذات الصلة. هذا، وقد تباينت تعريفات الهجوم السيبراني من قبل متخصصين في المجالين القانوني والفني، ومن أهم هذه التعريفات أن الهجمات السيبرانية هي: « الإجراءات التي تتخذها الدول لاختراق أجهزة الكمبيوتر لدولة أو دول أخرى لإحداث ضرراً وتعطيل»<sup>(١٣)</sup>.

كما تُعرّف الهجمات السيبرانية على أنها: «فعل يقوِّض من قدرات وظائف الشبكة المعلوماتية من خلال استغلال نقاط الضعف، ما يمنح المهاجم القدرة على التلاعب بالنظام، وتُعرّف كذلك بأنها الاستغلال المعتمد لأنظمة الكمبيوتر والشبكات المعتمدة على التكنولوجيا من خلال البرمجيات الضارة»<sup>(١٤)</sup>.

ويمكننا التمييز وإظهار الفروق بين الجريمة السيبرانية والحرب السيبرانية والهجوم السيبراني على النحو التالي:

**الجريمة السيبرانية (الإلكترونية):** هي إجراءات سيبرانية يتم اتخاذها فقط من قبل المهاجمين غير الحكوميين، ويتم تنفيذ الإجراءات السيبراني بواسطة نظام كمبيوتر، وهو ما يُعد انتهاكاً للقانون الجنائي.

**الهجوم السيبراني والحرب السيبرانية:** الغرض من الهجوم السيبراني هو تدمير وتعطيل تشغيل شبكة الكمبيوتر، وأن الهجوم يتم لأغراض سياسية أو أمنية، وأن آثار الهجوم السيبراني هي آثار الهجوم المسلح نفسه أو الفعل السيبراني الذي حدث في سياق هجوم مسلح<sup>(١٥)</sup>.

## ٣- مفهوم الأمن الرقمي :

غالباً ما تتضمن معايير الصناعة الدولية والوطنية الخاصة بأمن المعلومات تعريفاً للأمن الرقمي. مع الإشارة إلى إنه لا يوجد تعريف مقبول عالمياً أو إجماع عالمي حول ما يشمله المصطلح بدقة. وفي سياق الأمم المتحدة لاحظ المفتشون أنه لا توجد أي توجيهات على نطاق المنظومة من المنتديات المشتركة بين الوكالات ذات الصلة توصي بالإجماع بتعريف معين باعتباره موثقاً للمنظومة، كما أن الأطر التنظيمية لدى المنظمات لا تحاول بشكل منهجي فرض تعريف للأمن الرقمي. ووفقاً للاتحاد الدولي



للأمن الرقمي بأنه: «مجموعة من الأدوات والسياسات والمفاهيم الأمنية والضمانات الأمنية والمبادئ التوجيهية، ونهج إدارة المخاطر، والإجراءات، والتدريب، وأفضل الممارسات، والضمان، والتقنيات التي 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 في البيئة السيبرانية، ويسمى الأمن السيبراني لضمان تحقيق وحفظ الخصائص الأمنية لأصول المنظمة والمستخدمين ضد المخاطر الأمنية ذات الصلة في البيئة السيبرانية، وتتألف الأهداف الأمنية العامة من التوافر، والسلامة التي يمكن أن تشمل المصدقية وعدم التنصل، والسرية» (١٦).

أما وكالة الأمن الرقمي الأوروبية في أول تشريع أصدرته عام ٢٠٠١م عرّفت الأمن الرقمي بأنه: «قدرة النظام المعلوماتي على مقاومة محاولات الاختراق، أو الحوادث غير المتوقعة التي تستهدف البيانات المتداولة أو المخزنة وفق إطار توافقي» (١٧).

كما يُعرّفه مركز هردول لعدم التعبير الرقمي بأنه: «كيفية استخدام شبكة الإنترنت استخدامًا فعالاً دون التعرض لأي تهديدات أو مخاطر أو مراقبة تهدد خصوصية وسرية المعلومات» (١٨).

وما يمكن الإشارة إليه بخصوص مفهوم الأمن الرقمي هو أنه يشكل أداة لتوحيد التعاون في مجال مكافحة الجرائم الرقمية بمختلف أصنافها والوقوف في وجه مخاطرها. والجدير بالذكر أنه من قبيل الدول التي اهتمت بمفهوم الأمن الرقمي كانت بريطانيا وتحل المرتبة الأولى عالمياً وفقاً لتصنيف المؤشر العالمي للأمن السيبراني (جى سى آى) الذى أصدره الاتحاد الدولي للاتصالات التابع للأمم المتحدة ثم الولايات المتحدة الأمريكية، ومن الدول العربية التى اهتمت بالأمن الرقمي وفقاً للتصنيف جاءت المملكة العربية السعودية فى المرتبة الأولى عربياً 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

**ومن أمثلة الهجمات السيبرانية من الجيل الأول:**  
- (١٩٨٢ - *ELK Cloner*) 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 أيضاً 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 :**  
- (٢٠٠٠ - *I Love you*) - دودة تصيب عشرات الملايين من أجهزة *SQL* - *Windows 2005* - *slammer* - رفض الخدمة لـ ٧٥٠٠٠ مضيف.

**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 :**  
- (٢٠٠٥ - *Stux net 10*) - تطوير ترعاه الدولة ويستهدف أنظمة *SCADA* فى البنية التحتية الحيوية بما فى ذلك البرنامج النووى الإيرانى.

- هجوم (*DYN-2016*) ليس فيروساً مستقلاً ولكنه هجوم ضخم لرفض الخدمة الموزعة (*DDOS*) على مزود *DNS* الرئيسى.



(التصيد بالبريد الإلكتروني - *Email Phishing*) ، التصيد من خلال «تسميم محركات البحث» - (*SEO Poisoning*) .

- هجمات حجب الخدمة (*DRDOS/DDOS/DOS*)
- هجوم الوسيط (*Man-In-The-Middle*) ، ومن أنواع هجوم الوسيط (التصيد على الواي فاي - سرقة بريد إلكتروني أو *SSL* - انتحال *IP* أو *HTTPS* أو *DNS*) .

### ب. الهجمات القائمة على النظام:

والهجمات التي 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 السيبراني (٢٠٢٣م-٢٠٢٧م) في مصر عن تزايد أعداد الهجمات السيبرانية في الأعوام السابقة بشكل كبير، كما تسببت الهجمات السيبرانية في خسائر ضخمة للاقتصاد العالمي، مما يشكل عبئاً كبيراً 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 الهوية ، ويمكن الإشارة إليهم على النحو التالي (٢٣) :

### الجريمة السيبرانية (*Crime Cyber*) :

إن الجريمة السيبرانية هي المسؤولة 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 في 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*) :

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

الجيل الخامس (٢٠١٧م) : حيث بدأت هجمات ضخمة واسعة النطاق بتمويل من بعض الحكومات في عام ٢٠١٧م حتى تتمكن العديد من الشركات من تنفيذها. فالجرائم السيبرانية لها شبكات الإنترنت والضمان الخاصة بها. ومن أمثلة الاعتداءات من الموجة الخامسة : - (*Wannacry-2017*) هجوم كبير ببرامج الفدية يؤثر على ٢٠٠٠٠٠ جهاز كمبيوتر في ١٥٠ دولة.

### ثالثاً: أنماط الجرائم والهجمات السيبرانية :

#### ١ - أنماط الجرائم السيبرانية :

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

ومن الأفعال المُصنفة كجرائم سيبرانية مايلي (٢١):

- التعدي على البيانات المعلوماتية.
- التعدي على الأنظمة المعلوماتية.
- إساءة استعمال الأجهزة أو البرامج المعلوماتية.
- الجرائم على الأموال.
- الاستغلال الجنسي للقاصرين.
- التعدي على الملكية الفكرية للأعمال الرقمية.
- جرائم البطاقات المصرفية والنقود الإلكترونية.
- الجرائم التي تمس 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 التي تحدث على مواقع الويب أو تطبيقات

الويب، ومن أمثلتها :

- هجمات الحقن : وتشمل حقن (*SQL*)، وحقن (*XML*)، وحقن التعليمات البرمجية، وحقن السجل وهو الهجوم الذي يتم فيه حقن بعض البيانات في تطبيق ويب لمعالجة التطبيق وجلب المعلومات المطلوبة .
- انتحال (*DNS*) .
- هجمات التصيد ويشمل : (التصيد بالرمح - *Spear phishing*) ، (تصيد الحيتان - *whaling*) ، (التصيد الاحتيالي - *Smishing*) ، (التصيد الصوتي - *Vishing*) ،

• **مجرمو الفضاء السيبراني:**

جهات فاعلة تتخرب في نشاط إجرامي مُمكن سيبرانيًا (الجرائم الشائعة مثل الاحتيال والسرقة والابتزاز وما إلى ذلك) بمساعدة الوسائل الحاسوبية أو في نشاط إجرامي معتمد على الفضاء السيبراني، مثل نشر الفيروسات أو البرمجيات الخبيثة وغيرها من الأنشطة التي لا يمكن ارتكابها إلا من خلال الوسائل المُحوسبة.

• **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 التي ترعاها دولة:**

جهات فاعلة متطورة للغاية وذات موارد جيدة يصعب عادة اكتشاف أنشطتها أو تعقبها أو تحديدها، يمكن أن تلتزم 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 تدريباً سيئاً، أو مقدمة الخدمة المتعاقد معهم والمدربين تدريباً سيئاً، إلى جانب جهات أخرى.

**خامساً: المخاطر الاجتماعية للجرائم والهجمات السيبرانية على الأمن الرقمي:**

تسببت الجرائم السيبرانية (الإلكترونية) في 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 التي يتحملها الاقتصاد العالمي بسبب حوادث الجرائم الإلكترونية تزيد على (٤٠٠) مليار دولار، وإن تأثيرات الجرائم السيبرانية ستزداد تدريجياً مع ازدهار وظائف الأعمال عبر الإنترنت، ومع اتصال المزيد من الشركات والعملاء في العالم بالإنترنت. كما تسبب الجريمة السيبرانية في البلدان المتقدمة في معدل التوظيف حيث كشفت نتائج الأبحاث أن الخسارة الناجمة عن الجريمة السيبرانية يمكن أن تلحق الضرر بـ (٢٠٠٠٠) وظيفة

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.

- **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.

- **التهديدات الداخلية (Insiders):**

مع تزايد استخدام تكنولوجيا المعلومات داخل المؤسسات، تزايدت احتمالات المخاطر الناتجة، قصدًا أو دون قصد، من الموظفين المخوّلين باستخدام أنظمة المعلومات. فقد يكون هؤلاء الموظفون مصدرًا لتهديد المؤسسات عن طريق سرقة بيانات حساسة تؤدي إلى خسائر مادية جسيمة أو إلى تهديد سمعة المؤسسة. وقد يعرض الموظف بيانات المؤسسة الحساسة للخطر دون قصد عن طريق بعض الهجمات السيبرانية مثل التصيد الإلكتروني (Phishing) أو الهندسة الاجتماعية (Social Engineering).

- **الهواة (Kiddies Script):**

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

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

وتتمثل الأنواع الرئيسية لجهات التهديد في البيئة السيبرانية على النحو التالي (٢٤):

• **القرصنة الحاسوبية:**

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

• **نشاط القرصنة الحاسوبية:**

لديهم دوافع محددة ويرون في نشاطهم شكلاً من أشكال العصيان المدني أو وسيلة للتعبير عن الذات سياسياً أو أيديولوجياً.



## الانعكاسات والمخاطر الاجتماعية للجرائم والهجمات السيبرانية على الأمن الرقمي وآليات المواجهة في ضوء رؤية مصر ٢٠٣٠

أ.م.د/ أسماء جابر مهران

مرتفع، فقد أظهرت نتائج الدراسات الاستقصائية التي أجريت إلى أن ما يصل إلى (٨٠٪) من الشركات التي شملتها الدراسة اعترفت بخسائر مالية بسبب انتهاكات أجهزة الكمبيوتر تُقدر قيمتها بمبلغ ٤٥٠ مليون دولار، وما يقرب من (١٠٪) من الاحتيال المالي، حيث تتزايد الهجمات الجديدة التي تؤثر على سرية أنظمة الكمبيوتر وسلامتها وتوافرها يمكن أن تتراوح ما بين سرقة معلومات التعريف الشخصية وهجمات رفض الخدمة (٢٨).

وتماشياً مع ما تم ذكره فإنه في السنوات الخمس عشرة الماضية حدث العديد من المشكلات التي أثرت على التحول من أمن المعلومات إلى الأمن الرقمي: مثل زيادة التهديدات الداخلية (كحوادث تسريبات الويكي الداخلية وانتهاكات البيانات والمهمات الخبيثة من الداخل، والتقنيات الناشئة وتحديدًا التقنيات الرقمية ذات التوجه الخارجي التي تتيح الاتصال، والتقنيات المعرفية، الذكاء الاصطناعي وتكنولوجيا الهاتف المحمول، ووسائل التواصل الاجتماعي، وما إلى ذلك)، وزيادة التهديدات الخارجية مثل (البرامج الضارة وبرامج الفدية واختراق البيانات، الأجهزة المترابطة وأجهزة الإنترنت والحرب السيبرانية والهجمات التي ترعاها الدولة). فعلى سبيل المثال قدّر معهد بويتومون أن التكاليف المباشرة لاختراق البيانات في عام ٢٠١٧م قد بلغت (٦٢، ٣) مليون دولار أمريكي (٢٩).

ليس هذا فحسب، حيث إن أقسام الشرطة في جميع أنحاء البلاد قد ذكرت أنها تلقت عددًا متزايدًا من جرائم الاحتيال والسرقة الكبرى في السنوات الأخيرة، ويتزامن هذا مع الاتجاه الوطني الناتج عن زيادة استخدام الكمبيوتر والأعمال التجارية عبر الإنترنت. وفي عام ٢٠٠٤م حققت الجريمة السيبرانية عائدًا أعلى من الاتجار بالمخدرات، ومن المتوقع أن تنمو أكثر مع توسع استخدام التكنولوجيا في البلدان النامية. كما أظهرت النتائج لعام ٢٠١١م أن أكثر من (٧٤) مليون شخص في الولايات المتحدة كانوا ضحايا للجرائم الإلكترونية في عام ٢٠١٠م، وأدت هذه الأعمال الإجرامية إلى خسائر مالية تُقدّر بقيمة ٣٢ مليار دولار، وأن (٦٩٪) من البالغين المتصلين بالإنترنت قد وقعوا ضحايا لجرائم الإنترنت مما أدى إلى وقوع مليون ضحية لجرائم الإنترنت يوميًا. ويعتقد الكثير من الناس أن الجريمة السيبرانية هي جرائم تتعلق بممارسة الأعمال التجارية عبر الإنترنت (٣٠).

أمريكية أي ما يقرب من ثلث الانخفاض في التوظيف، كما أن (٣٠٠٠) شركة في الولايات المتحدة تعرضت للاختراق في عام ٢٠١٤م، كما تكبدت البرازيل (٤، ١) مليار دولار بسبب أضرار الهجمات السيبرانية، لأن أكثر من (٤٥٪) من البرازيليين يستخدمون الإنترنت، وفي عام ٢٠١٣م خسرت فرنسا (١٩، ٥) مليون دولار بسبب الهجمات السيبرانية، كما أنها واجهت ١٩٠٠ هجوم سيبراني منذ الهجوم الإرهابي في عام ٢٠١٤م، حيث إن نحو (٩١٪) من الشركات في المملكة المتحدة و (٣١٪) من الأسر لديها إمكان الوصول إلى الإنترنت، كما تُقدّر التكلفة المحسوبة للجرائم الإلكترونية في المملكة المتحدة بنحو (٢٧) مليار دولار (٢٥).

وتأسسًا على ذلك جاء في تقرير الاتحاد الدولي للاتصالات (ITU) عام ٢٠١٠م بشأن الأبعاد الاجتماعية للأمن الرقمي أن الثورة الرقمية غيرت كيفية التعامل التجاري وكيفية عمل الحكومات، وأدت العولمة والتقدم التكنولوجي إلى إضعاف البنية التحتية، وبالتالي جعلتها هدفًا محتملاً لهجمات إرهابية، حيث تواجه البلدان مخاطر حقيقية، وأن المجرمين يقومون باستغلال مواطن الضعف التي تعانيها أنظمة المعلومات الدقيقة من أجل تعطيل البنية التحتية والموارد الأساسية ومن ثم تهديد الأمن القومي (٢٦).

وتتمثل أهم المخاطر الاجتماعية للجرائم والهجمات السيبرانية على الأمن الرقمي في:

### ١- زيادة معدلات الجرائم المستحدثة والخسائر الناجمة عنها :

في ٢٢ ديسمبر ٢٠١٥م هاجم قراصنة شبكة الكهرباء في أوكرانيا وعطلوا أنظمة التحكم المستخدمة في المحطات الكهربائية الفرعية عن بعد، وتركوا الناس والجزء الغربي من البلاد دون كهرباء لعدة ساعات، وقد أُلقت الخدمة الأوكرانية (SBU) اللوم على الحكومة الروسية في الهجوم السيبراني، وهو الاتهام الذي وجد دعمًا لاحقًا في تحليل البرامج الضارة من قبل شركات خاصة لأمن الكمبيوتر. كان الاختراق الأوكراني هذا أول حالة مُعترفًا بها علنًا لهجوم سيبراني تسبب بنجاح في انقطاع التيار الكهربائي كما أنها مجرد واحدة من آلاف الأنشطة السيبرانية ومعظمها منتشرة تحدث جنبًا إلى جنب مع القتال الجسدي في أوكرانيا (٢٧).

ونظرًا لأن المستهلك أصبح يعتمد بشكل متزايد على أجهزة الكمبيوتر والشبكات والمعلومات التي يتم استخدامها لتخزينها وحفظها، فإن خطر التعرض للجرائم الإلكترونية



التحتية للمعلومات. فقد ورد في تقرير (ITU-2017) بالمؤتمر العالمي لتنمية الاتصالات في مشروع الخطة الاستراتيجية للاتحاد ضرورة وجود بنية تحتية وأمنة للاتصال وتكنولوجيا المعلومات، وضرورة تعزيز تنمية البنية التحتية والخدمات بما في ذلك بناء الثقة والأمن في 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 التكنولوجي من هذه الخسائر في حالة عدم إيلاء اهتمام كاف بالأمن والبنية التحتية<sup>(٣٣)</sup>.

ومن إحدى الوثائق الأساسية لفهم كيفية تأثير الهجمات على البنية التحتية على المجتمعات: مسح القصف الاستراتيجي الذي أجرته الولايات المتحدة في أثناء الحرب العالمية الثانية وبعدها خلال الحرب؛ حيث أطلقت بريطانيا وأمريكا آلاف القاذفات الثقيلة التي ألفت ملايين الأطنان من المتفجرات الشديدة الانفجار على ألمانيا سعياً إلى شل بنيتها التحتية وتدمير قاعدتها الصناعية وكسر إرادة السكان في مواصلة الحرب، وقد توقع منظرو الحرب الجوية الأوائل أن مثل هذا الهجوم من شأنه أن يشل الهدف ومع تزايد وتيرة الهجوم الجوي لم يتمكن الألمان من منع تدهور اقتصادهم وانهيائه<sup>(٣٤)</sup>.

### ٤- سرقة الهوية الرقمية والبيانات الخاصة :

تعد سرقة الهوية الرقمية من أخطر الجرائم التي تهدد مستخدمى الإنترنت ومستقبل الخدمات الإلكترونية، حيث قد تتعرض البيانات الشخصية للمستخدم إلى السرقة بهدف انتحال شخصيته والاستيلاء على ممتلكاته وأمواله أو للزج باسمه في تعاملات مشبوهة أو غير قانونية. وعادة ما يستعين سارق الهوية 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. فضلاً على أنه قد تتعرض الأدوات والأنظمة المستخدمة في إجراء المعاملات الإلكترونية للسرقة أو التخريب، مما يشكل خطراً كبيراً على مصالح المستخدمين ومستقبل الخدمات الإلكترونية، وقد

### ٢- استهداف القطاعات الحيوية :

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

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

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

#### القومي للدولة :

لا يشمل مفهوم الحرب السيبرانية استهداف المعدات والأنظمة العسكرية فحسب، ولكن أيضاً استهداف البنية التحتية الحيوية للمجتمع بما في ذلك الشبكات الذكية وشبكات المراقبة الإشرافية وحياسة البيانات (SCADA) التي تسمح لها بالعمل والدفاع عن نفسها، ومن ثم يتمخض النزاع السيبراني عن عواقب تهدد الحياة إذا تم إفساد البيئة



للمجابهة القانونية للإرهاب بإجراءات ناجزة وعقوبات رادعة، حيث استمدت أحكام ذلك القانون من قرارات مجلس الأمن والصكوك والاتفاقيات الدولية والإقليمية في مجال مكافحة الإرهاب، كما قرر المعاقبة على الشروع في ارتكاب الجريمة الإرهابية أو التحريض عليها بذات العقوبة المقررة للجريمة التامة، ولم يترتب على التحريض أثر. ونظم المُشرع فيه ضوابط تجميد الأموال والمنع من التصرف فيها، وأوجب القانون تخصيص دوائر لنظر الجرح والجنايات والاستئناف والطعون في قضايا الجرائم الإرهابية<sup>(٣٩)</sup>.

### (٢) التدخل الاستراتيجي:

#### أ- الاستراتيجية الوطنية للذكاء الاصطناعي:

أطلقت مصر الاستراتيجية الوطنية للذكاء الاصطناعي بهدف استخدام هذه التكنولوجيا في دعم تحقيق أهداف التنمية المستدامة، فضلاً عن القيام بدور رئيس في تيسير التعاون الإقليمي في المنطقتين الإفريقية والعربية، وترسيخ مكانة مصر بوصفها طرفاً دولياً فاعلاً في ذلك المجال. يأتي ذلك في إطار حرص مصر على التفاعل مع معطيات العصر الرقمي الذي تتوالى فيه المُستجدات التكنولوجية كل يوم<sup>(٤٠)</sup>.

#### ب - الاستراتيجية الوطنية للأمن السيبراني

(٢٠١٧م - ٢٠٢١م):

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

#### ج- استراتيجية الحوسبة السحابية الحكومية:

تسعى استراتيجية الحوسبة السحابية الحكومية لتحسين كفاءة الحكومة وأدائها، فهي تساعد في تقديم القيمة المثلّي من خلال زيادة الكفاءة التشغيلية والاستجابة بشكل أسرع للاحتياجات المتكاملة. ويدعم نموذج الحوسبة السحابية الوكالات الحكومية التي تعاني الحاجة لتوفير خدمات سريعة للغاية وموثوقة ومبتكرة على الرغم من القيود المفروضة على الموارد<sup>(٤٢)</sup>.

تؤثر الهجمات الموسعة على القطاع المالي الوطني 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 الوطني بوجه عام<sup>(٣٥)</sup>.

### سادساً: آليات وجهود الدولة المصرية في التصدي للجرائم والهجمات السيبرانية في ضوء رؤية مصر ٢٠٣٠:

كشف مؤشر الأمن السيبراني (GCI) الصادر عن الاتحاد الدولي للاتصالات أن مصر قد احتلت المرتبة (٢٢) عالمياً من بين (١٩٢) دولة، كما جاءت في المرتبة الأولى عالمياً في تنافسية قطاعي الإنترنت والهاتف خلال عام ٢٠٢١م وفقاً لمؤشر المعرفة العالمي، كما تقدّم ترتيب مصر (٣) مراكز في مؤشر جاهزية الحكومة للذكاء الاصطناعي الصادر من مجموعة أكسفورد لتصل إلى المركز (٦٢) مقارنة بالمركز (٦٥) عن عام ٢٠٢٢م<sup>(٣٦)</sup>.

ويمكن الإشارة إلى آليات وجهود الدولة المصرية في مجال الأمن السيبراني وقوتها في التصدي للجرائم والهجمات السيبرانية على النحو التالي:

### (١) التشريعات الوطنية المصرية:

#### - الدستور المصري:

نصّت المادة (٣١) من الدستور المصري - وفقاً للتعديلات الدستورية التي أدخلت عليه في ٢٣ أبريل ٢٠١٩م- على أن: «الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي، تلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه على النحو الذي ينظمه القانون»<sup>(٣٧)</sup>.

#### - قانون مكافحة جرائم تقنية المعلومات (القانون رقم

١٧٥ لسنة ٢٠١٨م):

لأول مرة يُنص القانون على «تجريم الممارسات السيبرانية غير المشروعة» مثل إنشاء المواقع الإلكترونية التي تحت على الإرهاب، التزوير السيبراني وغير ذلك. ووفقاً له تتحدد العقوبة وفقاً لحجم وطبيعة الجريمة، ففي حالة جرائم تقنية المعلومات، تُفرض عقوبات كبيرة؛ لما لتلك الجرائم من تداعيات جسيمة على الأمن القومي، علاوة على العقوبات الأخرى المتعلقة بجرائم الاختراق السيبراني، والتزوير وغير ذلك<sup>(٣٨)</sup>.

#### - القانون رقم ٩٤ لسنة ٢٠١٥م لمكافحة الإرهاب:

هو قانون شامل للتصدي لجرائم الإرهاب وتمويله من الناحيتين الموضوعية والإجرائية وقد تناول المحاور اللازمة

المعلومات والاتصالات والخدمات المصرفية والحكومية من أجل مساعدتهم في مواجهة تهديدات الأمن السيبراني بما في ذلك هجمات الحرمان من الخدمة. وتتركز المهمة الرئيسية للمركز المصري للاستجابة للطوارئ المعلوماتية (سيرت) حول توفير نظام للإنذار المبكر ضد البرمجيات الخبيثة والهجمات الإلكترونية التي تنتشر بنطاق واسع ضد البنية التحتية الحيوية للمعلومات المصرية (٤٥).

**ج - إنشاء المجلس الأعلى لتأمين البنى التحتية للاتصالات والمعلومات (المجلس الأعلى للأمن السيبراني) :**  
تم إنشاؤه في ١٦ ديسمبر ٢٠١٤م، لحماية وتأمين البنى التحتية للاتصالات وتكنولوجيا المعلومات، ويهدف المجلس الأعلى للأمن السيبراني إلى وضع خطط استراتيجية للتصدي للهجمات السيبرانية فضلاً عن الإشراف على كيفية تنفيذ الاستراتيجيات الوطنية لمواجهة التهديدات السيبرانية، ويتم تحديث تلك الاستراتيجية بشكل دوري، بالإضافة إلى ذلك أنشئ المكتب التنفيذي والأمانة الفنية للمجلس الأعلى للأمن السيبراني الذي يختص بالإشراف على تنفيذ أعمال المجلس والخطط التي يقرها في ضوء الاستراتيجيات والسياسات المحددة، وتختص الأمانة الفنية للمجلس بالقيام بالأعمال والدراسات الفنية التي يطلبها المجلس ومكتبه التنفيذي، وتنظيم وإطلاق حملات وطنية دورية للتوعية بمخاطر التهديدات السيبرانية في مختلف القطاعات، وتنظيم ورش عمل ودورات للتوعية بالأمن السيبراني على المستوى القطاعي وإعداد مواصفات نظم التبادل الآمن للمعلومات المتعلقة بتأمين البنى المعلوماتية للدولة (٤٦).

**سابعاً : المعايير والنموذج المقترح لمجابهة المخاطر الاجتماعية للجرائم والهجمات السيبرانية على الأمن الرقمي في مصر :**

**١ - المعايير المقترحة لمواجهة المخاطر الاجتماعية للجرائم والهجمات السيبرانية على الأمن الرقمي :**  
- المعيار الأول : وضع قوانين ولوائح الأمن السيبراني :

تتطلب مواجهة الجرائم والتهديدات السيبرانية وضع القواعد القانونية التي تشمل جميع أنواع الجرائم السيبرانية والتهديدات المستمرة، إلى جانب وضع التشريعات واللوائح الضامنة لحماية حقوق الأفراد في الفضاء الرقمي، وتأمين بياناتهم الشخصية والوعي بعدم مشاركة المعلومات الشخصية.

**د - إطلاق الاستراتيجية الخمسية الوطنية للأمن السيبراني (٢٠٢٣م - ٢٠٢٧م) :**

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

**(٣) إنشاء المراكز الوطنية والمجالس المتخصصة :**

**أ - المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات :**  
أنشئ المركز في عام ٢٠٠٩م من أجل مواجهة خطر الإرهاب السيبراني وغيره من التهديدات السيبرانية، ويختص بتقديم الدعم للقطاعين الحكومي والمالي من خلال الدعم التقني والميداني، وتقديم التقارير الفنية للجهات المختصة لحماية البنية التحتية القومية للمعلومات والقطاع المالي، وهناك فريق عمل متخصص على أعلى مستوى يقومون على مدار الساعة بمراقبة الأمن السيبراني والاستجابة للحوادث، وتحليل معامل الطب الشرعي الرقمي، وتحليل البرمجيات الخبيثة والهندسة العكسية، ويتمثل هدفه الرئيس في تعزيز أمن البنية التحتية المصرية للاتصالات والمعلومات من خلال اتخاذ إجراءات استباقية وجمع وتحليل المعلومات الخاصة بالحوادث الأمنية والتنسيق والوساطة بين الأطراف المعنية في حل تلك الحوادث الأمنية والتعاون الدولي مع مختلف الفرق المعنية بالاستجابة لطوارئ الحاسبات والشبكات في الدول الأخرى (٤٤).

**ب - المركز المصري للاستجابة لطوارئ الحاسب الآلي (سيرت) :**

لقد قام الجهاز القومي لتنظيم الاتصالات بتأسيس المركز المصري لاستجابات طوارئ الحاسب الآلي (سيرت) في إبريل ٢٠٠٩م حيث يعمل به فريق من ستة عشر متخصصاً، ويقدم الفريق الدعم الفني على مدار ٢٤ ساعة لحماية البنى التحتية الحيوية للمعلومات. ويقدم المركز منذ عام ٢٠١٢م الدعم لمختلف الجهات عبر قطاعات تكنولوجيا



## الانعكاسات والمخاطر الاجتماعية للجرائم والهجمات السيبرانية على الأمن الرقمي وآليات المواجهة في ضوء رؤية مصر ٢٠٣٠

أ.م.د/ أسماء جابر مهران

- ٢- نموذج مقترح لتطوير وتعزيز أنظمة الأمن الرقمي والسلامة المعلوماتية لمجابهة الجرائم والهجمات السيبرانية:
- أ- مداخل مواجهة الجرائم والهجمات السيبرانية وتشمل:
- الحوكمة - تنمية وعى أفراد المجتمع - إنفاذ القانون
- التعاون الدولي - 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 السيبراني - الحرب السيبرانية - التجسس السيبراني - التخريب السيبراني - الذكاء الاصطناعي - إنترنت الأشياء - الهندسة الاجتماعية - البلوكشين - المرونة السيبرانية - الحوسبة الكمومية - الاختراق الحيوي - 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 التي ترتفع فيها معدلات الجرائم الإلكترونية.
- الدول التي تعاني الهجمات السيبرانية.
- الدول التي تعاني الإرهاب السيبراني.
- الدول التي تعاني جرائم الهندسة الاجتماعية.
- و- المخرجات المستهدفة وتتمثل في:
- إرساء أفضل الممارسات في مجال الأمن الرقمي والمعلوماتي والسيبراني 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 التعافي من الحوادث السيبرانية.

- بالإضافة إلى تعزيز التعاون بين أجهزة إنفاذ القانون وأجهزة القضاء على المستويين الوطني والدولي، وأن تعمل القوانين على حماية الأطفال والشباب في الفضاء الرقمي.
- المعيار الثاني: التوعية المجتمعية:
- حيث يتطلب مواجهة الجرائم والتهديدات السيبرانية كفاية برامج ومداخل توعية المواطنين من مختلف الفئات والأطياف ووجوب إشراك المجتمع المدني في ديناميكيته.
- 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 في مجال الأمن السيبراني والمعاملات الإلكترونية والتحول الرقمي.
- المعيار الخامس: بيئة حيوية للأمن السيبراني:
- تعتمد على تشجيع البحث العلمي والابتكار في مجال الأمن السيبراني وحماية الشبكات وأنظمة المعلومات، وتعزيز المهارات وتأهيل الكفاءات الوطنية في مجال السلامة المعلوماتية والجرائم الإلكترونية.
- المعيار السادس: استحداث طرائق لتأمين النظام الأمني الرقمي:
- والذي يجب أن يتركز على ثلاثة أركان أساسية:
- الوقاية من الهجمات والتهديدات السيبرانية:
- باستخدام جدار الحماية وبرنامج الأمان لمكافحة الفيروسات والديدان والبرامج الضارة.
- الكشف والتعافي: سرعة اكتشاف التهديدات والثغرات وتحديث الأنظمة.
- سرعة رد الفعل: إذا تم اكتشاف الهجمات ولم يتم التصدي لها يصبح الاكتشاف ليست له قيمة وأهمية فلا بد من توافر جاهزية قدرات التصدي 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 في مجال الأمن السيبراني التي تركز على تطوير البنية التحتية المرقمنة بما يساهم في تحقيق رؤية مصر ٢٠٣٠.



## ثامناً : نتائج الدراسة ومقترحاتها :

### ١- النتائج :

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

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

٢- يُعد الأمن الرقمي ضرورة مُلحة فرضها التطور التكنولوجي ومنظومة التحول الرقمي لضمان سلامة وأمن المعلومات وتكنولوجيا الاتصالات.

٣- هناك صعوبة في حصر أنماط الجرائم الإلكترونية والهجمات السيبرانية، نتيجة اعتماد مُركبها من المجرمين على التقنيات والوسائل المرتبطة بالتقدم التكنولوجي الذي تزداد وتيرة تغيره يوماً بعد يوم.

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

٥- أوضحت النتائج أن الجرائم الإلكترونية والهجمات السيبرانية تؤثر تأثيراً بالغ الخطورة على البناء الاجتماعي للدول فهي جرائم عابرة للقارات؛ وتستهدف البنية التحتية والأنشطة الاجتماعية التي تتعلق بالأفراد والمجتمع ككل.

٦- تشكل الجرائم الإلكترونية والسيبرانية تهديداً خطيراً ومتزايداً، وأن تكاليف مجابهة الأثار الناجمة عنها واكتشافها تُعد كثيرة جداً بالنسبة للدول لأنها تعتمد كلياً على التكنولوجيا والتقنيات الحديثة والمتطورة.

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

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

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

### ٢- المقترحات :

في ضوء ما كشفت عنه النتائج تقترح الدراسة مايلي :

١- أن مواجهة الجرائم والتهديدات السيبرانية تتطلب توفير مزيد من المعرفة والوعي لدى مستخدمي الإنترنت والشبكات الاجتماعية لتفادي الحوادث والأضرار السيبرانية المباشرة وغير المباشرة التي من الممكن أن يتعرضوا أو يكونوا ضحايا لها، وتوفيراً للتكاليف التي تتكبدها الدولة في مواجهتها.

٢- وجوب تفعيل استراتيجيات وقوانين وسياسات الأمن الرقمي؛ لأنها من سُبُل تحقيق الأمن القومي لمصر، ونشر ثقافة الأمن الرقمي بين مختلف فئات المجتمع وتضمينها في مختلف الخطط والاستراتيجيات على جميع المستويات الإقليمية والدولية، حتى تتحقق السلامة السيبرانية والأمن المعلوماتي بما يتماشى مع التغيرات المتسارعة.

٣- يجب على الجامعات والمعاهد والمنظمات المختلفة الاهتمام بتطوير منهج الأمن السيبراني وتدريبه، بحيث يصبح مطلباً جامعياً، حتى تتوافر الخبرة العلمية والتقنية اللازمة في التصدي للهجمات والتهديدات الإلكترونية المتطورة والمتغيرة .

٤- يجب على صانعي السياسات والأكاديميين والمتخصصين التفكير في أفضل السبل لتطبيق مفهوم إدارة المخاطر المرتبطة بحماية الخصوصية والبيانات والمعلومات من التهديدات المحتملة.

٥- يُعد بناء الثقة أمراً ضرورياً في البيئة الرقمية وفي تطوير استراتيجيات حماية الخصوصية والتصدي



## الانعكاسات والمخاطر الاجتماعية للجرائم والهجمات السيبرانية على الأمن الرقمي وآليات المواجهة في ضوء رؤية مصر ٢٠٣٠

أ.م.د/ أسماء جابر مهران

زيادة الوعي لدى القائمين على إدارة التكنولوجيا الرقمية بمخاطر الخصوصية.

١٠- تعزيز الوعي بمفهوم المواطنة الرقمية لدى جيل الشباب الذين تتراوح أعمارهم بين ١٨ و ٤٠ عامًا بكيفية التعامل مع البيئة الرقمية ووسائل التكنولوجيا المختلفة لتحقيق الفوائد الشخصية والمجتمعية بطرق إيجابية.

١١- نشر الوعي حول الاستخدام الآمن للبطاقات الإلكترونية لتعزيز التصدي للاستخدامات غير المشروعة في المعاملات الإلكترونية.

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

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

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

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

٦- يجب على صنّاع القرار التعامل مع مخاطر الأمن الرقمي باعتباره خطرًا يهدد الأمن السياسي، والاقتصادي، والاجتماعي والتكنولوجي.

٧- يجب على الاستراتيجيات الوطنية التي تهدف إلى تحقيق الأمن الرقمي أن تعكس رؤية المجتمع وتعزز حماية الخصوصية في الفضاء الرقمي الذي يعتمد على البيانات كركيزة أساسية.

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

٩- يجب على المؤسسات والشركات الصغيرة والناشئة

### المواش :

- (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 في الملتقى العلمي- الجرائم المستحدثة في ظل التغيرات والتحولات الإقليمية والدولية ٢-٤/٩/٢٠١٤م عمان - الأردن.
- (٦) فوزي حسين الزبيدي : منهجية تقييم مخاطر الأمن القومي : دراسة تحليلية لمنهجية تقييم مخاطر الأمن القومي NSRA، رؤى استراتيجية، مركز الإمارات للدراسات والبحوث الاستراتيجية، المجلد (٢) العدد (١١)، ٢٠١٥م، ص ١١.
- (٧) أولريش بك، مجتمع المخاطر العالمي بحثًا عن الأمن المفقود، ترجمة علا عادل وآخرون، القاهرة، المركز القومي للترجمة، ٢٠١٣م، ص ٢١٤.
- (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 القومي المصري، دراسة سوسيو تحليلية، جامعة الفيوم، مجلة كلية الآداب، الإنسانيات والعلوم الاجتماعية، المجلد (١٥)، العدد (١) يناير ٢٠٢٢م، ص ٢١٠٤.
- (١٠) إسلام فوزي : الأمن السيبراني، الأبعاد الاجتماعية والقانونية، تحليل سوسولوجي، القاهرة، المجلة الاجتماعية القومية، المجلد السادس والخمسون، العدد الثاني، مايو ٢٠١٩م.
- (١١) مكتب الأمم المتحدة المعنى بالمخدرات والجريمة : دراسة شاملة عن الجريمة السيبرانية، فيينا، ٢٠١٢م، 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) سامي محمد بونيف : دور الاستراتيجيات الاستباقية في مواجهة الهجمات السيبرانية، الردع السيبراني 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 كايبيخاس، عائشة عفيضى، نيكولاي لوزنيسكى : الأمن السيبرانى فى مؤسسات منظومة الأمم المتحدة تقرير وحدة التفتيش المشتركة، الأمم المتحدة ، ٢٠٢١م، ص٧.
- (١٧) أمينة 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
- (٢٢) الاستراتيجية الوطنية للأمن السيبرانى (٢٠٢٣م-٢٠٢٧م)، وزارة الاتصالات وتكنولوجيا المعلومات.
- (٢٤) خورجى فلوريس كايبيخاس، عائشة عفيضى، نيكولاي 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
- (٢٣) إسلام فوزى : مرجع سابق، ص ١١٢ - ١١٣ .
- (34) James A. Lewis: Op Cit.
- (٢٥) الاستراتيجية الوطنية للأمن السيبرانى (٢٠١٧م - ٢٠٢١م).
- (36) [https://mcit.gov.eg/Ar/Media\\_Center/Press\\_Room/Press\\_Releases/67460](https://mcit.gov.eg/Ar/Media_Center/Press_Room/Press_Releases/67460) تاريخ الدخول ٢٤/٤/٢٠٢٤م الساعة ١١,٥٠ مساء
- (٢٧) الدستور المصرى ٢٠١٤م.
- (٢٨) القانون رقم ١٧٥ لسنة ٢٠١٨م قانون مكافحة جرائم تقنية المعلومات.
- (٢٩) 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 ، ٢٠١٤م ، 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  
الرقمي وآليات المواجهة في ضوء رؤية مصر ٢٠٣٠

أ.م.د/ أسماء جابر مهران

## الانعكاسات والمخاطر الاجتماعية للجرائم والهجمات السيبرانية على الأمن الرقمي وآليات المواجهة في 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 سوسيولوجي للمخاطر الاجتماعية للجرائم والهجمات السيبرانية على الأمن الرقمي ورصد آليات وجهود الدولة المصرية في ضوء رؤية مصر ٢٠٣٠ .  
لقد أظهرت النتائج أن الأمن الرقمي يعد ضرورة ملحة فرضها التطور التكنولوجي ومنظومة التحول الرقمي لضمان سلامة وأمن المعلومات وتكنولوجيا الاتصالات .  
بيّنت النتائج أن معظم دول العالم تعرّضت للعديد من الجرائم والهجمات السيبرانية التي استهدفت القطاعات الحيوية في المجتمع، ومن ثم قامت بإصدار القوانين المختلفة من أجل التغلب على التهديدات والأخطار الناجمة عنها . أوضحت النتائج أن مصر من أوائل الدول التي قامت بسن التشريعات والقوانين وإنشاء المراكز والمجالس المتخصصة، ووضع الكثير من الاستراتيجيات التي تتضمن العديد من البرامج الاستراتيجية المختلفة، وعقد المؤتمرات من أجل حماية الدولة من مخاطر الجرائم والهجمات السيبرانية، ولتحقيق بيئة رقمية آمنة وموثوقة للمجتمع المصري بمختلف أطيافه.

**الكلمات المفتاحية :** الجرائم السيبرانية - الهجمات السيبرانية - الأمن الرقمي - 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

