مُتطلبات تحقيق الأمن السيبراني في ضوء رؤية مِصر ٢٠٣٠
"رؤية استشرافية".

ولاء أسعد عبد الجواد*

المُلخص:

تهدف الدراسة الحالية إلى وضع رؤى استشرافية حول مُتطلبات تحقيق الأمن السيبراني، في ضوء رؤية مِصر ٢٠٣٠؛ وذلك من خلال تطوير آليات تحقيق الأمن السيبراني، بشكل ينعكس على مُمارسات الدولة من أجل تحقيق التنمية الشاملة وفق رؤيتها للتنمية المُستدامة. استعانت الباحثة في هذه الدراسة بنظريتي: مُجتمع المخاطر لـ "أويرليش بيك"، والتشكيل البنائي لـ "أنتوني جيدنز"؛ وذلك لرصد ركائز ومُمارسات الأمن السيبراني وتحليله. واعتمدت الباحثة على بناء السيناريوهات المُستقبلية لصياغة مسارات مُحتملة؛ لتطوير مُتطلبات تحقيق الأمن السيبراني، اعتمادًا على مُعطيات الوضع الراهن، كما اعتمدت على المنهج الوصفي التحليلي لفهم مُتغيري الأمن السيبراني، والجريمة الإلكترونية من واقع التُراث البحثي، وصولًا إلى تحليل واقع الأمن السيبراني في مصر في ضوء "رؤية مِصر ٢٠٣٠"، كما قدمت الدراسة قراءة لأهم التحديات والاستراتيجيات الأمنية والتقنية لمواجهة الجريمة الإلكترونية. وتوصلت الدراسة لوضع ثلاثة سيناريوهات مُستقبلية، تؤكد على وجود مجموعة من المُتطلبات: السيناريو الأول مُحتمل، والثاني مُتوقع، والثالث مرغوب فيه لتحقيق الأمن السيبراني في المُجتمع المِصري، خاصة في ظل انتشار تقنيات الذكاء الاصطناعي Artificial Intelligence (AI).

الكلمات المُفتاحية: الأمن السيبراني، الذكاء الاصطناعي، رؤي استشرافية.

*- مُدرس بقسم علم الاجتماع- كلية البنات- جامعة عين شمس.

أولًا- مدخل لإشكالية الدراسة، وتساؤلاتها:

شهد المُجتمع الإنساني في العقدين الأخيرين من القرن العشرين موجات مُتلاحقة من التحول الرقمي Digital Transformation، لم يسبق لها مثيل في نطاق وعُمق تأثيرها على العالم بِرمته، ومن المُتوقع أن تنمو سُرعة التحول الرقمي في العقود القادمة مدفوعة بالفُرص التي توفرها المنصات الرقمية، بتقنياتها المُختلفة، ويُشير التحول الرقمي بشكل مُبسط ومُباشر إلى عمليات إدخال التكنولوجيا الرقمية، لتطوير النشاط الإنساني. وعلى الرغم من أن الأمن السيبراني عُنصر أساسي لضمان نجاح التحول الرقمي؛ غير أنه واجه العديد من التحديات الأمنية المُعاصرة في فهمه ومُسايرته في الدول كافة، مما جعل له بُعدًا مفاهيميًا تجدُر دراسته من طرف الأوساط الأكاديمية والمَعرفية، وإيجاد نسق مَعرفي يُسهل على صانع القرار إيجاد الحلول للمُشكلات كافة على المستوى الإمبيريقي التحليلي (سمير قلاع الضروس، ٢٠٢٢م: ٢٥٢). وخاصة أن نشأة الأمن السيبراني ارتبطت بظهور الهجمات والاختراقات التي حدثت في مُنتصف خمسينيات القرن العشرين. وازدادت أهميته مع ظهور شبكة الإنترنت التي فتحت الباب لظهور مجالات جديدة، يتم من خلالها حفظ المعلومات إلكترونيًا ونقلها. وهذا ما تطلب مواكبة سريعة لسُرعة تطور تكنولوجيا الأنظمة، والشبكات، والبرمجيات الحديثة من خلال حزم الآليات التي تكفُل الحِماية بمفهومها الجديد، وتحد من المخاطر الإلكترونية عن طريق: جدار الحِماية، وأنظمة كشف التسلُل، وتطبيقات مُكافحة الفيروسات، وتقنيات التشفير وإدارة المعلومات... وغيرها من تقنيات الحِماية، مما يؤدي إلى حِماية وسرية البيانات (وليد عبد الرحمن جاب الله، ٢٠٢١م: ٤٩).

وبناءً عليه، حظيت التكنولوجيا الرقمية في الآونة الأخيرة بدراسات مُستفيضة في تخصُصات مُختلفة مثل: تكنولوجيا الاتصالات والمعلومات، والقانون، وعلم المعلومات، والإعلام، وعلم النفس والاجتماع... وغيرها من العلوم؛ ويرجع ذلك لكون التكنولوجيا الرقمية مجالًا مُتداخلاً يُلقي الضوء على عدد من الاختصاصات التي تخُص الأمن السيبراني الذي يُمكن النظر إليه، والسعي لمُعالجته من عِدة زوايا، وخلفيات مَعرفية مُتعددة، ومن هُنا تعددت النظريات المُفسرة لتلك القضية، ومن بين هذه النظريات والمفاهيم المُفسرة للأمن السيبراني نجد نظريات: كالأمن مُتعدد الطبقات، والهندسة الاجتماعية، ومُجتمع المخاطر، والشفافية الأمنية، والتشكيل البنائي، والشبكات المُعقدة، والفجوة الزمنية والفجوة الرقمية...وغيرها من النظريات التي تهتم بفهم وتفسير التحديات الأمنية، وكيفية مواجهتها.

كما كشفت الدراسات التي أُجريت في مجال تكنولوجيا المعلومات أن الجرائم السيبرانية Cyber–Crime التي تقوم بها بعض المواقع كَلفت دول العالم العديد من الخسائر، وكان من المُتوقع أن تصل الخسائر إلى ما يُقارب من ٦ تريليونات دولارًا سنويًا في العام ٢٠٢١م، وهو ضعف المبلغ الذي تم خسارته عام ٢٠١٥م. فكُل هذه الخسائر ناتجة عن الأضرار التي خلفتها الجرائم السيبرانية، والتي تتمثل في: سَرقة البيانات أو تخريبها، وسَرِقة الأموال، وفقد الإنتاجية، وسَرقة الملكية الفكرية، والاِختلاس، والاِحتيال التُجاري، واختراق الأنظمة، والإضرار بالسُمعة (عبد الله بن شرف الغامدي، ٢٠١٨م: ٦)، وأشار تقرير "مؤسسة دبي للمُستقبل" إلى ارتفاع تكلفة مُكافحة الجرائم السيبرانية، والتي بلغت ٣ تريليون دولارًا عام ٢٠٢٠م، كما أشار التقرير أيضًا إلى عدد من الجرائم الإلكترونية، وازدادت الجرائم بصورة ملحوظة فترة تفشي وباء كورونا عالميًا (صلاح الدين محمد توفيق، وشيرين عيد مرسي، ٢٠٢٢م: ٧٤٢).

ولتحقيق الأمن السيبراني، لابد من العمل على بناء جُدران الحِماية من الهجمات الإلكترونية، وتقليل تأثير رقابة واختراق الحسابات، وأنظمة المَعلومات، سواء الحُكومية منها أو الخاصة. فلا يُمكن حِماية البيانات والمعلومات دون جُدران الحِماية (محمد زين العابدين، ٢٠٢٣م: ٥٨)؛ لذلك بدأت الحُكومات بتطوير استراتيجيات "الأمن السيبراني"، وأعدت الفضاء الإلكتروني قضية دولية لها أهميتها. ولهذا؛ أشارت الأجندة الوطنية للتنمية المُستدامة "رؤية مِصر ٢٠٣٠م" في النسخة الصادرة عام ٢٠٢٣م إلى عدد من المُمكنات الضرورية، والأدوات المُقترحة لتنفيذ سياسات الدولة، ومنها: التحول الرقمي الذي "يُعد أحد المُمكنات الأساسية التي تُساعد على تحقيق جميع أهدف رؤية مِصر ٢٠٣٠: الاقتصادية والاجتماعية والمؤسسية والبيئية، ويعمل على إنشاء بنية تحتية مرنة للحكومة والمؤسسات تسمح بمواكبة مُستجدات الثورة التكنولوجية. كما يُتيح القدرة على الابتكار والتكيف باستمرار مع المُتغيرات المُتسارعة عالميًا، ومُتطلبات المُستهلكين. وأخيرًا، يُسهم التحول الرقمي في تخفيض تكلفة المُعاملات وتحسين حوكمة المؤسسات، إذ يُجري فصل مُتلقي الخدمة عن مُقدمها، مما يكفل كفاءة تقديم الخدمات وفاعليتها، ويُعزز من الشفافية، ومستوى الثقة لدى المواطن" (الأجندة الوطنية للتنمية المُستدامة رؤية مِصر ٢٠٣٠، ٢٠٢٣م: ٢٥). وعلى الرغم من التحديات التي واجهت الأمن السيبراني في القيام بدوره لحِماية البيانات والمعلومات، غير أنه استمر في الاِزدهار مع استمرار الطلب القومي لأدوات جديدة ومُبتكرة في هذا المجال؛ وهذا ناتج عن التطور التكنولوجي المُتسارع الذي أدى إلى ارتفاع الطلب لوجود شركات الأمن السيبراني في الدول كافة.

وفي ظل الحاجة المُلحة، التي زادت مع التهديدات والهجمات السيبرانية، ونتيجة لاستمرار الحِراك المعلوماتي، والتطور التقني والتكنولوجي، والتحول الرقمي الذي أصبح ظاهرة العصر الحديث، مما أدى إلى تضاعُف الاعتماد على المنصات الرقمية ووسائل الاتصال؛ الذي أدى لزيادة مُعدلات الخَطر من الهجمات السيبرانية، ومخاطر الإعتداء على البُنى التحتية؛ وسُرعان ما أدى إلى زيادة مُعدلات انتشار الشائعات والمعلومات المُفبركة، هذا بالإضافة إلى وجود أسلحة رقمية موجهة لضرب الأمن المعلوماتي، مما جعل الدول عُرضةً إلى مخاطر وتهديدات الهجمات السيبرانية؛ أكدت الاستراتيجية الوطنية للأمن السيبراني على تنفيذ تدعيم الأهداف الاستراتيجية للأمن السيبراني من خلال توزيع الأدوار بين الحُكومة والقطاع الخاص، فضلًا عن دور مؤسسات الأعمال والمُجتمع المَدني، مع التأكيد على أهمية الشراكة المُجتمعية بهدف تنفيذ الإجراءات اللازمة لتحقيقه (نهى مجدي محمد السيد، ٢٠٢١م: ٤٩٩).

ونتيجة لزيادة مُتطلبات وكالات الأمن السيبراني في مِصر، احتلت مِصر الجانب الأكبر على مُستوى منطقة الشرق الأوسط وشمال أفريقيا، من حيث عدد الصفقات الموجهة إلى تمويل شركات الأمن السيبراني الناشئة في مِصر خلال عام ٢٠٢٣م. واستحوذت على ٤٠% من عدد صفقات التمويل الموجهة إلى شركات الأمن السيبراني الناشئة في شركات الشرق الأوسط وشمال أفريقيا، وهذا وفقًا لتقرير مُراجعة الاستثمار في الشرق الأوسط الصادر عام ٢٠٢٣م، وإن دل ذلك على شيء، فإنه يدُل على القُدرة التنافسية العالية للقطاع العام، واستعداده للنمو في مِصر، كما بلغت حجم الاستثمارات الموجهة لشركات الأمن السيبراني الناشئة في مِصر عام ٢٠٢٣م نحو ٧٥٠ ألف دولارًا (مركز المعلومات ودعم اتخاذ القرار، ٢٠٢٤م، ١٧). هذا ما جعل مُتطلبات الأمن السيبراني قضية أمن قومي توضع في أولويات الدولة، ويهتم بها الساسة وقادة النُخب الأكاديمية في الدول كافة دون استثناء. ولهذا، وفي ظل انتشار تقنيات الاتصال وتكنولوجيا المعلومات، وازدياد مخاطر الهجمات السيبرانية يتبلور دور الدولة المِصرية باستراتيجية لتحقيق مُتطلبات الأمن السيبراني، وفقًا لرؤيتها للتنمية المُستدامة، **وانطلاقًا من ذلك، تسعى الدراسة الراهنة إلى الوقوف على مُتطلبات تحقيق الأمن السيبراني في ضوء رؤية مصر ٢٠٣٠. حتى يُمكن الحفاظ على المعلومات الإلكترونية كافة في المُستقبل القريب، والحفاظ على سِرية البيانات والمعلومات، وتحصينها من أي تخريب أو اختراق إلكتروني، خاصة في ظل عملية التحول الرقمي التي تُنميها الدولة في كافة المجالات في ظل التطورات التقنية العالمية.** وبناءً على ذلك، تطرح الدراسة التساؤلات التالية:

١- ما مفهوم الأمن السيبراني، وأنواعه؟

٢- ما المخاطر التي قد تنتج عن استخدام التقنيات الحديثة (الذكاء الاصطناعي)؟

٣- ما أهم التحديات الاستراتيجية والتقنية التي تواجه الأمن السيبراني؟

٤- ما دور الدولة في حِماية المواطنين من الهجمات السيبرانية في عصر المعلومات، انطلاقًا من رؤية مِصر ٢٠٣٠؟

٥- ما الرؤى المُستقبلية لتطوير سياسات بناء الإنسان، ودوره في تحقيق مُتطلبات الأمن السيبراني في ضوء رؤية مِصر ٢٠٣٠؟

٦- ما السيناريوهات المُستقبلية، المُحتملة والمتوقعة والمرغوب فيها، لتطوير الأمن السيبراني في ظل انتشار تقنيات الذكاء الاصطناعي؟

ثانيًا- أهمية الدراسة: تكمُن أهمية الدراسة في:

١- **أهمية الموضوع وحداثته:** يحتل موضوع مُتطلبات تحقيق الأمن السيبراني مكانة مُتميزة في الآونة الأخيرة، ضمن قائمة الموضوعات البحثية في المجالات المُختلفة، وعلى كافة الأصعدة محليًا وإقليميًا وعالميًا؛ نظرًا لأهمية تأمين الأنظمة والمعلومات في المجالات الاجتماعية والاقتصادية والسياسية كافة.

٢- **إثراء التُراث البحثي:** ببناء رؤى مُستقبلية في مجال سوسيولوجيا الذكاء الاصطناعي؛ وذلك من خلال تطوير آليات تحقيق الأمن السيبراني، بشكل ينعكس على مُمارسات الدولة من أجل تحقيق التنمية الشاملة، وفقًا لرؤية مصر ٢٠٣٠.

٣- **تُمثل الدراسة إضافة في مجال حِماية الأنظمة الرقمية والشبكات والمعلومات،** كونها تُسهم في تقديم رؤى للجهات المعنية حول الآثار السلبية الناجمة عن الهجمات السيبرانية، لتفاديها أو إدارة الموقف عند التعامل معها.

ثالثًا- المفاهيم الأساسية، والمفاهيم ذات صلة:

١- **الأمن السيبراني (Cyber security):** على الرغم من تعدُد وتنوع تعريفات الأمن السيبراني التي تعددت بتعدُد التخصُصات المُختلفة، غير أنها تتفق وتتكامل في جوهرها؛ فالأمن السيبراني كلمة لاتينيه مُقسمة لمقطعين: المقطع الأول Cyber، ويعني الفضاء المعلوماتي*، والمقطع الثاني

* - ويُعد الروائي الأمريكي ويليام جيبسون William Gibson أول من استخدم كلمة Cyber في رواية "نيورومانسر" التي كتبها عام ١٩٨٤م، وهي قصة جامعة استشرافية تتناول القتل، وأعمال الفوضى في عالم الفضاء السيبراني الإفتراضي (علي آل مداوي، ٢٠٢٣م: ١١٦).

security، ويُقصد بِهِ الأمن (علي آل مداوي، ٢٠٢٣م: ١١٦)، ولهذا يعني الأمن السيبراني، بأنه: أمن الفضاء المعلوماتي، كما عرفه "إدوارد أموروسو Edward Amoroso" صاحب كتاب "الأمن السيبراني" الصادر عام ٢٠٠٧م، بأنه: "مجموع الوسائل التي من شأنها الحدّ من خطر الهجوم على البرمجيات، أو أجهزة الحاسوب أو الشبكات"، وتشمل تلك الوسائل الأدوات المُستخدمة في مواجهة القرصنة، وكشف الفيروسات الرقمية ووقفها، هذا بالإضافة إلى توفير الاتصالات المُشفرة (هبة جمال الدين، ٢٠٢٣م: ١٩٠). كما عرفه كُلَ من ليتو مارتي Lehto Martti ونيتاناماكي بيكا Pekka Neittaanmaka في كتابهِما الموسوم بـ Cyber Security: Analytics, Technology and Automation الصادر عام ٢٠١٥م، بأنه: مجموعة من الإجراءات التي تم اتخذها في الدفاع ضد هجمات قراصنة الكمبيوتر وعواقبها، ويتضمن هذا تنفيذ التدابير المُضادة المطلوبة (Martti Lehto, Pekka Neittaanmäki, (2015): p8).

كما عرفته وكالة الأمن السيبراني التابعة للاتحاد الأوروبي، بأنه: "جميع الأنشطة اللازمة لحِماية الفضاء السيبراني ومُستخدميه، والأشخاص المُتضررين من التهديدات السيبرانية" (Brookso Charles, Cadzow Scott et al, 2015: p7). ومن جانب آخر عرَّفه أحد الباحثين بأنه: مجموعة من الوسائل التقنية والإدارية التي يتم استخدامها لمنع الاستعمال المُصرح بِهِ، وسوء الاستغلال، واستعادة المعلومات الإلكترونية، وتأمين حِماية وسرية البيانات الشخصية لحِماية المواطنيين (محمد خليفة، ٢٠٠٨م: ٤٥). ويُعرِّفها البعض الآخر، بأنه: عملية حِماية الأنظمة والشبكات والبرامج ضد الهجمات الرقمية؛ كما تهدف هذه الهجمات إلى الوصول للمعلومات الحساسة، وتعمل على تغييرها وتدميرها؛ بهدف الاستيلاء على الأموال من المُستخدمين أو مقاطعة عمليات الأعمال العادية (عبد العزيز قاسم محارب، ٢٠٢٣م: ٥). ومن الناحية القانونية عرَّفته "هدى عدلي" بأنه: مجموعة من الإجراءات التقنية والإدارية، تشمل العمليات والآليات التي يتم اتخاذها لمنع أي تدخل غير مقصود، أو غير مُصرح به بالتجسُس، أو سوء الاستغلال للمعلومات والبيانات الإلكترونية الموجودة على نُظم الاتصالات والمعلومات، هذا بالإضافة إلى تأمين وحِماية وسرية وخصوصية البيانات الشخصية للمواطنين (هدى عدلي، ٢٠٢٣م: ١٨٥).

وانطلاقًا من التعريفات التي قُدمت للأمن السيبراني، وجد أن له ثلاثة أبعاد، وهي (عبد الرحمن عاطف أبو زيد، ٢٠١٩م: ٥٥): ١- **البُعد الاقتصادي:** حيث ينقسم البُعد الاقتصادي إلى مجالين،

الأول: يتعلق بصناعة تكنولوجيا المعلومات والاتصالات، بما يحتويه من تطوير الأجهزة وبرمجياتها وإنتاجها، وخدمات أخرى. **والثاني:** هو مجال التجارة الإلكترونية من خلال فتح سوق حُر على شبكة الإنترنت. ٢- **البُعد الثاني: يتعلق بأمن المعلومات؛** لذلك نجد العديد من الدول تُخصص جُزءا كبيرًا من ميزانيتها؛ لأجل الحِماية من الهجمات السيبرانية، وتطوير أنظمة الأمان لديها. ٣- **البُعد الثالث: وهو البُعد الأمني،** خير دليل على ذلك، مركز تكامُل استخبارات التهديد السيبراني بالولايات المُتحدة الأمريكية، ذلك المركز الذي يعمل على التنسيق بين مُختلف أجهزة الأمن الأمريكية الأخرى مثل: مكتب التحقيقات الفيدرالي، وكالة الاستخبارات المركزية، ووكالة الأمن القومي. ويرتكز الردع السيبراني على ثلاث ركائز، وهي: مِصداقية الدفاع Credible Defence، القُدرة على الانتقام An Ability to Retaliate، والرغبة في الانتقام A will to Retaliate (سمير قلاع الضروس، ٢٠٢٢م: ٢٥٣).

ويُمكن تعريف الأمن السيبراني إجرائيًا، بأنه: تأمين الجهات المعنية بالدولة المِصرية المعلومات والبيانات كافة، سواء للأفراد أو المؤسسات، وحِمايتها من الاختراق والقرصنة، أو ما يُسمى "بالهجمات السيبرانية"؛ وذلك من خلال توفير بيئة آمنة، يُمكنها التعامل مع المعلومات كافة، والقُدرة على مُقاومة البرامج الخبيثة.

- **المفاهيم ذات صلة:**

١- **الفضاء السيبراني Cyber Space:** أدى تعدُد وتنوع مفهوم الفضاء السيبراني إلى ظهور عِدة مُحاولات لتعريفه، حيث يُعرف بأنه: "مجال عالمي يتكون من شبكة مُترابطة من البُنى التحتية لتكنولوجيا المعلومات، بما في ذلك الإنترنت، وشبكات الاتصال، اللاسيكية وغير اللاسلكية، وأنظمة الحاسوب، وآليات التحكُم المُتكاملة، ويشمل المعلومات الرقمية المنقولة، وكذلك أنظمة توفير الخدمات عبر الإنترنت (Bertrand Boyer, 2012: 50). وهُناك من عرَّف الفضاء السيبراني بأنه: جزء من شبكة الإتصالات، وهو عبارة عن شبكة تتألف من مِئات الحَاسبات الآلية المُرتبطة ببعضها البعض، وتكون إما لاسلكية أو غير لاسلكية، تمتد عبر العالم لتؤلف شبكة ضخمة، بحيث يُمكن للمُستخدمين الدخول إليها في أي وقت، وفي أي مكان (محمد ناصر، ٢٠٢٢م: ٩٤).

٢- **الجريمة السيبرانية CyberCrime:** تُعرف الجرائم السيبرانية، بأنها مجموعة من الأفعال غير القانونية، تتم من خلال الإنترنت عبر أجهزة الكمبيوتر، والهدف منها تغيير البيانات وتدميرها وسرقة الملكية الفكرية لهذه البيانات. ومن المعروف أن الإرهابيين يستخدمون الإنترنت للتواصل والإبتزاز، والترهيب، وجمع الأموال، وتنسيق العمليات. والتي تقوم بها الدول المُعادية بقدرات مُتطورة للغاية لشن الحروب السيبرانية (V.Karamchand Gandhi, 2012: p1-9).

٣- **الهجوم السيبراني Cyberattac:** ويُعد الذكاء الاصطناعي من أهم الأدوات التي تُعزز الهجمات السيبرانية، حيثُ تتخذ بعضها نمط "حجب الخدمة"، والذي يُعد من أكثر الهجمات السيبرانية شيوعًا على مدار عِدة عقود، والغرض الأساسي من تلك الهجمات، هو جعل نظام الكمبيوتر المُتصل بالإنترنت غير مُتاح مؤقتًا لمُستخدميه، من خلال استنفاد ذاكرته تمامًا عبر طلبات اتصال مُتعددة. وقد أطلق تنظيم "داعش" بين أواخر عام ٢٠١٦م وأوائل عام ٢٠١٧م أول سلسلة من هجمات حجب الخدمة، باستخدام أداة تُسمى "مدفع الخلافة Caliphate Cannon"، والتي استهدف من خلالها البنية التحتية العسكرية والاقتصادية والتعليمية لعدد من الدول (تقى النجار، ٢٠٢٤م: ٩٨).

رابعًا- التُراث البحثي:

حظيت الدراسات التي تناولت التطور التكنولوجي باهتمام كبير في الآونة الأخيرة في الدول العربية، مما مكن الباحثة من تقسيم التُراث البحثي لمحورين: تناول المحور الأول: دراسات ركزت على المخاطر السيبرانية. بينما ركز المحور الثاني على: الأمن السيبراني.

المحور الأول_ دراسات حول المخاطر السيبرانية:

ركزت الباحثة في هذا المحور على رصد المخاطر السيبرانية، كما أوضحتها الدراسات التي تمت في هذا المجال، فجاءت دراسة (جيهان سعد محمد الخضري وآخرين، ٢٠٢٠م) بالتعرُف على طُرق وقاية المُجتمع السُعودي من جرائم الفضاء السيبراني، والوصول إلى مُقترح يُسهم في تفعيل الأمن السيبراني، ولتحقيق تلك الأهداف، استخدمت الدراسة المنهج الوصفي اعتمادًا على استمارة الاستبيان، واتخذت من طُلاب الجامعات السُعودية، وأعضاء هيئة التدريس والإداريين عينة لها. توصلت الدراسة لعدة نتائج أهمها: وجود اتفاق بين أفراد العينة حول تعدُد أسباب حدوث المخاطر، يرجع السبب في ذلك إلى عدم وجود سياسات أمنية واضحة وبرامج حِماية للمجال السيبراني، لذلك أوصت الدراسة بزيادة توعية المؤسسات الجامعية السُعودية حول

إمكانية تطبيق أمن المعلومات، والدعوة إلى تنظيم دورات تدريبية للطُلاب، وأعضاء هيئة التدريس والإداريين لتدريبهم على تطبيق أمن المعلومات. هذا بالإضافة إلى تنظيم دورات تدريبية للقيادات التربوية هدفها تنمية الاعتماد على الذكاء الاصطناعي في صُنع القرار التعليمي. في حين رصدت دراسة (محمد ناصر، ٢٠٢٢م) أشكال انتهاك الفضاء السيبراني في المملكة العربية السُعودية، وتحديد وسائل الإجرام المُستخدمة في انتهاك الفضاء السيبراني، تُقدم الدراسة بيانًا بتصنيف المُجرمين مُنتهكي الفضاء السيبراني، هذا بالإضافة إلى التعرُف على الآثار المُترتبة على جرائم انتهاك الأمن السيبراني. استخدمت الدراسة المنهج الوصفي الاستقرائي التحليلي، باعتباره المنهج الأنسب للدراسات القانونية. وتوصلت الدراسة لعدة نتائج من أبرزها: عدم وجود لائحة تنفيذية للمواد القانونية في النظام السُعودي لتوضيح النصوص، هذا بالإضافة إلى عدم إلمام بعض أفراد المُجتمع السعودي، ونقص وعيهم بالانتهاكات السيبرانية؛ مما جعلهُم عُرضه لارتكابها أو وقوعهُم ضحية لاستغلال المُنتهكين لهُم، وارتكاب الجرائم تجاههُم.

كما اهتمت دراسة (بدر عدنان أحمد سعد، ٢٠٢٣م) بإلقاء الضوء على ماهية الأمن السيبراني، وذلك من حيث: التعريف والأهداف والأهمية، هذا بالإضافة إلى رصد بعض التحديات والتهديدات التي تواجه الأمن السيبراني في الوقت الحالي، وتقديم مجموعة من الإجراءات والتوصيات للتغلب على التحديات والتهديدات أو التخفيف من حدتها. واعتمدت الدراسة على المنهج الوصفي؛ لوصف الظاهرة موضوع الدراسة. وتوصلت الدراسة لعدة نتائج أهمها: رصد بعض التحديات والتهديدات التي تواجه الأمن السيبراني في الوقت الحالي منها: سُرعة حدوث الجرائم والهجمات السيبرانية، وارتفاع خسائر الناجمة عن الجرائم والهجمات السيبرانية مُقارنة بالجرائم التقليدية، عدم وجود اختصاص قضائي خاص بهذه النوعية من الجرائم والهجمات، وغياب أو عدم كفاية أو ضعف التشريعات الدولية والإقليمية والوطنية في موضوع الأمن السيبراني، مما يؤدي إلى صعوبة أو عدم قُدرة الجهات الرقابية والحُكومية والمُنظمات من مُلاحقة المُهاجمين مُجرمي المعلومات والإنترنت. واستطاعت الدراسة أن تُحدد سُبل مواجهة التحديات والتهديدات التي تواجه الأمن السيبراني من خلال مجموعة من التطبيقات، تتم على مستوى الأشخاص مُتمثلة في: عقد دورات تدريبية للمُستخدمين في مجال الأمن السيبراني، على أن تتناول مفهوم الأمن السيبراني، وأهدافه وأهميته وأنواعه، هذا بالإضافة إلى ضرورة عقد ورش عمل حول إجراءات الحماية ضد تحديات وتهديدات ومخاطر الأمن السيبراني، تحت إشراف مُدربين ومُتخصصين في مجال الأمن السيبراني. وتطبيقات تتم على مُستوى

المُجتمع مُتمثلة في: توعية المواطنين بأهمية الأمن السيبراني، وبأساليب الحِماية من التهديدات والمخاطر التي تواجه الأمن السيبراني، وذلك من خلال وسائل الاتصال الجماهيرية، وخاصة التليفزيون والصُحف.

المحور الثاني- دراسات حول الأمن السيبراني:

ركزت دراسات هذا المحور على الأمن السيبراني، ودوره في حِماية البيانات والمعلومات، وكيفية التصدي للتهديدات السيبرانية حتى نتمكن من التعرُف على سُبل تعزيز الوعي الأمني، والامتثال للوائح والمعايير. ومن هذا الدراسات دراسة (سمير قلاع الضروس، ٢٠٢٢م) التي اهتمت برصد الأبعاد الإستراتيجية لمفهوم الأمن السيبراني والجريمة الإلكترونية في دولة الجزائر، وتحديد أهم التحديات والإستراتيجيات الأمنية، والتقنية لمواجهة الجريمة الإلكترونية التي تُحقق الأمن السيبراني الوطني الجزائري. واعتمدت الدراسة على المنهج التحليلي للتعرُف على واقع الأمن السيبراني، وأبعاده الإستراتيجية في الجزائر. كما قدمت الدراسة قراءة لأهم التحديات والإستراتيجيات الأمنية، والتقنية لمواجهة الجريمة الإلكترونية. وتوصلت الدراسة لعدة نتائج أهمها: إلزامية تفعيل جدار الحِماية Fire Well من خلال البصمة الإلكترونية والتوقيع الرقمي، وتقوية أنظمة الباسورد password، وهي تقنية تُفيد في تعزيز الحِماية وعدم الاختراق، وعدم تزوير الرسائل الإلكترونية من خلال: وضع سياسة أمنية عالية الدقة للمؤسسات والأجهزة التي تؤشر لوجود مواقع إرهابية وإجرامية، خاصة في المؤسسات الاقتصادية مثل: البنوك، والبورصة إلى جانب المؤسسات الرسمية، خاصة الوزارات ومؤسسة الرئاسة، وكافة الهيئات الرسمية التي تتعامل مع الأرقام والإحصائيات: كمجلس المُحاسبة، والمجلس الوطني الاقتصادي الاجتماعي، والبيئي والبرلمان بغرفتيه (مجلس النواب والشيوخ). هذا بالإضافة إلى وضع برامج للحِماية من الفيروسات من خلال مراسم تنظيمية تُنظمها الدولة، وتعمل على تدعيمها من خلال تخفيض أسعار هذه البرامج، وهو ما فعلته الجزائر من خلال توفير تطبيق KESPERSKEY، وهو تطبيق مُتوفر في الأجهزة والحواسيب كافة. هذا إلى جانب العمل على خلق جيل رقمي، يواكب تغيرات العصر.

في حين جاءت (دراسة فاطمة علي وآخرون، ٢٠٢٢م) للتعرُف على مفهومي كُلَ من: الأمن السيبراني، والنظافة الرقمية، ذلك المفهوم الذي يُشير إلى وصف نظافة أو عدم نظافة الوسيط الرقمي أو البنية الرقمية، ويُمكن استخدامها لوصف رموز سطح المكتب، وخصائص كُلَ منهُما، هذا بالإضافة إلى التعرُف على الهجمات التي تعترض عملية الأمن السيبراني، وكذلك المُشكلات التي تواجه النظافة الرقمية. واعتمدت الدراسة على المنهج الوصفي التحليلي من خلال الاستعانة بالإنتاج الفكري ذات الصلة بموضوع

الأمن السيبراني والنظافة الرقمية. وتوصلت الدراسة لعدة نتائج أهمها: وجود اختلاف بين مفهوم الأمن السيبراني والنظافة الرقمية من حيث الطبيعة والتطبيق. فالأمن السيبراني في الدراسة، يُعرف بأنه مجموعة من الوسائل والتدابير التكنولوجية التي يتم استخدامها من قبل الأفراد أو المؤسسات أو الهيئات، أو أي كيانات أخرى، هدفها حِماية كُل ما يتعلق بها من بيانات، أو أدوات، أو أنظمة وبرامج...إلخ. أما النظافة الرقمية ذلك المفهوم الذي يُشير إلى وجود نموذجًا جيدًا لتقليص تكلفة الأمن السيبراني فهي تعمل على تعزيز قيمته دون تكاليف باهظة، كما أنها تعمل على تقليل عمليات التسلل للأنظمة والشبكات من خلال اتباع نموذج جيد لمُمارستها. كما أكدت الدراسة أيضًا على أن النظافة الرقمية تُعد جزءًا أساسيًا من الأمن السيبراني، ويُمكن الاستفادة من تطبيقات الذكاء الاصطناعي لتعزيز عملتي الأمن السيبراني والنظافة الرقمية.

بينما تحاول دراسة (عبد العزيز بن أحمد المزيني، ٢٠٢٢م) الكشف عن تأصيل "الأساس الفقهي والنظامي" لوظيفة الدولة الحديثة في تحقيق الأمن السيبراني، والتعرُف على الإستراتيجيات التي ترسمها الدولة، والضوابط والمعايير التي تفرضها لضمان تحقيق ذلك، هذا إلى جانب الدور الذي تقوم به الجهات الرقابية في المملكة العربية السُعودية لتحقيق هذا المطلب. وتوصلت الدراسة لعدة نتائج جاءت على النحو التالي: التأكيد على أهمية الأمن السيبراني، باعتباره أهم جوانب الأمن الوطني في العصر الحالي، يرجع ذلك لاعتماد الدولة عليه بشكل عام، في كُل قطاعات الدولة، لذا يُعد تحقيق الأمن السيبراني أهم واجبات الدولة في العصر الحديث. ونظرًا لأن الأمن السيبراني يُعد من العلوم التي تحتاج قدرًا كبيرًا من العلم والمهنية، لذلك يجب على الدولة توفير عدد من المُتخصصين في هذا الجانب، وتدريبيهم على آخر ما توصلت إليه التقنيات الحديثة في هذا المجال، حتى يتسنى لهم الدفاع عن أمن الوطن. التأكيد على التعاون بين الدول وتوقيع الإتفاقيات في هذا الصدد. هذا إلى جانب عدم الاقتصار على الخلفية القانونية والشرعية للبحث عن الأمن السيبراني، بل لابد من التواصل مع المُختصين التقنين، من خلال الأطر الأكاديمية والبحثية، بإقامة ورش عمل أو مؤتمرات وندوات تتعلق بهذا الموضوع.

في حين جاءت دراسة (إسلام فوزي، ٢٠٢٣م) حول الأبعاد الاجتماعية والقانونية للأمن السيبراني، للبحث عن إيجاد آليات الحِماية لمُمارسات الأمن السيبراني. اعتمدت الدراسة على نظريتي: مُجتمع المخاطر، وتشكيل البنية، وذلك لرصد وتحليل ركائز ومُمارسات الأمن السيبراني. استخدمت الدراسة المنهج التحليلي الوصفي. وتوصلت إلى عدة نتائج من أهمها: التركيز على الأبعاد الاجتماعية للأمن السيبراني وخاصة البنية التحتية، والتي تمثلت في استحداث مركز الطوارئ (CERT)، واستمرار الخدمة فيه على مدار

الـ ٢٤ ساعة، كما أكدت الدراسة على وجود مؤشرات تضمن سلامة واستقرار الأمن القومي مثل: إتاحة خدمة الرصد، والاستجابة للحوادث على مدار ٢٤ ساعة يوميًا طوال الأسبوع. كما أكدت الدراسة تنوع العقوبات للخارجين عن القانون، وتمثلت في: الحبس، أو الغرامة، أو الحبس والغرامة معًا، وقد وردت في باب الجرائم والعقوبات بحد أدنى للحبس مُدة لا تقل عن شهر، وبحد أقصى مُدة لا تزيد عن خمس سنوات، أما الغرامة فوردت بحد أدنى عشرة آلاف جنيه، وبحد أقصى خمسمائة ألف جنيه، ولكن في حالة إتلاف أو تدمير أو إلغاء أو تعديل أو نسخ البيانات أو المعلومات تكون الغرامة بحد أدنى مليون جنيه. ويُمكن تضمين العقوبات مثل: الحبس والغرامة معًا، أو إحداهُما دون الأخرى.

بينما جاءت دراسة (أحمد سالم علي حسن، ٢٠٢٤م): للتعرُف على دور الأمن السيبراني في تعزيز الأمن والدفاع العراقي لمواجهة التهديدات الإلكترونية. هذا بالإضافة إلى التعرُف على وسائل نشر الوعي السيبراني من خلال عرض أهميته ومخاطره. وتوصلت الدراسة إلى: أن تأمين التكنولوجيا وتطور القُدرات السيبرانية يتطلب استثمارات كبيرة، وهو أمر يواجه صعوبة في ظل الضغوط المالية التي يُعاني منها المُجتمع العراقي حاليًا؛ لذا أكدت الدراسة على ضرورة مواكبة التطور الأمني العراقي، والصعود بسلم التطور الأمني العالمي خلال سد الثغرات الأمنية بواسطة الأمن السيبراني. كما توصلت الدراسة إلى غياب الوعي العام بالأمن السيبراني، وكذلك غياب الثقافة السيبرانية، وخاصة تلك المُتعلقة بالجرائم الإلكترونية لذلك يجب إشعار الأفراد بأنهُم يعيشون في أمان، وأنهُم مَحميون من الهجمات الإلكترونية.

وفي ضوء ما سبق، وبعد عرض المخاطر الناتجة عن الهجمات السيبرانية، والدراسات التي تناولت الأمن السيبراني، تُحاول الدراسة الراهنة أن تُثير قضية بحثية مُختلفة، وهي: تقديم رؤية استشرافية حول مُتطلبات تحقيق الأمن السيبراني في ضوء رؤية مِصر ٢٠٣٠؛ وذلك من خلال التركيز على استعداد الدولة المصرية لتحقيق مُتطلبات الأمن السيبراني من خلال تحليل الوضع الراهن، وبناء سيناريوهات مُستقبلية في ذلك المجال. كما تتفق الدراسة الحالية مع بعض دراسات التُراث البحثي في نوع الدراسة، والمنهج المُتبع؛ وهو المنهج الوصفي التحليلي، وهو المنهج المُلائم لتحليل مادة اتصالية جاهزة، مُتمثلة في استراتيجية الأمن السيبراني. بينما اختلفت الدراسة الحالية مع دراسات التُراث البحثي في كونها رؤية استشرافية، وذلك من خلال وضع سيناريوهات من شأنها أن تُحقق مُتطلبات الأمن السيبراني؛ كونه قضية أمن قومي، وأحد أهم الدوافع للحِماية من الهجمات السيبرانية، هذا بالإضافة إلى حِماية البيانات والمعلومات كافة من مخاطر الهجمات والاختراقات للوصول إلى البيانات والمعلومات الخاصة، ذلك مع ضرورة توعية العاملين بالجهات

المُختلفة، لكيفية استخدام برامج تُساعد في الحِماية من الهجمات السيبرانية. لذلك كان علينا أن نقوم بوضع رؤى استشرافية حول تحقيق مُتطلبات الأمن السيبراني في ضوء رؤية مِصر ٢٠٣٠، وخاصة أن مُعظم الدراسات التي تمت من قبل إجريت في المملكة العربية السُعودية والجزائر والعراق والقليل أُجري في مِصر على الرغم من الجهود المبذولة من قِبل الدولة المِصرية لتطبيق تقنيات الأمن السيبراني، والحِماية من الهجمات الإلكترونية. كما استعانت أيضًا بنظريات سبق وقد استخدمتها واحدة من الدراسات، ومن ثم يُمكن مُقارنة ما توصلت إليه هذه الدراسة بالدراسة الحالية.

خامسًا- الإطار النظري للدراسة:

سلط التُراث البحثي الضوء على عدد من الأُطر النظرية المُلائمة لدراسة موضوع الأمن السيبراني كما أوضحت سلفًا، غير أن الدراسة الراهنة سوف تقتصر على مدخلين نظريين فقط، ألا وهُما: نظرية مُجتمع المخاطر لـ "أويرليش بيك"، والتشكيل البنائي لـ "أنتوني جيدنز". ويرجع هذا لعِدة أسباب، ألا وهي: ١- أن المُجتمعات المُعاصرة أصبحت تعتمد بشكل كبير على التكنولوجيا والأنظمة الرقمية؛ مما جعلها عُرضة لمخاطر جديدة وغير مرئية أبرزها الهجمات السيبرانية. ٢- لا يُمكن تفسير العلاقة بين التكنولوجيا الرقمية والأمن السيبراني، دون التعرُف على تأثيرهُما في تشكيل المُجتمعات المُعاصرة.

أ. نظرية **مُجتمع المخاطر لـ "أولريش بيك" Ulrich Beck (١٩٤٤- ٢٠١٥م)**، عالم الاجتماع الألماني، الذي يُعد أول من صاغ مُصطلح مُجتمع المخاطر risk society، في كتابه الأول الذي يحمل العنوان نفسه، والصادر في العام ١٩٨٦م. حيث أشار "أولريش بيك" في هذا الكتاب إلى العولمة أو ما أطلق عليها "الحداثة المُتأخرة" أو الحداثة العالمية ...وغيرها من المُسميات التي تُعبر عن التحول الذي ساد المُجتمع العالمي. عبر "أولريش بيك" عن مُجتمع موجود في كُل مكان من العالم لا يحده زمان مُحدد، تنتشر فيه التكنولوجيا، وتزداد مخاطرها على الفرد والمُجتمع، ويرتبط بهذا العالم الجديد مجموعة من التصورات الجديدة والتخوفات، والمخاوف والآمال، ومعايير السلوك، وصراعات العقائد، وهذه المخاوف لها آثار جانبية قاتلة: فالأشخاص أو الجماعات ممن يصبحون "أشخاص- مُخاطرة" أو "جماعات- مُخاطرة"، لا يعدون أشخاصًا، وحقوقهم مُهددة: فالمُخاطرة تشطر وتستبعد وتُصنف، وهكذا توجد حدود جديدة للإدراك والاتصال بين الأفراد داخل المُجتمع الواحد (أولريش بيك، ٢٠١٣م: ٤٦). كما أكد "أولريش بيك" في نظريته عن الوجود المُتزايد لِانعدام اليقين الذي يُعد أمرًا مُنتشرًا في ظل التغيرات التي تحدُث في المُجتمع، حيث اندثر المُجتمع الصناعي، مفُسحًا المجال لمُجتمع المخاطر

التقني والتكنولوجي أو المعلومات، وهو ما يُطلق عليه منظرو ما بعد الحداثة "عالم الفوضى" العالم الذي تغيب فيه أنماط الحياة المُستقرة (أولريش بيك، ٢٠١٣م: ٢١٤). وتأسيسًا على ما تقدم، نجد أن الأمن الرقمي يشهد عِدة مخاطر؛ نتيجة للثورة الرقمية التي شهدتها دول العالم كافة في الآونة الأخيرة، وما نتج عنها من ارتكاب العديد من الجرائم والهجمات السيبرانية المُستحدثة. حيث أصبحت المخاطر تتسم بالطابع العالمي غير المرئي، وتتمثل في: البرامج الخبيثة والهجمات السيبرانية التي تعمل في الخفاء.

ب. نظرية **التشكيل البنائي** Structuration Theory التي صاغها عالم الاجتماع البريطاني "**أنتوني جيدنز**" **Antony Giddens** (ولد في لندن ١٨ يناير١٩٣٨م) ، أو نظرية "البنينة" بعد أن انتقد النظريات الكُبرى والصُغرى السابقة عليه، واعترض على فكرة أن دراسة المُجتمعات في أصلها تعتمد على البناء في النظريات الكُبرى، وكما اعترض أيضًا على فكرة الاعتماد على الفعل كوحدة أساسية لدراسة المُجتمعات لدى النظريات الصُغرى، واهتم بصياغة نظرية تجمع بين الفعل والمُجتمع أطلق عليها "التشكيل البنائي"، ويقصد بها التفاعل بين ثنائية البناء والفعل معًا. ودائمًا ما يقوم الفرد بعدد من السلوكيات والمُمارسات...وغيرها من التفاعُلات سواء الداخلية أو الخارجية، بما يُسهم في بناء مُجتمع مُتكامل، وبعد اكتمال هذا المُجتمع يُصبح الأفراد هُم الفاعلون الحقيقيون لما يحدث فيه (يحيى خير الله عودة، ٢٠١٢م: ٦). فإذا كُنا نبحث عن الطريقة التي يتشكل بها البناء، فإن مادتنا الخام هي المُمارسات اليومية للأفراد، ومن ثم أفعالهُم. لذلك كان مفهوم "المُمارسة" مفهومًا محوريًا في نظرية البنينة. لذا أعد "جيدنز" نظريته إعادة بناء نظرية حول الذات، لا تحاول أن تُحلل الذات إلى أبنية لغوية جامدة (كما فعلت البنيوية)، ولكنها تنظُر إلى الذات بوصفها كائنًا فاعلًا عاقلًا، تتحدد علاقته بالمُجتمع من خلال مُمارسات مُستمرة، بحيث يتشكل كُل من الفعل والبناء في ضوء هذه المُمارسات؛ لا الفعل سابق على البناء، ولا البناء سابق على الفعل، فكلاهُما مُتضمن الآخر(أحمد زايد، ١٩٩٦م: ٦٩). كما يؤكد "جيدنز" في كتابه (علم الاجتماع) بأن المُجتمعات الإنسانية تُبنى وتُشكل من جديد في كُل لحظة، ويُشبه بذلك المُجتمع بالبناء المِعماري، فالبناء المِعماري يتكون من طوب أو لبنات يُشكلها، ويكونها الفرد بنفسه في مرحلة مُسبقة، ويُعدل عليها بعد ذلك (أنتوني جيدنز، ٢٠٠٥م: ٧٠٣). وهذا يعني أن البناء يُعاد إنتاجه مرة أخرى، وفقًا لتغيُر السياقات الاجتماعية المُحيطة بالفرد، وبما أننا نعيش اليوم في

عصر تكنولوجيا المعلومات يجب علينا مواكبة تلك التغيرات؛ من خلال تفسير بناء المُجتمع، وإعادة إنتاجه كنتيجة للنشاط الإنساني.

وبهذا يؤكد "جيدنز" على أن البنية الاجتماعية هي المسئولة بصورة أساسية عن أفعال الأفراد، كما أن الأفراد أيضًا هُم الفاعلون الحقيقيون لما يحدُث في مُجتمع اليوم. فالبناء الاجتماعي من وجهة نظر "جيدنز" يُعاد إنتاجه مرة أخرى في ظروف أخرى مُغايرة هي التي تُساعد على إعادة إنتاجه بصورة مُختلفة. ووفقًا لرؤية "جيدنز" حول العلاقة بين الفعل والبناء، فإن المخاطر السيبرانية تأتي من أفعال الأفراد الذين تُمثل أفعالهُم إعادة لتشكيل البناء الاجتماعي، وفقًا لهذه الأفعال. ومن ثم وبعد عرض أهم مظاهر التشكل البنائي نجد أن الفاعلين الرئيسين لحدوث المخاطر السيبرانية، هم من يقومون بالتأثير السلبي على البناء الاجتماعي للمُجتمع الذي يعيشون فيه. فإذا استطاع الفرد تأمين المُجتمع من مخاطر الأمن السيبراني، والتقليل من الهجمات الإلكترونية التي تؤثر عليه سلبًا، فهذا يؤكد على حِماية المُجتمع من الهجمات السيبرانية.

سادسًا- الإجراءات المنهجية للدراسة:

١- **نوع الدراسة، ومنهجيتها:** تنتمي هذه الدراسة إلى الدراسات الوصفية التحليلية التي تهدف إلى وصف الظاهرة موضوع الدراسة، وتحليلها، وفي هذه الدراسة، تسعى الباحثة إلى تحليل ظاهرة الأمن السيبراني، وفقًا للمُمارسات التي تقوم بها الدولة داخل مؤسسات المُجتمع؛ وذلك بهدف الحصول على معلومات كافية ودقيقة، تؤكد على أهمية تحيقيق مُتطلبات الأمن السيبراني. ومن ثم اعتمدت الدراسة الراهنة على منهجية **بناء السيناريوهات المُستقبلية***، وذلك من خلال صياغة ثلاثة مسارات: مُحتمل، ومتوقع، ومرغوب فيه. وسوف تعتمد هذه السيناريوهات الثلاثة على معطيات التُراث البحثي حول موضوع الدراسة، واستراتيجية مصر ٢٠٣٠. وقد تم ذلك انطلاقًا من خمس مراحل لوضع تصور مُقترح:

- المرحلة الأولى: تحديد عناصر التصور المُقترح.
- المرحلة الثانية: تحديد الهدف من السيناريوهات (رؤى المُستقبلية).

---

*- يقصد ببناء السيناريوهات صياغة مسارات محتملة لتطور ظاهرة مُعينة، اعتمادًا على مُعطيات الوضع الراهن والمعلومات المُتاحة، وترجيح أحد السيناريوهات باعتباره الأكثر احتمالًا، وتحديد درجة احتمالية السيناريوهات الأخرى، لمزيد من التفاصيل انظر: محمد العربي، (٢٠١٨م): بناء السيناريوهات المستقبلية دليل نقدي، مركز الدراسات الاستراتيجية، القاهرة.

- المرحلة الثالثة: تحديد الأُسس التي يقوم عليها التصور المُقترح.
- المرحلة الرابعة: تحديد دواعي بناء التصور المُقترح للتوجهات المُستقبلية في ضوء رؤية مِصر ٢٠٣٠.
- المرحلة الخامسة والأخيرة: تحديد آليات تنفيذ وبناء التصور المُقترح للتوجهات المُستقبلية.

٢- **مصادر جمع البيانات:** اعتمدت الدراسة الحالية على مصدرين من مصادر جمع البيانات، وهما:

- **المصادر الأولية:** تمثلت في الوثيقة الرسمية لاستراتيجية التنمية المُستدامة رؤية مِصر ٢٠٣٠ والمنشورة على الموقع الرسمي لوزارة التخطيط والتنمية الاقتصادية. والتقارير السنوية لوزارة التخطيط والتنمية الاقتصادية، بالإضافة إلى استراتيجية الأمن السيبراني ٢٠٢٣-٢٠٢٧ المُقررة برئاسة المجلس الأعلى للأمن السيبراني وزارة الاتصالات وتكنولوجيا المعلومات.
- **المصادر الثانوية:** تمثلت في الاستعانة بالتُراث البحثي ذات الصلة بموضوع الدراسة من أجل تحديد مفاهيم الدراسة والمفاهيم ذات صلة بموضوع الدراسة، ووضع التعريف الإجرائي، وتحديد الأساليب المنهجية والنظرية المُلائمة لموضوع الدراسة.

سابعًا- مُناقشة النتائج:

المحور الأول: أنواع الأمن السيبراني من واقع التُراث البحثي، وخصائصه:

أ. أنواع الأمن السيبراني:

نتيجة لتنوع تعريفات الأمن السيبراني، تتعدد أيضًا أنواع الأمن السيبراني بتعدد تعريفاته، تتمثل أنواعه فيما يلي: (علي آل مداوي، ٢٠٢٣م: ١١٩): ١- **أمن البنية التحتية الحيوية:** تعتمد على البنية التحتية الفيزيائية الإلكترونية للشبكة، وتتواجد عادةً في وسائل النقل، والمدارس، والمُستشفيات، والدوائر الحُكومية، وفي شبكات المراكز التُجارية. وهذا النوع يتطلب دراسة إلكترونية لنقاط ضعف المنظومة، والقاعدة الفيزيائية للشبكة، وتطويرها وحمايتها من عمليات الاختراق.

٢- **تطبيقات الأمن:** وهو الاختيار السليم للبرامج التي تحمي الأجهزة والشبكات من عمليات الاختراق الإلكتروني. ولها عدة أنواع مثل: برامج مُكافحة الفيروسات، والجدران النارية، وبرامج التشفير المعلوماتي، وهذه البرامج الثلاثة تضمن حِماية المحتوى من عمليات الاختراق الإلكتروني؛ فكُلما كان مُستخدم الإنترنت أكثر اطلاعًا على برامج الحِماية الحديثة واستخدامها، كان أبعد احتمالية من التعرُض للإبتزاز الإلكتروني.

٣- **أمن الشبكة:** هو الذي يهتم بالاختراقات الخارجية التي تُهدد المنظومة الإلكترونية والمواقع التكنولوجية،

ويرتبط أمن الشبكة بعدة خطوات، وهي: كلمات مرور جديدة، وبرامج الحِماية من الفيروسات، برامج مُكافحة التجسُس، والجُدران النارية. ٤- **سحابة الأمان:** وهي نظام مراقبة وحِماية لكل مصادر المعلومات والبيانات التابعة للمستخدم عبر المواقع والمنصات الإلكترونية. ٥- **إنترنت الأشياء:** تشمل عدة منظومات أساسية مثل: أجهزة التلفاز، وأجهزة الاستشعارات والطابعات، وهذا النوع صُنف كنوع من الأمن السيبراني يحمي البيانات.

ب. خصائص الأمن السيبراني:

للأمن السيبراني مجموعة من الخصائص الأساسية، كما حددتها الهيئة الوطنية للأمن السيبراني التي تعمل معًا لضمان حِماية الأنظمة والمعلومات والحسابات الشخصية من الهجمات الإلكترونية، ولعل أبرزها ما يلي (الهيئة الوطنية للأمن السيبراني، ٢٠١٨م: ١٦):

١- ضمان حِماية الأمن السيبراني للوصول المنطقي (Logical Access) إلى الأصول المعلوماتية والتقنية للجهة، من أجل منع الوصول غير المُصرح بِهِ.

٢- قُدرة الأمن السيبراني على حِماية أنظمة وأجهزة مُعالجة البيانات والمعلومات.

٣- القُدرة على حِماية وإدارة أمن الشبكات.

٤- ضمان وحِماية أجهزة المؤسسة المحمولة كأجهزة الحاسب الآلي والهواتف الذكية من المخاطر السيبرانية، وضمان التعامل بشكل آمن مع المعلومات، سواء الحساسة أو الخاصة بأعمال الجهة، وحمايتها أثناء النقل والتخزين عند استخدام الأجهزة الشخصية للعاملين في المؤسسة.

٥- السرية وسلامة البيانات وحِمايتها من السرقة ودقة توافرها، وفقًا للسياسات والإجراءات التنظيمية للمؤسسة.

المحور الثاني: الجهود المبذولة في مجال الأمن السيبراني في ضوء رؤية مِصر ٢٠٣٠ (تحليل الوضع الراهن):

تؤكد الدراسة الراهنة على الدور الذي تلعبه الدولة المِصرية في تسليط الضوء على أهمية الأمن السيبراني خاصة، فيما يتعلق بالمؤسسات والأجهزة الأمنية، حيث جاءت رؤية مِصر ٢٠٣٠ لدعم مُتطلبات تحقيق الأمن السيبراني، وتعزيز البنية التحتية الرقمية. وبناءً عليه، وضعت الدولة المِصرية هدفًا استراتيجيًا في خطة التنمية المُستدامة تحت مُسمى أولوية قصوى للأمن بمفهومه الشامل، سواء على المُستوى الوطني أو الإقليمي يهتم بتحقيق الأمن الاجتماعي أو السيبراني، كما أكدت أيضًا الاستراتيجية الوطنية للأمن السيبراني

على تنفيذ برامج تدعم الأهداف الاستراتيجية للأمن السيبراني، على نحو ما ذهب إليه "المُشرع المِصري بسن قانون رقم ١٥١ لسنة ٢٠٢٠م بهدف حِماية البيانات الشخصية، عن طريق قيام مركز حِماية البيانات الشخصية بتنظيم مُعالجة وإتاحة البيانات الشخصية" (الاستراتيجية الوطنية للأمن السيبراني ٢٠٢٣-٢٠٢٧: ٨). وبهذا تسعى الاستراتيجية إلى تعزيز ريادة مِصر الدولية من خلال قيادة مِصر للتكتُلات الإقليمية من خلال قيامها بدور نشط وفعال في المحافل الدولية، والعمل على خلق أجيال من المُتخصصين في هذا المجال، ونشر الوعي في كافة مؤسسات الدولة، والتأكيد على أهمية ودور الذكاء الاصطناعي ورفع كفاءة العاملين في مُختلف الوزرات من خلال برامج تدريبية بالتعاون مع شركات عالمية مُتخصصة. هذا بالإضافة إلى التعامل مع المُنظمات الإقليمية والدولية في تبني تقنيات الذكاء الاصطناعي، ومُناقشة قضايا وثيقة الصلة بالأمن السيبراني مثل: الأخلاقيات وحِماية البيانات، وفقًا لما سجله أول اجتماع للمجلس الوطني للذكاء الاصطناعي (معتز نادي، ٢٠٢٤م: ١١٧). واتضح ذلك بصورة جلية وفقًا لتقرير مؤشر قياس استعداد الدول في مجال الأمن السيبراني الصادر عن الاتحاد الدولي للاتصالات (ITU) عام ٢٠١٧م، حيث جاءت مِصر في المرتبة الرابعة عشر من بين ١٩٣ دولة من دول الاتحاد الدولي للاتصالات. وفيما يخُص الدول العربية، تتصدر مِصر المرتبة الثانية بعد سلطنة عُمان التي احتلت المركز الرابع عالميًا والأول عربيًا. وأكد التقرير على أن مِصر لديها استعداد قوي في مجال الأمن السيبراني من خلال هيكلة بنية تحتية تبنتها استراتيجية وطنية، كما عُقدت اتفاقيات عديدة دعت لتبادل الخبرات، ونشر ثقافة الوعي بالأمن السيبراني، كما تم عقد العديد من المُنتديات والمُبادرات والمؤتمرات، ومن خلال تلك المُمارسات استطاعت مِصر التغلُب على أزمة الثقة التي تُهدد انتشار ثقافة الأمن السيبراني، سواء محليًا أو عالميًا من خلال خمسة معايير حددها مؤشر قياس استعداد الدول في مجال الأمن السيبراني (ITU) وهما: الإمكانيات (التقنية، والتنظمية، والقانونية، والتعاون وإمكانية النمو) (إسلام فوزي، 2019 :١٢١).

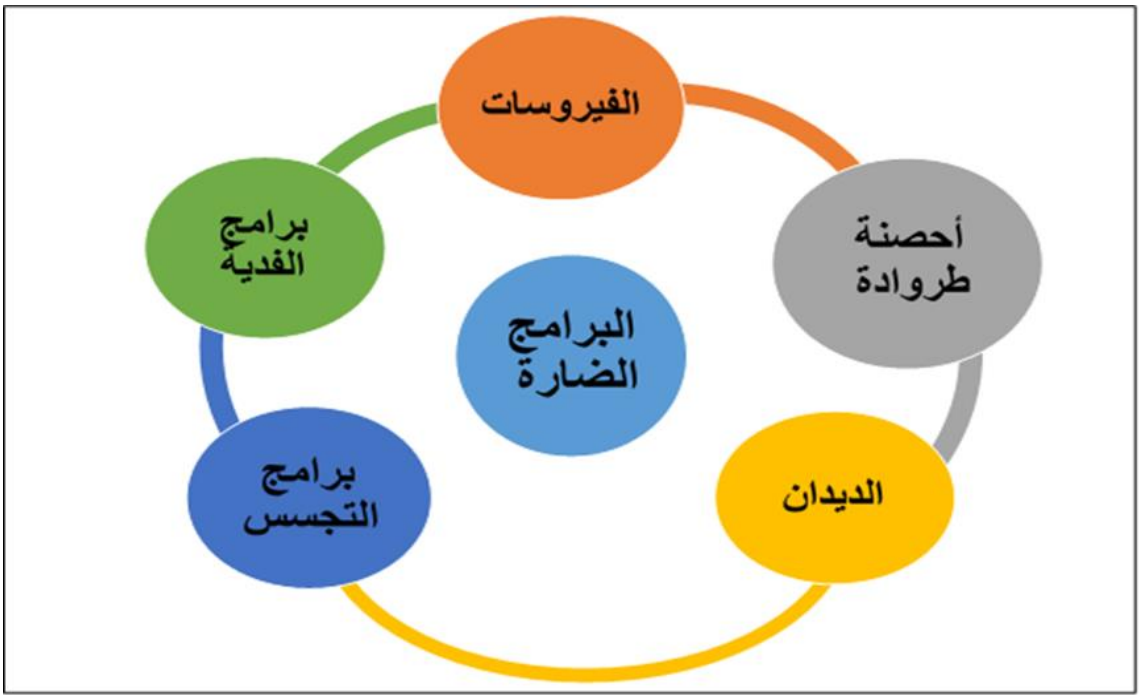
ولهذا أصبح الأمن السيبراني بعد ذلك من الضروريات المُلحة لحماية الأنظمة والمعلومات الإلكترونية، وحِمايتها من الهجمات السيبرانية، هذا ما جعل الأمن السيبراني بمثابة ركيزة أساسية لأي تحول رقمي. كما تميزت مِصر بتوفير اِطار تشريعي ومؤسسي داعم لخدمات الأمن السيبراني، مما يُسهم في تحسين البنية التحتية المعلوماتية، ويتيح المجال لإنشاء المزيد من شركات الأمن السيبراني في المُجتمع المِصري. لذلك اتجهت الدولة إلى توجيه قدر كبير من استثماراتها المُستقبلية إلى مشروعات البنية التحتية التكنولوجية مثل: ضخ الحكومة ٣٠ مليارًا لتطوير شبكات الألياف الضوئية، وهذا ما أسهم في رفع كفاءة

الإنترنت، وتضاعف متوسط سُرعته إلى ١ ضعف سُرعة الإنترنت في مارس ٢٠٢٠م، كما احتلت مِصر المركز الثاني على مستوى دول أفريقيا، وأنشأت شبكة جديدة من كابلات الألياف الضوئية لربط ٣٢٥٠٠ مبنى حُكوميًا، وإنشاء مصنع كابلات للألياف الضوئية بمدينة بدر في مارس ٢٠١٨م وافتتاحه، حيث تبلغ استثمارات المصنع ٣٠ مليون دولارًا، جُزء منها استثمارات أجنبية مُباشرة. ونتيجة لهذه الإجراءات، أعلن الإتحاد الدولي للاتصالات (ITU) عن حصول مِصر خلال عام ٢٠٢٠م على المركز ٢٣ عالميًا من بين ١٨٣ دولة في مؤشر الأمن السيبراني؛ وهذا يرجع إلى أن مِصر بيئة داعمة لشركات الاتصالات وتكنولوجيا المعلومات، مما دعم التوسع في نشاطها، سواء من الجهات الحُكومية وغير الحُكومية، حيث وجدت بمِصر ٣٢ خاضنة أعمال للشركات التكنولوجية الناشئة، و٥٤ جهة تمويل واستثمار في هذا المجال، هذا بالإضافة إلى ٣٦ مُنظمة حُكومية و٢٢ مُنظمة غير حُكومية داعمة، ومُعدة لتيسير أعمال نشاط الشركات الناشئة في مجال تكنولوجيا الأعمال في مِصر (مركز المعلومات، ودعم اتخاذ القرار، ٢٠٢٤م: ٢٢ –٢٤). لذا عندما ننظر إلى رؤية مِصر ٢٠٣٠ في مجال الأمن السيبراني، نجد توسعًا في استخدام التكنولوجيا الرقمية في القطاعي الحُكومي وغير الحُكومي، وفي ظل التسارع التكنولوجي والخدمي والإلكتروني حاولت الدولة المِصرية تطوير الضوابط الأساسية للأمن السيبراني.

المحور الثالث، المخاطر والتحديات التي تُهدد الأمن السيبراني:

شهد الأمن السيبراني في الفترة الأخيرة عِدة تحديات، أثرت عليه تأثيرًا ملحوظًا، وخاصة فترة انتشار وباء كورونا كوفيد١٩، حيث زاد انتشار الهجمات السيبرانية بصورة مُلفتة للنظر، وتُعد هذه التحديات من أبرز أنواع الجرائم الإلكترونية، وهي كالآتي:

١- **البرامج الضارة Malware:** تُعد من أخطر البرامج التي تُهدد الأمن السيبراني، تلك البرامج التي تضرب شبكات الإنترنت، وتستهدف الوصول إلى البرامج والملفات وإلحاق الضرر بها؛ بهدف سرقتها أو حذفها، ويُمكن الوقاية منها من خلال: تثبيت البرامج الخاصة بمكافحة البرامج الضارة، والتعرف عليها، وتحديثها بصورة دورية، والمراقبة الدائمة، إذا كانت هُناك ملفات غير مُعرفة على أجهزة الحاسوب (عبد العزيز قاسم محارب، ٢٠٢٣م: ١٦). يوضح الشكل التالي أكثر البرامج الضارة انتشارًا.



شكل رقم (١) يوضح أكثر البرامج الضارة انتشارًا

من تصميم الباحثة

وتُعد هذه البرامج من أكثر أدوات الهجمات السيبرانية شيوعًا، وتشتمل هذه البرمجيات على: **الفيروسات Viruses**؛ هي برامج لها القدرة على نسخ نفسها أكثر من مرة، وتنتج ملفات مُزيفة تحل محل الملفات الأصلية، **وأحصنة طروادة Trojans Horse** هي برامج تجسُسية، وتعرف بأنها نوع من البرامج الضارة تظهر في صورة مُتخفية على أنها برامج وملفات شرعية، أما **برامج التجسُس Spyware**؛ هي برامج تقوم بمراقبة الضحية، وإرسال كافة المعلومات التي يقوم بها فور اتصاله بشبكة الإنترنت، **والديدان Warms**؛ وهي برامج تنتقل عبر البريد الإلكتروني تمتاز بقدرة على التنقل عبر شبكات الإنترنت، الهدف منها تشويش سرعة الإنترنت في نقل المعلومات، **وبرامج الفدية Ransomware**، وهي من أكثر البرامج التي تهدد الأمن السيبراني على مستوى العالم، تلك البرامج التي تستهدف تشفير ملفات الضحايا، وتطلب دفع فدية مُقابل فك تشفير الملفات، ومُهمتها أن تمنع الضحايا من الوصول إلى معلوماتهم. ومن ثم، فإن دمج الذكاء الاصطناعي في الهجمات السيبرانية يمكن أن يعزز بشكل كبير من تأثيرات هذه الهجمات، ويزيد من فاعليتها (تقى النجار، ٢٠٢٤م: ٩٨) ومن ضمن المُشكلات التي حدثت عام ٢٠٢٠م اختراق بيانات أبحاث فيروس كورونا

في كاليفورنيا، وفي المُقابل يتم دفع مبلغ مالي بمقدار ١.١٤ مليون دولارًا (هدى عدلي، ٢٠٢٣م: ٢٠٩). كُل هذه البرامج تستهدف سرقة البيانات والمعلومات الحساسة.

٢- **الهندسة الاجتماعية:** ظهرت الهندسة الاجتماعية نتيجة للتقدُم التكنولوجي في عصر المعلومات وتكنولوجيا الاتصالات، وأصبح من الصعب تحديد الفرق بين ما هو حقيقي، وما هو زائف، وزاد الاستغلال والتلاعُب بالمُعتقدات والمعارف عبر وسائل التواصل الاجتماعي؛ مما أدى إلى انتشار المعرفة الفوضاوية التي كانت سببًا في اختراق العقول وهندستها، حيث تعتمد الهندسة الاجتماعية على سمات مُحددة؛ لاتخاذ القرارات والمعروفة باسم التحيُزات المعرفية، تلك التحيُزات التي تُسمى أحيانًا بالأخطاء في الأجهزة البشرية، وهي تُعد نتاج مُعالجة المُخ للمعلومات بصورة سريعة، وتُصنف جرائم الهندسة الاجتماعية لصنفين، **أولهُما: الهندسة الاجتماعية القائمة على أساس تقني،** ويقصد بها البرامج والتقنيات التي تُساعد المُخترقين في الوصول إلى المعلومات، ومنها: الاحتيال الإلكتروني، والاحتيال الصوتي، والرسائل الاقتحامية المُزعجة. **ثانيها: الهندسة الاجتماعية القائمة على أساس بشري أو إنساني،** وهي التي تتضمن الانتحال الإلكتروني (عبد الرحمن محمد عبد الظاهر، ٢٠٢٤م: ٤٤٤). وفي عام ٢٠٢٠م ظهر عدد من القضايا والتحديات التي واجهت الأمن السيبراني، ومنها ما يخُص الهندسة الاجتماعية، وكان ٩٠% من المُشكلات تتعلق بالنصب والاحتيال، وكان من أشهر هذه الحوادث التي ظهرت في ٢٠٢٠م سرقة مُجرمي الإنترنت ما يُقارب من ٢.٣ مليون دولارًا أمريكيًا من مدرسة في مدينة تكساس (وهي ثاني أكبر ولاية في الولايات المُتحدة الأمريكية)، مما عرض بيانات الطُلاب للخطر (هدى عدلي، ٢٠٢٣م: ٢٠٩). كما تستخدم الهندسة الاجتماعية عرضًا مُشوقًا لخداع الأفراد وإقناعهُم بالكشف عن معلوماتهم سرية، أو التفاعل مع روابط أو رسائل خبيثة. قد تتضمن الهندسة الاجتماعية **الاحتيال الإلكتروني،** ويعني إرسال رسائل تُحيل إلى روابط ضارة. أما **التصيد الاحتيالي،** ويعني اختراق البريد الإلكتروني عبر رسائل قصيرة تُستخدم على أنها رسائل شرعية تقوم هذه الرسائل بتوجيه الضحايا على مواقع الويب الضارة (فاطمة علي إبراهيم، ٢٠٢٢م: ٤٠٦). قد يكون هذا الحادث من ضمن الحوادث التي سلطت الضوء على أهمية تعزيز الأمن السيبراني بصفة عامة، وفي المؤسسات التعليمية بصفة خاصة لما تحتويه من معلومات حساسة، وموارد مالية مُتزايدة، مما يُهدد الأمن القومي.

٣- **الامتناع عن الخدمة:** والتي تهدف إلى تعطيل الخدمات من خلال تعطيل الشبكة بتكرار الطلبات الضارة، أو زيادة حجم الخدمات المُرسلة إلى الخادم، مما يؤدي إلى تعطيل المواقع الإلكترونية. هذا بالإضافة إلى **سرقة الهوية:** باستخدام سرقة البيانات الشخصية للأفراد بهدف استخدامها في أنشطة غير قانونية للأفراد مثل: الاحتيال المالي، وسرقة الهوية الرقمية (أحمد سالم علي حسين، ٢٠٢٤م: ١٦٨٩).

لذلك يجب على المواطنين أن يكونوا على وعي ودراية بأنواع الهجمات الإلكترونية، وأساليب الاحتيال، والابتزار الشائعة، وحِماية أنفسهُم وأجهزتهُم من هذه الهجمات، وضرورة الحذر من المخاطر المُحتملة مثل: فقدان الهوية الرقمية، وانتشار المعلومات المُضللة، وفقدان الوظائف...إلخ. والحرص على تثبيت برامج مُضادة للفيروسات، واستخدام كلمات مُرورية قوية، وتجنب الاستجابة لأي رسائل احتيالية مجهولة المصدر، فالأمن السيبراني ليس مُجرد تقنية، بل هو ثقافة يجب ترسيخها في المُجتمع.

المحور الرابع- مُتطلبات تحقيق الأمن السيبراني:

هُناك عدد من المُتطلبات الأساسية التي يجب توافرها لتحقيق الأمن السيبراني، وتتمثل في:

١- **مُتطلبات مادية:** تتمثل المُتطلبات المادية في توفير عدد من الأجهزة الإلكترونية الحديثة، وتزويدها بعدد من البرامج الخاصة بالوقاية، والحماية من الهجمات السيبرانية، إضافة إلى ربط هذه الأجهزة بقاعدة بيانات مؤمنة ومحمية، فضلًا عن توفير برامج مُضادة للفيروسات، وكذلك تنصيب أجهزة الجدار الناري تلك الأجهزة المُخصصة تقوم بمراقبة العمليات التي تمر بالشبكات، وترفض أو تسمح بمرور البرامج طبقًا لعدد من القواعد الأمنية (علي عبد الصمد آل فرهاد، ٢٠٢٣م: ٢٦٤). استطاعت مِصر أن تقوم بإنشاء وحدة لطوارئ الإنترنت والحاسب الآلي عام ٢٠١٢م، تحت مُسمى "المركز المصري للاستجابة للطوارئ المعلوماتية" (EG- CERT) تختص تلك الوحدة بأمن وحِماية المعلومات.

٢- **مُتطلبات إدارية:** لابد وأن تحدد كُل مؤسسة الإجراءات التنفيذية للازمة، لتحقيق الأمن السيبراني، وذلك حسب طبيعتها، ولابد من تحديد المبادئ والقواعد اللازمة لتحقيق الأمن السيبراني، وتحديد الصلاحيات المتاحة، وعدم السماح باستخدام النظام، إلا فيما هو مُعد لأجله، وفي الإطار المسموح بِه. وهو ما أشارت إليه دراسة (بهاء الدين حمودة حسن حمودة، ٢٠١٤م: ٥٩) بضرورة إنشاء وحدة

إدارية تهتم بُمتابعة تحقيق اللاوازم الخاصة بتحقيق الأمن السيبراني، وذلك للحِماية من الهجمات السيبرانية، وإعداد وثيقة تتضمن مجموعة من التعليمات والقوانين التي تتوافق مع سياسات الإدارة العُليا ومُتابعة تطبيقها. كما أن من أبرز المُتطلبات الإدارية لتحقيق الأمن السيبراني، وضع سياسات وإجراءات مكتوبة توضح للعاملين في أي مؤسسة، سواء كانت حُكومية أو خاصة، كيفية حِماية البيانات والمعلومات التي تخص الكيان المؤسسي. هذا بالإضافة إلى إجراء عدد من التدريبات لتدريب الموظفين والعُمال حول مبادئ الأمن السيبراني، مثل: التعرُف على رسائل التصيد الاحتيالي، والتأكيد على أهمية استخدام كلمات مرور قوية.

٣- **مُتطلبات بشرية:** تتمثل المُتطلبات البشرية في توفير كوادر بشرية مؤهلة لمواكبة التطورات التكنولوجية الحديثة، لذلك أطلقت الدولة المِصرية مُبادرة "مهارات سيبرانية" بتاريخ ١٩ مايو ٢٠٢٤م بهدف إعداد جيل جديد من الكوادر في مجال الأمن السيبراني، الذي يُعد من ضمن أكثر التخصُصات طلبًا في سُوق العمل. كما تهدف المُبادرة إلى تأهيل ١٠٠٠ طالب جامعي سنويًا، للتوظيف مُباشرة بعد التخرج من الجامعة في هذا المجال، وتعتمد المُبادرة على تدريس مناهج عملية تتلاءم مع مُتطلبات سوق العمل، لتقليص الفجوة بين العرض والطلب على مستوى الكوادر البشرية المُتخصصة في الأمن السيبراني. وسيتم تنفيذ المُبادرة أثناء الدراسة الجامعية للطالب من خلال شراكات استراتيجية، وأطر تعاون بين جهات حُكومية وأكاديمية، وشركات القطاع الخاص؛ حيث سيتم دمج المواد الدراسية العملية، والتدريب العملي في المعامل الموجودة بالجامعات، ومراكز التدريب الخاصة بوزارة الاتصالات، وتكنولوجيا المعلومات (مركز المعلومات، ودعم اتخاذ القرار، ٢٠٢٤م: ٥٩).

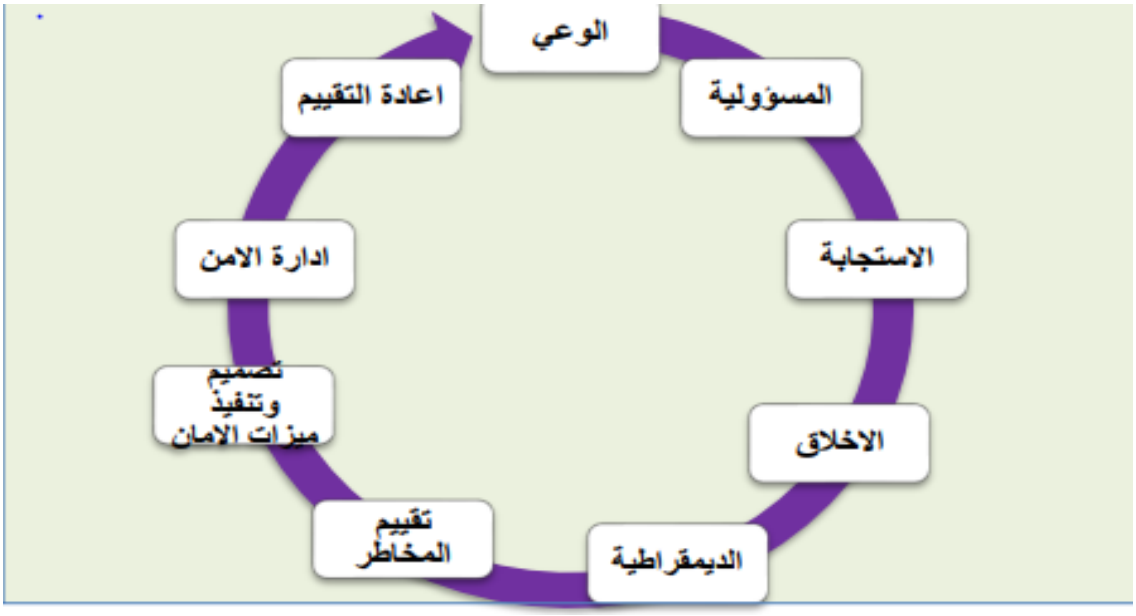
٤- **مُتطلبات تقنية:** تتمثل في تطوير البنية التحتية اللازمة لتحقيق الأمن السيبراني، وكما ذكر كُل من "ميلوس" و"ميراندا" (**Milos Zec & Miranda Kajtazi, 2015: 231**) أن الجانب التقني يُركز على إيجاد عدد من التدابير التكنولوجية الأساسية، مثل: وجود جدار حماية للإنترنت وسجلات أحداث النظام، ووجود قائمة جرد للأجهزة والبرامج. هذا بالإضافة إلى التأكيد على النسخ الاحتياطي للبيانات، وبرامج مكافحة الفيروسات وقواعد كلمة المرور. وبناءً على ذلك، استطاعت مِصر أن تقوم بتأسيس المجلس الأعلى للأمن السيبراني عام ٢٠١٤م، بهدف حِماية البنية التحتية المعلوماتية للدولة ككل بكافة مؤسساتها، كما استطاعت إطلاق الاستراتيجية الوطنية للأمن السيبراني (٢٠٢٣-

٢٠٢٧) بهدف التصدي للحوادث السيبرانية، كما أصدرت مِصر عدة قوانين لدعم الأمن السيبراني مثل: قانون مُكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨م، ذلك القانون الذي يُحدد العقوبات الخاصة بالجرائم الإلكترونية، هذا بالإضافة إلى قانون حماية البيانات الشخصية رقم١٥١ لسنة ٢٠٢٠م، لحماية البيانات الشخصية للأفراد، ووضع معايير لحمايتها.

المحور الخامس– الرؤى المُستقبلية لتطور سياسات مُتطلبات الأمن السيبراني:

حتى نتمكن من وضع تصور مُقترح لتطوير مُتطلبات تحقيق الأمن السيبراني في ضوء رؤية مِصر ٢٠٣٠، لابد من التعرُف على عناصر الأمن السيبراني، وأهدفه، ثم تحديد الأسس والمبادئ التي يقوم عليها التصور المُقترح.

أ. **عناصر الأمن السيبراني:** للأمن السيبراني عدة عناصر لابد من توفراها لمواكبة التغيرات التكنولوجية السريعة والمُتلاحقة، وبعد الاطلاع على التُراث البحثي، تبين وجود عدة عناصر تُهدد الأمن السيبراني، وتعمل على زعزعة الأمن القومي. انظر الشكل رقم (٢) لعناصر الأمن السيبراني.



الشكل رقم (٢)

المصدر: (ضحى لعيبي كاظم السدخان، ٢٠٢١م: ١٩٥).

ومن هذه العناصر ما ذكرته دراسة (ضحى لعيبي كاظم السدخان، ٢٠٢١م: ١٩٦) بأن **الوعي:** يُعد أحد أهم عناصر تحقيق الأمن السيبراني من خلال إدراك المُشاركين، وحاجتهم إلى أمن أنظمة المعلومات وشبكاتها. والتأكيد على **مسئولية المشاركين**، بأن المشاركين هُم المسئولون الحقيقيون عن أنظمة المعلومات

وتأمينها، وفقًا لأدوراهم وسياساتهم. هذا بالإضافة إلى **استجابة** وانتباه المسئولين عند حدوث أي هجمات سيبرانية، والحرص على تبادل المعلومات لتفادي المخاطر الإلكترونية التي يُمكن حدوثها في تلك الفترة. وزيادة التأكيد على مبدأ **الديمقراطية** من خلال اعتراف المُشاركين بضرورة تبادل الأفكار والمعلومات بُكل حُرية، مع ضرورة الحفاظ على سريتها وحمايتها، بما يتفق مع القيم المُتعارف عليها مع حقوق الملكية. والحفاظ على **الأخلاق** من خلال اعتراف المُشاركين بأنهُم المسئولون عن أفعالهم، وأن تقاعُسهم عن القيام بأعبائهم الوظيفية يضُر بمصلحة الآخرين. هذا بالإضافة إلى **التقييم الدوري للمخاطر** الذي يُساعد على اكتشاف التهديدات والتعرف على نقاط الضعف؛ مما يُساعد على اختيار أدوات مُناسبة لتفادي الأضرار المُتوقعة. إلى جانب **تصميم ميزات الأمان وتنفيذها** التي تؤكد على ضرورة الاعتبارات الأمنية كعُنصر أساسي من عناصر تحقيق الأمن السيبراني، الذي يُساعد في تخطيط وتنظيم وتشغيل واستخدام نُظم وشبكات المعلومات. والتأكيد على **إدارة الأمن،** وذلك من خلال اتباع نهج مُتكامل لإدارة الأمن، والعمل على التقييم الديناميكي للمخاطر، من أجل حِماية المُشاركين والعمليات التي يقمون بها. وفي النهاية يتم التأكيد على **إعادة التقييم،** وذلك من خلال أمن أنظمة وشبكات المعلومات، وإجراء التغييرات المُناسبة على السياسات والمُمارسات، والتدابير والإجراءات الأمنية، مع إمكانية ظهور تهديدات ومواطن ضعف جديدة. وللنهوض بالأمن السيبراني والاستثمار التكنولوجي في مِصر، يُقترح وجود هيئة مُستقلة تعمل على تعزيز وتطوير شركات الأمن السيبراني الناشئة، مُمثلة في شركات الأمن السيبراني، وخبراء الذكاء الاصطناعي والأمن السيبراني من المُتخصصين من أساتذة الجامعة، ومُمثلين الهيئات العامة، والخبراء ومُمثلين لرئاسة مجلس الوزراء...إلخ.

- **التصور المُقترح، وفقًا لتحليل الوضع الراهن:**

أ. **أهداف التصور المقترح:** تستهدف التوجهات المُستقبلية لتحقيق مُتطلبات الأمن السيبراني في ضوء رؤية مصر ٢٠٣٠، على ما يلي:

- مُحاولة الوقوف على العوامل المُساعدة في تطوير وتحسين تطبيقات استخدام الأمن السيبراني، والتغلُب على الصعوبات التي تُعيق تحديده.
- تحديد الدور الذي تقوم بِهِ مُنظمات الدولة، الحُكومية وغير الحُكومية، في بناء توجهات مُستقبلية تُساعد في توفير تطبيقات الأمن السيبراني للحد من الهجمات التي يتعرض لها.

- الحرص على إعداد مجموعة من الخطط والبرامج التي تُسهم في إصلاح ودعم مجالات الأمن السيبراني في المُجتمع المصري، والعمل على تطويره.
- توجيه المُنظمات، الحُكومية وغير الحُكومية، نحو استخدام مواقع إلكترونية أكثر خصوصية عند تقديم المعلومات الشخصية، بصورة أكثر احترافية حفاظًا على البيانات السرية. هذا بالإضافة إلى النسخ الاحتياطي للملفات.
- إعداد دورات تدريبية تعمل على توعية الموظفين في المؤسسات المُختلفة في التعامل مع البرامج التي تساعد في الحفاظ على المعلومات. هذا بالإضافة إلى توجيههم إلى الروابط التي تعمل على اختراق الملفات المهُمة.
- التوسع في البرامج المُقدمة في ضوء رؤية مِصر ٢٠٣٠، وإيجاد منظومة تنموية مُتطورة تعمل على زيادة وعي الأجيال القادمة بأهمية التحول الرقمي.
- العمل مع وجود كوادر بشرية مُدربة في التعامل مع مجال الأمن السيبراني وتكنولوجيا المعلومات والاتصالات؛ وذلك لمواكبة التغيرات السريعة والمُعقدة.

ج.الأُسس والمُقترحات التي يقوم عليها التصور المُقترح: اعتمدت الباحثة على عدد من الأُسس لوضع التصور المُقترح منها:

- **نتائج وتوصيات التُراث البحثي المعني بموضوع الدراسة،** وما نتج عنها من وضع بعد الاستنتاجات التي أسهمت في وضع عدد من المؤشرات منها: ١- **مؤشرات الأداء الأمني:** من خلال رصد الحوادث السيبرانية الناتجة عن الهجمات السيرانية، ومستوى تدريب الموظفين. ٢- **مؤشرات البنية التحتية الأمنية:** من خلال توافر مراكز مُتخصصة لمُراقبة الأنظمة، والاستجابة للتهديدات. هذا بالإضافة إلى توثيق الحوادث الأمنية. ٣- **مؤشرات التهديدات والضعف:** من خلال رصد عدد الاختراقات أو الهجمات التي تم التصدي لها، هذا بالإضافة إلى تحديد مستوى خطورة التهديد والضعف (مُنخفضة ومُتوسطة وعالية).
- **الإطار النظري المُتعلق بمقولات نظريتي:** مُجتمع المخاطر لـ "أويرليش بيك"، والتشكيل البنائي لـ "أنتوني جيدنز". وما تضمنه من استطلاع لواقع تحقيق متطلبات الأمن السيبراني والمُشكلات التي تحد تحقُقه في ضوء رؤية مِصر ٢٠٣٠.

د. دواعي بناء تصور مُقترح للتوجهات المُستقبلية في ضوء رؤية مصر ٢٠٣٠:

- ضرورة تعزيز التعاون الدولي لمُكافحة الانتهاكات السيبرانية، وتحديد المسئولية لمن يقف خلفها من أفراد أو مؤسسات أو دول، وذلك مع مُراعاة حقوق الإنسان.
- ضرورة إنشاء هيئات ومُنظمات خاصة بالتحول الرقمي لمواكبة تغيرات العصر الحديث.
- الحاجة إلى تفعيل دور المُنظمات المُختلفة لتبني برامج ومُبادرات توعوية لمخاطر الهجمات السيبرانية.
- القصور في العناية بالجوانب الثقافية للأجيال القادمة، كونهُم صُناع التغيير في المُجتمعات المُعاصرة.

هـ. آليات تنفيذ وبناء التصور المُقترح للتوجهات المُستقبلية بشأن الأمن السيبراني في ضوء رؤية مصر ٢٠٣٠:

- **دور المُنظمات الحُكومية (وزارة التعليم العالي والبحث العلمي، ووزارة الاتصالات وتكنولوجيا المعلومات ووزارة الثقافة):**

- على الجامعات، مُمثلة في: كُلية الحاسبات والمعلومات وكُليات الهندسة، أن تعمل على تدشين، وتفعيل عدد من المؤتمرات واللقاءات العلمية داخل وخارج الكُليات؛ في موضوعات تختص بمُتطلبات الثورة الصناعية الرابعة والخامسة، والعمل على إجراء عدد من الأبحاث والدراسات تخدم عددًا من المجالات لمواكبة سوق العمل.
- تفعيل مبدأ الشراكة بين الجامعات ومُنظمات المُجتمع المدني، بإجراء مُبادرات تُساعد على الاستثمار والعناية بمهارة الطلاب والباحثين في مجال ريادة الأعمال. هذا؛ بالإضافة إلى الاستفادة من التجارب العالمية المُتميزة في مجال التكنولوجيا، بما يخدم سوق العمل المِصري في ضوء تغيرات التحول الرقمي.
- تشجيع وزارة التعليم العالي والبحث العلمي بإنشاء كُليات للذكاء الاصطناعي، وإعداد عدد من البرامج المُختلفة التي تخدم سوق العمل.
- إقرار وزارة التعليم العالي والبحث العلمي بتخصيص بعض البرامج والدورات التي تختص بمجال تكنولوجيا المعلومات في المُقررات الدراسية، لا للكُليات العلمية فحسب؛ بل للنظرية أيضًا.
- تدريب الطُلاب على استخدام تكنولوجيا الذكاء الإصطناعي في البحث العلمي.
- حِماية شبكة تكنولوجيا الاتصال والمعلومات والعمل على إعداد برامج للمُساعدة في كشف هجمات العدو والعمل على التصدي لها.

- **دور مُنظمات المجتمع المدني الخاصة بتنمية مهارات الشباب في مجال الأمن السيبراني:**

- على مُنظمات المُجتمع المدني أن تقوم بمُساندة الدولة المِصرية في توفير نظام للإنذار المُبكر ضد البرمجيات الخبيثة، والهجمات والتهديدات الإلكترونية.
- إيجاد عدد من البرامج التي تعمل على توفير قاعدة معلومات شاملة عن تطبيقات الأمن السيبراني ومواجهة التحديات التي تقف عائقًا أمام تلك التطبيقات.
- مُساعدة تلك المُنظمات في توفير الموارد والإمكانات اللازمة لتوعية الأجيال القادمة بأضرار التحول الرقمي، إذا أساء استخدامه.
- تشجيع العمل التطوعي من جانب الشباب ذي الخبرة في مجال تكنولوجيا المعلومات بنشر الوعي بمزايا الأمن السيبراني، وعيوب الهجمات السيبرانية. وبهذا يستطيع الفرد تأمين المُجتمع من مخاطر الأمن السيبراني، والتقليل من الهجمات الإلكترونية التي تؤثر عليه سلبًا، فهذا يؤكد على حِماية المُجتمع من الهجمات السيبرانية، كما أكد "أنتوني جيدنز" في نظريته.

سادسًا_ السيناريوهات المُستقبلية لتحقيق الأمن السيبراني في مِصر:

تتطلب حِماية مِصر من مخاطر الهجمات السيبرانية، وضع استراتيجيات مُتكاملة لمواجهة التهديدات المُتزايدة التي تُلاحقها في ظل استخدام تقنيات الذكاء الاصطناعي، كما ذكرت سلفًا. لهذا تسعى الدراسة الراهنة إلى استشراف ملامح المُستقبل من خلال سيناريوهات؛ أحدهما مُحتمل، والثاني مُتوقع، والثالث مرغوب فيه. وسوف تُقدم الباحثة مع كل سيناريو العوامل المؤثرة، والنتائج المتوقعة، والتوصيات اللازمة لتحقيق كُل سيناريو، كما هو موضح في الجدول رقم (١):

جدول رقم (١) يوضح السيناريوهات المُستقبلية

السيناريو	العوامل المؤثرة	النتائج المُتوقعة	التوصيات
السيناريو الأول (المُحتمل)	-كُلما زادت الاستثمارات في الأمن السيبراني زادت قدرة مِصر على مواجهة التهديدات. – التعاون الدولي بين مِصر والاستفادة من الشراكات مع الدول المُتقدمة في الأمن السيبراني. – تدريب الكوادر وزيادة الوعي لدى الأفراد والمؤسسات بشأن الأمن السيبراني.	– زيادة الاستثمار في البنية التحتية الرقمية، مما يؤدي إلى قلة الهجمات السيبرانية. – تحسين التعاون بين القطاعي الحُكومي والخاص نتيجة لمُشاركة المعلومات حول التهديدات السيبرانية، مما يُساعد التصدي لها بكل فاعلية. – انتشار الوعي الأمني بين الأفراد والمؤسسات مما يؤدي إلى قلة أخطاء المُستخدمين.	– إنشاء مراكز استجابة سريعة للهجمات السيبرانية على مستوى الجمهورية. – نشر الوعي العام بين الأفراد والشركات حول أهمية الأمن السيبراني حتى لا نكون ضحية لاستغلال المُنتهكين، وارتكاب الجرائم تجاههُم.
السيناريو الثاني (المُتوقع)	– من المتوقع في الفترة القادمة أن يتم التركيز على أنظمة الذكاء الاصطناعي، وأدوات الحِماية من الهجمات السيبرانية، وذلك لرصد التهديدات والاستجابة لها بشكل لحظي. – يتطلب تحقيق الأمن السيبراني التعاون الدولي لوضع أطر تنظيمية موحدة لتبادل المعلومات حول الهجمات السيبرانية وسرعة التعامل معها. – ستصبح المهارات السيبرانية مطلبًا أساسيًا للعاملين في القطاعات كافة، مما يستدعي تنفيذ برامج تدريب دورية لتعزيز الوعي الأمني.	– تحسين الكفاءة الإنتاجية نتيجة للاعتماد على أنظمة الذكاء الاصطناعي. – تقليل حجم الاختراقات. – تقليص خسائر القطاعات.	– توجيه وزارة الاتصالات وتكنولوجيا المعلومات في العمل على إنشاء منصة للتوعية بالأمن السيبراني تشتمل على: فيديوهات، ومنشورات، وإرشادات توعوية بمخاطر الهجمات السيبرانية وكيفية مواجهتها.
السيناريو الثالث	-تطوير القوانين الخاصة بالأمن	– وجود لائحة تنفيذية شاملة للمواد	-إعداد الكثير من الكوادر في

(المرغوب فيه)	السيبراني مع تطبيق عقوبات صارمة على الجرائم السيبرانية مُتمثلة في قانون الأمن السيبراني لتجريم الجاني. خاصةً بعد أن أصدرت مِصر عددا من التشريعات القائمة على قانون جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨م، وفرض ضوابط ومعايير قياسية على المؤسسات لحماية البيانات والمعلومات من خلال قانون حِماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠م. – تبني تقنيات حديثة بشكل مُوسع حتى لا نترك المجال لأي اختراق. – أن تعمل الدولة على بناء برامج دفاعات سيبرانية قوية من خلال مُبادرات دفاعية مثل مُبادرة Clean Pipe Technology (مُبادرة تقنية الأنابيب النظيفة) وهي مُبادرة تهدف إلى تحسين كفاءة واستدامة خطوط الأنابيب المُستخدمة في نقل السوائل مثل: النفط والغاز والمياه، والمواد الكميائية. أسوة بالدول المُتقدمة كـ: الولايات المتحدة الأمريكية، وكندا والإمارات والمملكة العربية السعودية، وذلك مع مُقدمي خدمة الإنترنت لتقليل الهجمات الإلكترونية.	القانونية في النظام القانوني المصري، لتوضيح النصوص الخاصة بتقنية المعلومات، وحماية البيانات والمعلومات على شبكة الإنترنت.	مجال الأمن السيبراني من خلال إنشاء حاضنات للمشاريع الصغيرة من خلال عدد من البرامج تشتمل على: الدعم الفني والإداري والتسويقي والمادي لضمان استمرارية المشروعات ورفع كفاءة الشباب المصري، من خلال تشجيع الاستثمار المحلي على الأجنبي في مجال الأمن السيبراني.

المراجع:

١- المصادر:

- الأجندة الوطنية للتنمية المستدامة رؤية مصر ٢٠٣٠، (٢٠٢٣م): وزارة التخطيط والتنمية الاقتصادية.
- الاستراتيجية الوطنية للأمن السيبراني ٢٠٢٣-٢٠٢٧، وزارة الاتصالات وتكنولوجيا المعلومات، رئاسة مجلس الوزراء المجلس الأعلى للأمن السيبراني.

٢- المراجع العربية والمترجمة:

- أحمد زايد، (يناير/ مايو ١٩٩٦م): آفاق جديدة في نظرية علم الاجتماع: نظرية تشكيل البنية (نظرية البنينة)، المجلة الاجتماعية القومية، مج ٣٣، ع (١، ٢)، يناير ومايو، (٥٧- ٨٥).
- أحمد سالم علي حسين، (٢٠٢٤م): الأمن السيبراني القوة الرابعة لتعزيز الأمن والدفاع: البنية التحتية الفوائد والمخاطر، مجلة الدراسات المستقبلية، الجمعية العلمية للدراسات التربوية المستدامة، مج٦، ع١، (١٦٨٢- ١٧٠٥).
- إسلام فوزي، (٢٠١٩م): الأمن السيبراني: الأبعاد الاجتماعية والقانونية: تحليل سوسيولوجي، المركز القومي للبحوث الاجتماعية والجنائية، مج٥٦، ع٢، (٩٩- ١٣٩).
- أنتوني جيدنز، (٢٠٠٥م): علم الاجتماع، ترجمة وتقديم: فايز الصباغ، مركز دراسات الوحدة العربية، بيروت، ط٤.
- أولريش بيك (٢٠١٣م): مجتمع المخاطر العالمي: بحثًا عن الأمان المفقود، ترجمة : علا عادل وآخرون، المركز القومي للترجمة، القاهرة.
- بدر عدنان أحمد سعد الخبيزي، (٢٠٢٣م): تحديات وتهديدات الأمن السيبراني وكيفية التغلُب عليها، حوليات كلية الآداب جامعة عين شمس، مج٥١، (٢٣١- ٢٥٢).
- بهاء الدين حمودة حسن حمودة، (٢٠١٤م): سياسة أمن المعلومات في شبكة المكتبات بجامعة النيلين: دراسة حالة، المجلة العربية الدولية المعلوماتية، اتحاد الجامعات العربية، جمعية كليات الحاسبات والمعلومات، مج٣ ، ع٥، (٥٥-٦٢).
- تقى النجار، (٢٠٢٤م): الذكاء الاصطناعي والإرهاب..ازدواجية الأدوار، منشور في: التطور التكنولوجي بين التحديات والفرص، مجلة الديمقراطية، ع٩٦، (٩٦- ١٠١).

- جيهان سعد محمد الخضري، وهدى جبريل علي سلامي، ونعمة ناصر مدبش كليبي، (٢٠٢٠م): الأمن السيبراني والذكاء الاصطناعي في الجامعات السعودية "دراسة مُقارنة"، مجلة تطوير الأداء الجامعي، مج١٢، (٢٧٣٥- ٣٢٢٢).
- سمير قلاع الضروس، (٢٠٢٢م): الأمن السيبراني الوطني: قراءة في أهم الاستراتيجيات الأمنية والتقنية لمواجهة الجريمة الإلكترونية بالجزائر، مجلة الرواق للدراسات الاجتماعية والإنسانية، المركز الجامعي أحمد زبانة غليزان، مخبر الدراسات الاجتماعية والنفسية والأنثروبولوجية، مج٨، ع٢، (٢٤٩- ٢٦٧).
- صلاح الدين محمد توفيق، وشيرين عيد مرسي، (٢٠٢٢م): متطلبات تحقيق الأمن السيبراني بالجامعات المصرية في ضوء التحول الرقمي من وجهة نظر أعضاء هيئة التدريس "جامعة بنها أنموذجًا"، المجلة التربوية، كلية التربية، جامعة سوهاج، مج ١٠٥، (٧٣٧- ٨٦١).
- ضحى لعيبي كاظم السدخان، (٢٠٢١م): البعد الجيو سياسي للأمن السيبراني، مجلة العلوم الإنسانية، علي كافي تندوف الجزائر، مج ٥، ع١، (١٨٨- ٢٢٣).
- عبد الرحمن عاطف أبو زيد، (٢٠١٩م): الأمن السيبراني الوطن العربي: دراسة حالة المملكة العربية السعودية، آفاق سياسية، المركز العربي للبحوث والدراسات، ع٤٨، (٥٥- ٦١).
- عبد العزيز بن أحمد المزيني، (٢٠٢٢م): الأمن السيبراني واجب من واجبات الدولة الحديثة ووسائل تحقيقه التنظيمية: دراسة تأصيلية مقارنة، مجلة قضاء، جامعة الإمام محمد بن سعود الإسلامية الجمعية العلمية القضائية السعودية، (٤٩٢- ٥٤٢).
- عبد العزيز قاسم محارب، (٢٠٢٣م): الذكاء الاصطناعي والأمن السيبراني، مجلة المال والتجارة، العدد ٦٥٣، (٤- ٢٣).
- عبد الله بن شرف الغامدي، (٢٠١٨م): الجرائم السيبرانية والتحديات المُستقبلية، المجلة العربية: الأمن السيبراني حروب الأرقام الصماء، ع٤٩٨.
- عبد الرحمن محمد عبد الظاهر محمد، (يناير ٢٠٢٤م): فعالية برنامج في طريقة العمل مع الجماعات وتوعية الشباب الجامعي بمخاطر الهندسة الاجتماعية، في ضوء رؤية مصر ٢٠٣٠، مجلة دراسات في الخدمة الاجتماعية، ع٦٥، ج٢، (٤٣٥- ٤٧٨).

- علي آل مداوي، (٢٠٢٣م): الأمن السيبراني: تعريفه –أهميته– أنواعه– استراتيجيات الوقاية من الهجمات السيبرانية، مجلة الدراسات الدولية، ع٢٤، (١١٥– ١٢٤).
- علي عبد الصمد آل فرهاد، (٢٠٢٣م): مُتطلبات الأمن السيبراني لأنظمة المعلومات الإلكترونية، مجلة آداب البصرة، كلية الآداب، جامعة البصرة، ع١٠٦، (٢٥٥–٢٦٦).
- فاطمة علي إبراهيم ورحاب يوسف ووليد محمود السيد، (٢٠٢٢م): الأمن السيبراني والنظافة الرقمية، المجلة المصرية لعلوم المعلومات، كلية الآداب، جامعة بني سويف، مج٩، ع٢، (٣٩٠– ٤٢٢).
- محمد العربي، (٢٠١٨م): بناء السيناريوهات المستقبلية دليل نقدي، مركز الدراسات الاستراتيجية، القاهرة.
- محمد خليفة، (٢٠٠٨م): الحماية القانونية لمعطيات الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية.
- محمد زين العابدين علي حنفي، (٢٠٢٣م): الأمن السيبراني ومنظومة التعليم الدولية، مجلة القراءة والمعرفة، جامعة عين شمس، كلية التربية، الجمعية المصرية للقراءة والمعرفة، ع٢٦٠، (٥٥–٩٦).
- محمد ناصر، (٢٠٢٢م): أشكال انتهاك الفضاء السيبراني ووسائلها وأثارها، مجلة الندوة للدراسات القانونية، قارة وليد، ع٤٠، (٨٦–١٢٠).
- مركز المعلومات ودعم اتخاذ القرار، (٢٠٢٤م): شركات الأمن السيبراني الناشئة (جهود مصرية وفرص عالمية)، مجلس الوزراء المصري.
- معتز نادي، (٢٠٢٤م): طوفان العالم الرقمي..اختبار اقتصادي وتحدي الذكاء الاصطناعي، منشور في: الطبقة الوسطى المصرية خزانة القيم، مجلة أحوال مصرية، مركز الدراسات السياسية والاستراتيجية، جريدة الأهرام، ع٩٣، (١١٢–١١٩).
- نبيلة محمد عبد الدايم أحمد الحداد، (أغسطس ٢٠٢٢م): متطلبات تحقيق الأمن السيبراني في المكتبات الجامعية اليمنية "دراسة حالة"، مجلة جامعة البيضاء، مج٤، ع٢، (٧٠٣– ٧١٥).
- نهى مجدي محمد السيد، ٢٠٢١م: الأمن السيبراني وعلاقته بالمضمون الإعلامي في ظل رؤية مصر ٢٠٣٠م، المجلة العربية لبحوث الإعلام والاتصال، ع٣٥، (٤٨٤– ٥١٥).

- هبة جمال الدين، (٢٠٢٣م): الأمن السيبراني والتحول في النظام الدولي، مجلة كلية الاقتصاد والعلوم السياسية، جامعة القاهرة، مج٢٤، ع١، (١٨٩-٢٣٠).
- هدى عدلي، (٢٠٢٣م): واقع وتحديات الأمن السيبراني وإجراءاته، مجلة قانونك، ع١٦، (١٨٥- ٢١٨).
- وليد عبد الرحمن جاب الله، (٢٠٢١م): الأمن السيبراني بين الاحتكار والاستثمار، مجلة الديمقراطية، مؤسسة الأهرام، مج٢١، ع٨٢، (٤٩-٥٣).
- يحي خير الله عودة، (٢٠١٢م): نظرية التشكيل البنائي عند أنتوني جيدنز رفض الرؤية الأحادية للتفسير، مجلة آداب المستنصرية، العراق، ع٥٩، (١١٠- ١٢٩).

٣- المراجع الأجنبية:

- Bertrand Boyer, (2012): Cyberstratégie : l'art de la guerre numérique, Paris,NUVIS.
- Brookson Charles, Cadzow Scott, et al, (2015): Definition of Cybersecurity
- Martti Lehto, Pekka Neittaanmäki, (2015): Cyber Security: Analytics, Technology and Automation, intelligent Systems, Control and Automation: Science and Engineering.

Gaps and overlaps in standardization, European Union Agency for Network and Information Security, v1.0, pp (1-34).

- V.Karamchand Gandhi, (2012): An Overview Study on Cybercrimes in Internet, Journal of Information Engineering and Applications, ISSN 2224-5782 (print) ISSN 2225-0506 (online), Vol 2, No.1, pp (1-9).
- Zec Milos &Kajtazi Miranda, (September2015): Examining how IT Professionals in SMEs Take Decisions About Implementing Cyber Security Strategy, P aper Presented at Ecime 2015 - 9th European Conference , UK, this publication at: this publication at: https://www.researchgate.net/publication/338149057, pp (231- 239).