فاعلية استخدام الهيئة الوطنية للأمن السيبراني بالمملكة العربية السعودية لتقنيات الذكاء الاصطناعي كتوجه مستقبلي: دراسة استشرافية

إعـــداد:

أ.د/ دعـــاء فتحـــي سالـــم
أستاذ بقسم الاتصال التسويقي كلية الاتصال والاعلام
جامعة الملك عبد العزيز جدة المملكة العربية السعودية

أ.م.د/ محمد حاتم صلاح أبوالجدايل
أستاذ مشارك بقسم الاتصال التسويقي كلية الاتصال والاعلام
جامعة الملك عبد العزيز جدة المملكة العربية السعودية

فاعلية إستخدام الهيئة الوطنية للأمن السيبراني بالمملكة العربية السعودية لتقنيات الذكاء الاصطناعي كتوجه مستقبلي: دراسة إستشرافية

أ.د/ دعـــاء فتحـــي سالـــم
أستاذ بقسم الاتصال التسويقي كلية الاتصال والاعلام
جامعة الملك عبد العزيز جدة المملكة العربية السعودية

أ.م.د/ محمد حاتم صلاح أبوالجدايل
أستاذ مشارك بقسم الاتصال التسويقي كلية الاتصال والاعلام
جامعة الملك عبد العزيز جدة المملكة العربية السعودية

• **المستخلص:**

يتميز القرن الحالي بظهور تقنيات الذكاء الاصطناعي Artificial Tourism intelligence وتطبيقاتها في المجال الأمني بكافة عناصر المنظومة الأمنية، حيث أصبحت تلك التقنيات لها دور مهم على المستوى الدولي والعالمي في صناعة الأمن السيبراني وتسهم بدرجة كبيرة في الاقتصاد العالمي، مما يتطلب الاستعداد التام لتطوير كافة أطراف الصناعة الأمنية، من أجل ترسيخ مكانة المملكة العربية السعودية كمركز لوجستي عالمي، واعتمدت الدراسة في بنائها الرئيسي على نظرية انتشار المستحدثات التكنولوجية، وتعد هذه الدراسة من الدراسات الاستكشافية، حيث تم تطبيقها على عينة عشوائية بسيطة قوامها (١٠٦) مفردة من المسؤولين (العاملين) بالهيئة الوطنية للأمن السيبراني، من ذوي سنوات الخبرة والأعمار المختلفة، لرصد التأثيرات المتوقعة لفاعلية استخدام الهيئة لتقنيات الذكاء الاصطناعي كتوجه مستقبلي، مع توضيح الفائدة المتوقعة من استخدام تقنيات الذكاء الاصطناعي في مجال الامن السيبراني، والكشف عن واقع توظيف الذكاء الاصطناعي كأليه لحماية المعلومات والبيانات الخاصة بالمملكة، وتظهر أهمية تلك الدراسة من خلال الأهمية القصوى التي تحظى بها الهيئة الوطنية للأمن السيبراني في ظل رؤية المملكة٢٠٣٠ضمن محاورها الرئيسة، كما تظهر الأهمية من خلال الدور المهم الذى يمكن أن تؤديه تقنيات الذكاء الاصطناعي في خدمة القطاع الأمني من عدة زوايا، وأشارت الدراسة إلى العديد من النتائج من أهمها وجود علاقة دالة إحصائيًا بين الفائدة المتوقعة من استخدام تقنيات الذكاء الاصطناعي في الهيئة الوطنية للأمن السيبراني، وبين درجة نجاح هذا الاستخدام، كما أظهرت النتائج أيضا وجود علاقة دالة إحصائيًا بين إدراك المبحوثين لدور تقنيات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية، وبين اتجاهاتهم نحو دورها في دعم وتعزيز الأمن السيبراني، كما تعددت مجالات توظيف تقنيات الذكاء الاصطناعي في الهيئة الوطنية للأمن السيبراني، وفقا لما أجاب به مسؤولي الهيئة عينة الدراسة، وتمثلت أولى هذه المجالات في أمن الشبكات، كما أشارت النتائج عن الفائدة المتوقعة من استخدام تقنيات الذكاء الاصطناعي في الهيئة الوطنية للأمن السيبراني من وجهة نظر المبحوثين، والتي جاء في مقدمتها الاسهام في التخطيط الأمني على كافة أنحاء المملكة.

كلمات مفتاحية: تقنيات الذكاء الاصطناعي – الهيئة الوطنية للأمن السيبراني – الأمن السيبراني

The effectiveness of the use of artificial intelligence technologies by the National Authority for Cybersecurity in the Kingdom of Saudi Arabia as a future direction: a prospective study

Prof. Doaa Fathi Salim & Dr. Mohammad Hatim Abuljadail

Abstract:

The current century is characterized by the emergence of artificial intelligence technologies (artificial tourism intelligence) and its

applications in the security field in all elements of the security system, as these technologies have become an important role at the international and global level in the cybersecurity industry and contribute significantly to the global economy, which requires full preparation for the development of all parties to the security industry. , in order to consolidate the position of the Kingdom of Saudi Arabia as a global logistics center, and the study relied in its main construction on the theory of the spread of technological innovations, and this study is considered an exploratory study, as it was applied to a simple random sample of (106) single officials (workers) in the National Security Authority cyber, With years of experience and different ages, to monitor the expected impacts of the Authority's effective use of artificial intelligence technologies as a future direction, while clarifying the expected benefit of using artificial intelligence techniques in the field of cybersecurity, and revealing the reality of employing artificial intelligence as a mechanism for protecting information and data of the Kingdom, and showing the importance of this study Through the utmost importance that the National Authority for Cybersecurity enjoys in light of the Kingdom's Vision 2030 within its main axes, and the importance is also shown through the important role that artificial intelligence technologies can play in serving the security sector from several angles, The study indicated many results, the most important of which is the existence of a statistically significant relationship between the expected benefit of using artificial intelligence techniques in the National Authority for Cybersecurity, and the degree of success of this use. The results also showed a statistically significant relationship between the respondents' awareness of the role of artificial intelligence techniques in combating crimes. And between their attitudes towards its role in supporting and enhancing cybersecurity, and the fields of employing artificial intelligence techniques in the National Cybersecurity Authority, according to what the officials of the authority answered the study sample, The first of these areas was network security, and the results indicated the expected benefit of using artificial intelligence techniques in the National Authority for Cybersecurity from the respondents' point of view, foremost of which came the contribution to security planning throughout the Kingdom.

Key words: Artificial Intelligence Technologies - National Authority for Cyber Security- Cyber security

- **مقدمة:**

تسعي المملكة العربية السعودية لتحقيق رؤية ٢٠٣٠ في التحول الرقمي والأمن السيبراني لبداية عصر جديد يتزايد ويتنوع فيه الاقتصاد، الذي يعتمد على الاستفادة من الخدمات الرقمية والمعلوماتية، ومع تزايد الهجمات

الهائلة على المعلومات والبيانات الرقمية التي يصعب على أعضاء فرق الأمن السيبراني ملاحقتها بالدقة المتناهية المطلوبة، كان من الضروري استخدام تقنيات الذكاء الاصطناعي وقدراته في تحليل كميات هائلة من البياناتٍ والمعلومات لتسريع وتيرة الاستجابة وزيادة عمليات الأمن السيبراني وايضا قدرته على التصدي لتلك التهديدات لما تتميز به تلك التقنيات من سرعة هائلة وقدرة فائقة على مراقبة البيانات والكشف عن القيم المتطرفة التي تشير إلى احتمال وجود اختراقات معلوماتية، مما جعل الذكاء الاصطناعي حليفا لبرامج الأمن السيبراني.

وتعتبر تقنيات الذكاء الاصطناعي من أبرز التطورات التكنولوجية التي ظهرت في الآونة الأخيرة، ولهذه التقنية المتطورة كثير من الاستخدامات المختلفة في القطاعات والشركات والمجالات المتنوعة، وحديثا تم استخدام هذه التقنية وتطبيقها في مجالات العلوم المتطورة والحديثة، مثل مجال الأمن السيبراني وأمن المعلومات، والهجمات والاختراقات الكبيرة في مجال الحماية السيبرانية على الانترنت، الأمر الذي هدد الكثير من المستخدمين والصناعات والأعمال على الانترنت، والحماية السيبرانية بشكل يحمي البشر ويتخذ القرارات التي تفوق قرارات البشر في دقتها وصحتها، ومن هنا فرضت تقنيات الذكاء الاصطناعي واقعا جديدا على الدول بصفة عامة، حيث سعتٍ إلى تطبيق هذه التقنيات تماشيا مع المستحدثات التكنولوجية، وتعزيزا لدورها الحيوي في المنافسة مع بعضها البعض، والتي أدت إلى اتجاه نسبة كبيرة من الأنشطة الخاصة بالدول نحو الاعتماد عليها في العديد من الأمور المهمة، بل وتقديم فرص فريدة لقياس التصور العام للأشخاص والأفكار المختلفة، حيث يتضمن ذلك الوصول الفعال إلى مشاعرهم نحو ما يقومون بمتابعته، وردود الفعل التي يقدمونها للكشف عن الرؤى الذكية، كما أن قوة الذكاء الاصطناعي هائلة على الأمن السيبراني، حيث يوجه هذا الذكاءٍ التحليلات الاجتماعية السريعة والآلية والدقيقة التي تستخلص حلولا مبتكرة وتخطيطا أفضل ومشاركة أسرع للمعرفة، خاصة في ظل ما يسمى بالثورة الصناعية الرابعة والتي من المتوقع أن تتيح تقنيات جديدة للأمن السيبراني.

وتهدف الهيئة الوطنية للأمن السيبراني إلى تعزيز حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات، مراعية في ذلك الأهمية الحيوية المتزايدة للأمن السيبراني في حياة المجتمعات، ومستهدفة التأسيس لصناعة وطنيةٍ في مجال الأمن السيبراني تحقق للمملكة الريادة في هذا المجال انطلاقا مما تضمنته رؤية المملكة العربية السعودية ٢٠٣٠، وتتلخص الأهداف في تعزيز الأمن السيبراني للدولة، وحماية مصالح المملكة

الحيوية، وحماية أمن المملكة الوطني، وحماية البنى التحتية الحساسة في المملكة، وغيرها العديد من الأمور المهمة، وتشكل الهيئة الوطنية للأمن السيبراني الآن في ظل الرؤية المتطورة ٢٠٣٠ حلقة مهمة في تقييم تقنيات الذكاء الاصطناعي المستخدمة وقدرتها على محاكاة الذكاء البشرى في الأعمال الأمنية.

وبناء على ذلك جاءت الدراسة الحالية للتعرف على فاعلية استخدام الهيئة الوطنية للأمن السيبراني بالمملكة العربية السعودية لتقنيات الذكاء الاصطناعي كتوجه مستقبلي: دراسة استشرافية.

• مشكلة الدراسة:

في ظل تنامي هيمنة تقنيات الذكاء الاصطناعي، تتركز مشكلة الدراسة الحالية في استكشاف رؤى العاملين في الهيئة الوطنية للأمن السيبراني حول مدى فاعلية استخدام الهيئة الوطنية للأمن السيبراني بالمملكة العربية السعودية لتقنيات الذكاء الاصطناعي، في ظل ما أثارته حول تأثيراتها الإيجابية على مستقبل أمن السعودية، إضافة إلى تحديد العلاقة بين المنفعة المدركة وسهولة الاستخدام والنية السلوكية المتوقعة من استخدام هذه التقنيات وتقييمهم لها، ومقترحاتهم لتحقيق الاستخدام الأمثل لهذه التقنيات في الهيئة الوطنية للأمن السيبراني.

ومن هنا تتحدد المشكلة البحثية في قياس مدى فاعلية استخدام الهيئة الوطنية للأمن السيبراني بالمملكة العربية السعودية لتقنيات الذكاء الاصطناعي كتوجه مستقبلي: دراسة استشرافية.

• أهمية الدراسة:

شكلت ثورة الذكاء الاصطناعي تأثير أعمق في صناعة الاتصال والتفاعل من أي ثورات أخرى سابقة، ومن هنا تبرز أهمية دراسة التأثير المتوقع لتقنيات الذكاء الاصطناعي، ومدى تقبل الأفراد لهذه التقنيات المستحدثة وإدراكهم للاستفادة المتوقعة منها لاسيما في الأمن السيبراني، وكيف يمكنهم توظيفها في ضوء التغييرات المرتقبة التي ستطرأ على أمن المملكة العربية السعودية، ومن ثم تنبع أهمية هذه الدراسة وفقا لعدة جوانب:

• الأهمية العلمية:

- تناول الدراسة الحالية لتقنيات الذكاء الاصطناعي، والتي تمثل ذروة التطور التكنولوجي التي لاقت رواجاً في السنوات الأخيرة، إضافة إلى حداثة موضوع الدراسة الحالي، ونُدرة الدراسات العلمية العربية والسعودية الخاصة به، شكل ذلك دافعاً لاهتمام الفريق البحثي بدراسة فاعلية استخدام الهيئة الوطنية للأمن السيبراني بالمملكة العربية السعودية لتقنيات الذكاء الاصطناعي، وتحديد تأثيراتها على بنيتها

وطرق عملها، خاصة وأن معظم الدراسات أجنبية وتم تطبيقها في دول غربية.

- أهمية دراسة استخدام تقنيات الذكاء الاصطناعي في مجال الأمن السيبراني، حيث اقتصرت معظم الدراسات العربية الحالية على ضرورة توظيف مجال الأمن السيبراني لتلك التقنيات ولم يتم التوجه إلى قياس فاعلية استخدامها.

• الأهمية النظرية:

- تأتى هذه الدراسة في ظل حالة الجدل الذي صنعته تقنيات الذكاء الاصطناعي بين الأوساط المحلية والدولية وتأثيرها المستقبلي، في ظل ما أحدثته من ثورة تقنية في قدرة الوسائل المختلفة على التأثير ومخاطبة وجذب الجمهور نحو الأنشطة المختلفة، وإتاحتها لأدوات أكثر ذكاءً وتقدمًا وسرعة في نقل الأحداث والترويج لها وكذلك الخدمات إلى المتلقين، وتوفيرها لتقنيات أكثر تفاعلية وحرفية لتلبية احتياجاتهم المختلفة.

• الأهمية التطبيقية:

- لوحظ في الفترة الأخيرة قيام العديد من الهيئات السعودية بتطوير بنيتها الأساسية مما جعلها في مكانة متطورة، ولذا كان لابد من إلقاء الضوء على تلك التطورات للتعرف على مدى إفادتها من تقنيات الذكاء الاصطناعي المميزة في تطوير خدماتها.
- تكشف هذه الدراسة عن مدى فاعلية استخدام تقنيات الذكاء الاصطناعي في الهيئة الوطنية للأمن السيبراني، من وجهة نظر العاملين بالهيئة، وذلك في ظل تصوراتهم حول الجهد المتوقع والفائدة المرجوة والاستخدامات المتاحة، والتأثيرات الاجتماعية والنية السلوكية، وصولا إلى الوقوف على اتجاهاتهم نحو الملامح المستقبلية لاستخدام تقنيات الذكاء الاصطناعي من قبل الهيئة.
- التأثير الذي يمكن أن يحدثه استخدام هذه التقنيات في تطوير بيئة العمل في الهيئة الوطنية للأمن السيبراني.

• أهداف الدراسة:

تمثل الهدف الرئيس للدراسة في التعرف على مدى فاعلية استخدام الهيئة الوطنية للأمن السيبراني بالمملكة العربية السعودية لتقنيات الذكاء الاصطناعي كتوجه مستقبلي، وهناك العديد من الأهداف التي تسعى هذه الدراسة إلى تحقيقها، أبرزها:

- تحديد درجة معرفة المبحوثين بتقنيات الذكاء الاصطناعي، وإدراكهم لأهميتها وفاعليتها بالهيئة الوطنية للأمن السيبراني.

- التعرف على أهمية توظيف تقنيات الذكاء الاصطناعي في مجال الأمن السيبراني.
- الوقوف على مجالات استخدام تقنيات الذكاء الاصطناعي في مجال الأمن السيبراني.
- الكشف عن مدى تأثير استخدام تقنيات الذكاء الاصطناعي في الهيئة الوطنية للأمن السيبراني.
- تحديد درجة نجاح استخدام تقنيات الذكاء الاصطناعي في مجال الامن السيبراني
- توضيح الفائدة المتوقعة من استخدام تقنيات الذكاء الاصطناعي في مجال الامن السيبراني
- الكشف عن واقع توظيف الذكاء الاصطناعي كأليه لحماية المعلومات والبيانات الخاصة بالمملكة.
- استشراف مستقبل استخدام تقنيات الذكاء الصناعي في الهيئة الوطنية للأمن السيبراني وتأثيراتها الإيجابية المحتملة.

• الدراسات السابقة:

تم تناول الدراسات السابقة من خلال المحاور الآتية:

- المحور الأول: الدراسات التي تناولت استخدام تقنيات الذكاء الاصطناعي في المجالات المختلفة.
- المحور الثاني: الدراسات التي تناولت الذكاء الاصطناعي وعلاقته بالأمن السيبراني.

• أولا: الدراسات التي تناولت استخدام تقنيات الذكاء الاصطناعي في المجالات المختلفة.

تعمل تقنيات الذكاء الاصطناعي على تحسين أداء المؤسسات وإنتاجيتها عن طريق أتمتة العمليات أو المهام التي كانت تتطلب القوة البشرية فيما مضى، كما يمكن للذكاء الاصطناعي فهم البيانات على نطاق واسع لا يمكن لأي إنسان تحقيقه، وهذه القدرة يمكن أن تعود بمزايا كبيرة على الأعمال، وفى هذا نجد دراسة (ماجد الفتلاوى، حسن الأعسم، ٢٠٢٢) حول اسهامات تقنيات الذكاء الاصطناعي في الريادة الاستراتيجية، وتم إجراء الدراسة على مطار النجف الأشرف الدولي، وتوصلت إلى أن عمليات اتخاذ القرار في المطار تعتمد بالدرجة الأولى على عمليات استرجاع البيانات والمعلومات عبر قاعدة بيانات وأرشيف الكتروني وورقي لديها، ألا أنها ليست بالمستوى المطلوب بما يتناسب مع التحديات المتلاحقة، ولذا كانت من أهم توصيات الدراسة تبنى الأفكار والمقترحات الجديدة من خلال تشجيع روح الابتكارات لدى الموارد البشرية وتعزيز قدراتهم بذلك، وفى ذات الإطار كان استخدامها في المجال الإعلامي، حيث نجد دراسة (مي عبد الرازق، ٢٠٢٢) والتي تناولت استخدام

تقنيات الذكاء الاصطناعي في الإعلام، حيث سعت الدراسة إلى التعرف على اتجاهات القائمين بالاتصال نحو تبنى واستخدام تقنيات الذكاء الاصطناعي، وتأثير ذلك على واقع ممارستهم الإعلامية، وأشارت النتائج إلى اتفاق المبحوثين على قدرة تقنيات الذكاء الاصطناعي على محاكاة السلوك البشري في القيام بالعديد من المهام الإعلامية بإيجابية كبيرة، وجاء المجالات الأكثر استخداما في استخدام تقنيات الذكاء الاصطناعي مرتبة كالتالي المجال التسويقي، والمجال الإعلامي، ثم المجال الفني والإداري، وتمثلت أهم تقنيات الذكاء الاصطناعي من وجهة نظر المبحوثين في صحافة البيانات كتحويل النصوص لبيانات مختلف الأشكال، وتقنيات الترجمة الآلية للغات الأخرى، واستخدام الروبوتات في التحرير الصحفي وتقديم الأخبار واستخدام ال BOTS في الدردشة الآلية للرد على الاستفسارات وتعليقات الجمهور، وتمثلت أهم الموضوعات الأكثر توظيفا لتقنيات الذكاء الاصطناعي في أحوال الطقس وأسعار العملات والذهب، واتفقت معها دراسة (دعاء سالم، ٢٠٢١) والتي سعت إلى تحقيق هدف رئيس يتمثل في التعرف على فاعلية استخدام تقنيات الذكاء الاصطناعي في مواقع التواصل الاجتماعي من وجهة نظر طلاب الإعلام التربوي، والوقوف على مجالات استخدام تقنيات الذكاء الاصطناعي في مواقع التواصل الاجتماعي، إضافة إلى رصد التأثيرات الإيجابية والسلبية وأشكال القلق والتوتر من خلال استخدام تقنيات الذكاء الاصطناعي في مواقع التواصل الاجتماعي، وتوصلت الدراسة إلى عدة نتائج منها أن الطلاب أكدوا على معرفتهم بتقنيات الذكاء الاصطناعي المختلفة، كما أشارت نسبة كبيرة من المبحوثين إلى مدى اعتماد مواقع التواصل الاجتماعي على تقنيات الذكاء الاصطناعي، وجاء تحليل المشاعر الاجتماعية كنقطة أولى من حيث فاعلية استخدام تقنيات الذكاء الاصطناعي في مواقع التواصل الاجتماعي، كما جاء الاسهام في التخطيط للتأثير على النية السلوكية بشكل أفضل كفائدة متوقعة من استخدام تقنيات الذكاء الاصطناعي في مواقع التواصل الاجتماعي.

وكذلك اتفقت معها دراسة (Anja Bachmann, Geoffrey C Bowker, 2019) والتي أوضحت كيف أثر استخدام تقنيات الذكاء الاصطناعي على إنتاج المعرفة البشرية عبر وسائل التواصل الاجتماعي لاسيما Facebook، وذلك من خلال عمل نماذج للبيانات الضخمة كطريقة لتحويل البيانات إلى معرفة قيمية، من خلال خوارزميات معدة مسبقا ومصممة تصميما خاصا لحوكمة هذه البيانات، وعلى درجة عالية من الشفافية والاستقلالية والأتمتة، حتى يتم التمكن من فرزها، واستكمالا لدور الذكاء الاصطناعي في تحليل البيانات الضخمة جاءت دراسة (Vimala Nunavath; Morten Goodwin,2018) حول دور الذكاء الاصطناعي في وسائل التواصل الاجتماعي من خلال تحليلات البيانات الضخمة لإدارة الكوارث، فعند حدوث أي نوع من الكوارث، غالبًا ما ينشر الضحايا المتأثرون بشكل مباشر وغير مباشر

بالكارثة قدرًا هائلاً من البيانات (مثل الصور والنصوص والكلام والفيديو) باستخدام العديد من وسائل التواصل الاجتماعي، حيث أصبحت تلك الوسائل مؤخرًا قناة اتصال أساسية بين الناس لإبلاغ الجمهور أو موظفو الطوارئ بالكارثة، وفي غضون دقائق معدودة تغمر وسائل التواصل الاجتماعي بأنواع مختلفة من البيانات الضخمة، والتي قد تحتوى على محتوى متكرر وغير ذي صلة، ومن ثم يصبح من الصعب على موظفو الطوارئ فهم واتخاذ القرارات بشأن تلك البيانات المتاحة، وذلك على الرغم من التطورات الحديثة في تكنولوجيا البيانات، إلا أنه لا تزال معالجة وتحليل البيانات الضخمة لوسائل التواصل الاجتماعي المتعلقة بالكوارث مهمة صعبة، ومن ثم حاولت تلك الدراسة وضع آلية حول تطبيق الذكاء الاصطناعي لتحليل / معالجة البيانات الضخمة لوسائل التواصل الاجتماعي من أجل إدارة فعالة للكوارث، من خلال تصنيف النصوص والصور والفيديوهات الحقيقية المتعلقة بالكارثة، واتفقت معها دراسة (Purva Grover, Arpan Kumar Kar & Yogesh K. Dwivedi/ Annals,2020) حيث أشارت أن البيانات الضخمة هي النفط الجديد والذكاء الاصطناعي هو أداة التعامل مع تلك البيانات، وركزت الدراسة على التنقيب على البيانات التي تظهر عبر twitter، والتي تشمل الآثار الناتجة عن تلك البيانات، والعوامل الاجتماعية لذلك.

وفى إطار استخدام تقنيات الذكاء الاصطناعي في المجال الصحي كانت دراسة (Muhammad Imran,2018) Luis Fernandez-) فقد اتجهت إلى إنشاء نموذج جديد للمعلومات الموضوعية والمعلومات المضللة الخاصة بالأزمات الصحية، لاسيما بعد ظهور تقنيات Web 2.0 ومنصات الوسائط الاجتماعية مثل Twitter وذلك باستخدام الذكاء الاصطناعي، حيث تم تصميم استراتيجية البحث الخاصة للحصول على نظرة عامة واسعة على التطبيقات المختلفة للذكاء الاصطناعي في الأزمات الصحية والتحديات التي تواجهها من خلال دراسة الجدوى ونشر التكنولوجيا غير المناسب للعديد من سياقات الأزمات الصحية، وتحليل العديد من التغريدات، الأمر الذى سيؤدى إلى اتخاذ قرارات سريعة نحو إنشاء نموذج لبيان صحة أو تضليل المعلومات حول الأزمات الصحية، واستكمالا لدور الذكاء الاصطناعي في تحليل المعلومات وبيان الأدق منها كانت دراسة Amir Hussain, Aziz (Sheikh,2021) حول المعلومات المنتشرة عبر وسائل التواصل الاجتماعي عن لقاح كورونا covid-19، ومحاولة معالجة مخاوف المتشككين في اللقاح عن طريق الذكاء الاصطناعي الذى يمكن من الوصول الفعلي إلى الأشخاص المتشككين في اللقاح من خلال تحليل مشاعرهم المتغيرة وتطوير استراتيجيات للاتصال ثنائي الاتجاه عبر المنصات الاجتماعية.

أما عن استخدام تقنيات الذكاء الاصطناعي في مجال حماية الأنظمة ضد الهجمات الإلكترونية والتنمر الإلكتروني، فكانت دراسة Bhavani (Thuraisingham,2020)، والتي هدفت إلى التعرف على دور كل من

الذكاء الاصطناعي والأمن السيبراني في حماية أنظمة وسائل التواصل الاجتماعي من الهجمات الإلكترونية على أنظمة المعلومات، وانتهاك خصوصية الأفراد، ومشاركة المعلومات الخاطئة المعروفة باسم fake news، والأخبار التي تحتوي على الاتجار بالأطفال والعنف ضد المرأة، وركزت الدراسة على Facebook وTwitter اللذان يلعبان دورا رئيسا في المجتمع من خلال تمكين الأشخاص من التواصل وتبادل المعلومات، واتفقت معها دراسة (AltunbeyOzbay,BilalAlatas,2020) Feyza والتي حاولت الكشف عن الأخبار المزيفة بوسائل التواصل الاجتماعي باستخدام خوارزميات الذكاء الاصطناعي، وذلك بعدما ازداد انتشار تلك الأخبار على نطاق واسع، وتفاقمت المشكلة لمحاولة تحديد الفرق بين الأخبار الحقيقية والمزيفة، وتم اقتراح خطوتين لتحديد الأخبار المزيفة على وسائل التواصل الاجتماعي، تمثلت الخطوة الأولى في تطبيق المعالجة المسبقة على مجموعة البيانات المدخلة من قبل مستخدمي وسائل التواصل الاجتماعي، من أجل تحويل البيانات غير المنظمة إلى بيانات منظمة، أما الخطوة الثانية فتم تطبيق ٢٣ خوارزمية ذكاء اصطناعي على مجموعة البيانات المنظمة، باستخدام أساليب التنقيب عن النص، ومن ثم مقارنة البيانات قبل وبعد المعالجة.

واتفقت معها دراسة (F.A.H. Ambreen, Varsha D. Jadhav,2020) والتي أشارت إلى أنه لابد من وضع نموذج فعال للتصدي لخطر التنمر الإلكتروني على الشبكات الاجتماعية، والذى يشمل المضايقة أو الإهانة لأي فرد أو جماهير عن طريق إرسال أو نشر رسائل تؤذي المشاعر أو تهددهم مما يتسبب في تهديد كبير للصحة الجسدية والعقلية للضحايا، ومن ثم توفير التدابير الوقائية لذلك، من خلال اقتراح نموذج يحدد مصطلحات التنمر عبر الإنترنت وتصنيف أنشطة التسلط في الشبكات الاجتماعية باستخدام خوارزمية التعلم الآلي، كما اتفقت معها دراسة (Rana Mohamed Eisa, Merna Labib; Amr ElMougy,2019) والتي هدفت إلى استخدام تقنيات التعلم الآلي لاكتشاف واستخراج السمات الأكثر تحديداً لكل حساب شخصي عبر منصتي Facebook وTwitter، والتي يتم استخدامها لبناء ملف تعريف سلوكي لكل مستخدم، والذي يمكن من خلاله الكشف عن الحالات الشاذة التي تسببها هجمات المتطفلين، والتي تتسبب في الحاق الضرر بالمستخدمين.

وعلى سبيل استخدام تقنيات الذكاء الاصطناعي في المجال الأمني فكانت دراسة (عمار البابلي، ٢٠٢٠) والتي تناولت توظيف تقنيات الذكاء الاصطناعي في العمل الأمني، ومعرفة أنواع تطبيقات، وأنظمة الذكاء الاصطناعي المستخدمة في عمليات التحقيق الجنائي، ولحل ألغاز القضايا الكبيرة والغامضة، وكذلك توظيفها في التعرف على الوجه والهوية الرقمية داخل الاستنتاجات والتحليل الأمني، المتصلة بمواقع التوصل الاجتماعي، بما يساعد

الأجهزة الأمنية في التعرف على الأشخاص المطلوبين وجمع معلومات عنهم، بغرض حفظ الأمن العام ومنع وقوع الجرائم، وتوصلت إلى اعتماد الذكاء الاصطناعي على قاعدة بيانات يزود بها على عكس الذكاء البشري الذي يكتشف تلك البيانات بنفسه، ويعتمد الذكاء الاصطناعي على أساليب عدة تختلف باختلاف الغاية من النظم الذكية، واتفقت معها دراسة (لخضر دولي، ونفيسة ناصري، ٢٠١٨) والتي تناولت دور الذكاء الاصطناعي في مواجهة الجرائم الإلكترونية، لاسيما الخاصة بالتحديات التي تواجهها الاقتصاديات العالمية، وتوضيح الاستراتيجيات الواجبة لحماية الشركات ومختلف شبكاتها من التهديدات الحقيقية لأمن المعلومات، وقد توصلت إلى ضرورة اتخاذ القرارات الدقيقة من قبل الخبراء وأصحاب المعرفة ودعم عمليات إدارة أمن المعلومات واكتشاف عمليات التلاعب والتجسس.

- **ثانيا: الدراسات التي تناولت الذكاء الاصطناعي وعلاقته بالأمن السيبراني.**

يُعدُّ الذكاء الاصطناعي أحد الأصول الحاسمة للمنظمات التي تستخدم الأتمتة من أجل زيادة إنتاجية عملياتها وفعَّاليتها، وَوَفقا للهيئة الوطنية للأمن السيبراني، فيعد الذكاء الاصطناعي أحد التطبيقات التي يتم استخدامها أكثر من أي تطبيق آخر، حيث يمكن أن يكون أداة قوية في الحماية من الهجمات السيبرانية.

وفى هذا تناولت دراسة (خليل سعيدي، مرزوق بن مهدى، ٢٠٢٢) تسليط الضوء على أهمية الذكاء الاصطناعي في تحقيق الامن السيبراني والحفاظ على البيانات والمعلومات المعرضة للاختراق، وكذلك تسليط الضوء على واقع الذكاء الاصطناعي في ظل البيئة الرقمية الجديدة، والتعرف على دور الذكاء الاصطناعي في تحقيق الامن السيبراني لدى مستخدمي مواقع التواصل الاجتماعي، وتوصلت الدراسة إلى وجوب التفكير في توظيف تقنيات الذكاء الاصطناعي لحماية خصوصيات الأفراد والمستخدمين عبر مختلف المنصات الرقمية وعلى صعيد جميع المجالات، في حين تناولت دراسة (جيهان الخضري، هدى سلامي، نعمة كليبي، ٢٠٢٠) العديد من الأهداف منها التعرف على مدى توفر الوعي لدى طلاب الجامعات السعودية بالأمن السيبراني، وأيضا التعرف على دور الذكاء الاصطناعي في الوقاية من الهجمات السيبرانية، وتمثلت نتائج البحث في زيادة الاهتمام بتوعية المؤسسات الجامعية السعودية بتطبيق معايير أمن المعلومات حتى يتسنى لها مواجهة أي هجوم أو دخول غير مصرح به على أنظمة المعلومات، وتنظيم دورات تدريبية للطلاب وأعضاء هيئة التدريس والإداريون لتدريبهم على تطبيق أمن المعلومات، وتنظيم دورات تدريبية للقيادات التربوية تنمى الاعتماد على الذكاء الاصطناعي في صنع القرار التعليمي، والعمل على توظيف الذكاء الاصطناعي في حل المشكلات ودعم اتخاذ القرار. وفى نفس الإطار تناولت دراسة (جعفر العدوان، ٢٠٢٢) استكشاف أبرز أدوار الأمن السيبراني المعتمد

على الذكاء الاصطناعي المنبثقة من أمن المعلومات والمرتبطة بمرحلة الوقاية ومرحلة الاكتشاف ومرحلة الاستجابة، كما هدفت إلى معرفة أبرز التحديات التي تواجه الأمن السيبراني المعتمد على الذكاء الاصطناعي، ولتحقيق أهداف الدراسة، تم تبني منهجية دراسة الحالة المعتمدة على التسلسل من الإطار العام، وهو أمن المعلومات، إلى الإطار الخاص، وهو الأمن السيبراني المعتمد على الذكاء الاصطناعي، وتوصلت الدراسة إلى وجود تسعة أدوار هامة للأمن السيبراني المعتمد على الذكاء الاصطناعي موزعة على المراحل الثلاث كما يلي: ثلاثة أدوار في مرحلة الوقاية وهي التقييم الآلي للثغرات الأمنية، والتوعية والتدريب، والمصادقة، ودوران في مرحلة الاكتشاف وهما اكتشاف التسلل والاختراقات الأمنية، واكتشاف رسائل التصيد الإلكترونية المزعجة ورسائل التصيد الاحتيالي، وأربعة أدوار في مرحلة الاستجابة وهي تحليل البرمجيات الضارة، وأتمتة المهام الروتينية، ونشر المصائد للإطاحة بالمهاجمين، وعزل الأصول الهامة، كذلك حددت الدراسة ثمانية عناصر تمثل أبرز التحديات التي تواجه الأمن السيبراني المعتمد على الذكاء الاصطناعي، وهي اللوائح والأنظمة، والثقة، والمساءلة، والخصوصية، والتحيز، ومجموعات البيانات التدريبية، والموارد البشرية، والتكاليف المالية، في حين تناولت دراسة (فاطمة أحمد، رحاب يوسف، وليد السيد،٢٠٢٢) التعرف على مفهوم كلا من الأمن السيبراني والنظافة الرقمية، ومعرفة الفرق بينهما، والوقوف على أهم الهجمات التي تعترض عملية الأمن السيبراني، وكذا المشكلات التي تواجه النظافة الرقمية، وخرجت بعدة نتائج أهمها أن النظافة الرقمية جزء من الأمن السيبراني، أنه يوجد علاقة فيما بين النظافة الرقمية والأمن السيبراني والذكاء الاصطناعي.

وقد هدفت دراسة (ليلي بن برغوث،٢٠٢٣) إلى كشف واقع الأمن السيبراني وخصوصية البيانات الرقمية الموجودة على قواعد البيانات والمواقع الإلكترونية في الجزائر، والتعرف على أهم التقنيات المستحدثة التي تستخدم في اختراق البيانات الرقمية، وتوصلت إلى الدور المهم التي يقوم به الذكاء الاصطناعي في التصدي للهجمات السيبرانية ودحض الجريمة الإلكترونية.

وجاءت دراسة (نانسي الدمرداش، ٢٠٢٢) في إطار تنمية مهارات الأمن السيبراني معتمدة على العناصر الافتراضية المدعومة بالذكاء الاصطناعي وأدوات إدارة المعرفة، وتم تقسيم عينة البحث إلى مجموعتين تجريبيتين من طلاب الجامعات المصرية، وتقديم العناصر الافتراضية المدعومة بالذكاء الاصطناعي بأداتين من أدوات إدارة المعرفة وهي (العصف الذهني، مجتمعات التعلم)، وعليه تم تصميم اختبار لقياس التحصيل المعرفي لمهارات الأمن السيبراني، وبطاقة ملاحظة لقياس مهارات الأمن السيبراني، ومقياس مهارات حل المشكلات، وأظهرت نتائج البحث أثر تفاعل العناصر الافتراضية المدعومة بالذكاء الاصطناعي وأدوات إدارة المعرفة على متغيرات البحث

بشكل عام، والعناصر الافتراضية المدعومة بالذكاء الاصطناعي مع أداة العصف الذهني على غالبية متغيرات البحث بوجه خاص، حيث أظهرت النتائج فروق دالة إحصائيا بين المجموعتين التجريبيتين (أ)، (ب) في القياس القبلي/ البعدي لاختبار التحصيل المعرفي، والذي يؤكد على أن الطلاب اكتسبوا المعلومات والمعارف باختلاف العناصر الافتراضية المدعومة بالذكاء الاصطناعي وأدوات إدارة المعرفة؛ ولكن بنسب متفاوتة أكثرها تأثيرا المجموعة التجريبية (ب) التي استخدمت العناصر الافتراضية المدعومة بالذكاء الاصطناعي وأداة مجتمع التعلم.

في حين تناولت دراسة (سوزي عبد العزيز، ٢٠٢٢) التعرف على تطور المجال السيبراني وتقنيات الذكاء الاصطناعي اللذان يمثلان موجات من استخدام التطور التكنولوجي في قضايا السياسة الدولية، وكشف النوع الجديد من التهديدات الأمنية التي أطلق عليها "التهديدات الهجين" وكذلك التعرف على طبيعة التهديدات الأمنية الجديدة وأثرها في العلاقات الدولية من خلال دراسة نموذجين لتلك التهديدات وهما السيبرانية والذكاء الاصطناعي، وخلصت الدراسة إلى أن تلك النماذج كان لها تأثير على مستوى التفاعلات ومستوى المفاهيم في حقل العلاقات الدولية من حيث تطور مفهوم القوة والأمن والحرب والصراع وأدواتهم.

وكشفت دراسة (مجدي الداغر،٢٠٢١) عن اتجاهات النخبة نحو توظيف الإعلام الأمني لتطبيقات الذكاء الاصطناعي في مكافحة الجرائم الالكترونية وانعكاساته على دعم وتعزيز الأمن السيبراني في مصر، وتم تطبيق الدراسة على عينة من النخبة المصرية (الإعلامية، الأمنية، الأكاديمية)، وقسمت الدراسة إلى عدة محاور، تناول الأول الذكاء الاصطناعي في الإنتاج الإعلامي. واستعرض الثاني مراحل تطبيق الذكاء الاصطناعي في مجال الاعلام، وكشف الثالث عن خصائص تطبيقات الذكاء الاصطناعي في الإنتاج الإعلامي، وأشار الرابع إلى مجالات تطبيق الذكاء الاصطناعي في الإعلام الأمني، وتحدث الخامس عن آليات توظيف الذكاء الاصطناعي في إنتاج المحتوي الإعلامي، وناقش السادس تطبيقات الذكاء الاصطناعي في مكافحة الجرائم الالكترونية، وأشارت نتائج إلى وجود فروق ذات دلالة إحصائية حول مقترحات توظيف تطبيقات الأعلام الأمني في مكافحة الجرائم الإلكترونية باختلاف متغير السن، وذلك لصالح كبار السن الذين يدركون أبعاد التطبيقات الحديثة في انتاج المحتوي الإعلامي والتي يرون فيها خطورة على الأمن من سوء الاستخدام.

تمثلت دراسة (عبد الله الزهراني، حسن الشهري، ٢٠٢٠) في تحديد استراتيجيات الأمن السيبراني في ضوء التقنيات والتحديات الحديثة، وتكونت

عينة الدراسة من منسوبي مركز بحوث الفضاء والمركز الوطني لتقنية أمن المعلومات بمدينة الملك عبد العزيز للعلوم والتقنية، وإدارة أمن المعلومات بهيئة الاتصالات وتقنية المعلومات، وأوضحت النتائج ضرورة تطوير وتأهيل الكفاءات البشرية المتخصصة في الأمن السيبراني والتي تعد من أهم التحديات.

- **التعليق على الدراسات السابقة:**

باستقراء الدراسات السابقة يمكن استخلاص العديد من المؤشرات المهمة وذلك على النحو التالي:

- تعتبر الدراسات الغربية في سياق تقنيات الذكاء الاصطناعي أكثر تنوعاً وثراءً على المستويين النظري والتطبيقي، مع تنوع المجتمعات الخاصة بتطبيقها، والتي اهتمت برصد ملامح توظيف هذه التقنيات في المجالات المختلفة، وكيفية أتمتة المعلومات والبيانات بها، لاسيما التأثيرات الناتجة من جراء هذا الاستخدام، في حين لا توجد (في حدود علم الباحثين) دراسة عربية/ سعودية تختص بفاعلية استخدام الهيئة الوطنية للأمن السيبراني بالمملكة العربية السعودية لتقنيات الذكاء الاصطناعي، مما يعطي الأهمية النسبية للدراسة الحالية.
- اعتمدت الدراسات السابقة على عدة مدخل نظرية لفهم تعامل الجمهور مع تقنيات الذكاء الاصطناعي ومدى تقبلهم لها كان أبرزها نموذج قبول التكنولوجيا، والنظرية الموحدة لقبول واستخدام التكنولوجيا، ونظرية السلوك المبرر، نظرية انتشار المبتكرات.
- أوضحت الدراسات السابقة أهمية تقنيات الذكاء الاصطناعي في التصدي لهجمات الأمن الإلكترونية والأخبار المزيفة، وأن نجاح شركات البث الرقمي لا يتم بدون فهم معرفتهم الدقيقة بقاعدة المشتركين لديهم وتركيزهم على الذكاء الاصطناعي في دراسة الملايين من التقييمات وعمليات البحث و "التشغيل" يومياً.
- هناك توجع عام لدي الدراسات بتوظيف تقنيات الذكاء الاصطناعي كابتكار له فوائد اقتصادية كبيرة بجميع المجالات.
- ركزت معظم الدراسات السابقة على تسليط الضوء على أهمية الذكاء الاصطناعي في تحقيق الأمن السيبراني والمهارات اللازم توافرها لتحقيق ذلك، كما ركزت على بعض أدوار التي تقوم بها تقنيات الذكاء الاصطناعي للحفاظ على الأمن السيبراني.

- **أوجه الاستفادة من الدراسات السابقة:**

يمكن رصد أوجه الاستفادة من الدراسات السابقة على النحو التالي:

- على المستوى المعرفي: ساعدت الباحثين على تحديد المشكلة البحثية ووضع تساؤلات الدراسة وصياغة الفروض العلمية بشكل أفضل وتحديد العينة، والمعاملات الإحصائية التي يمكن استخدامها في ثنايا الدراسة.

- على المستوى النظري: ساعدت على إثراء الإطار النظري وتوسيع معلومات الباحثين في تحديد الأهمية الخاصة بتقنيات الذكاء الاصطناعي في المجالات المختلفة، حيث قدمت تلك الدراسات نموذجاً معرفياً عن الذكاء الاصطناعي، وآخر عن تأثيرات التقنيات الحديثة في المسائل الأمنية، مما ساعد على إيضاح جوانب النظرية، وأهم المتغيرات التي يعتمد عليها الباحثون في اختباراتهم لفروض نظرية نشر الأفكار المستحدثة.
- على المستوى التطبيقي: استفاد الباحثين من طريقة تطبيق الدراسات السابقة على العينات المختلفة، والتوصل إلى نتائج مهمة يمكن الاسترشاد بها في دعم الجانب التطبيقي للدراسة الحالية، وسهولة إجراء المقارنات الخاصة بالفروق بين نتائج ما توصلت إليه الدراسات السابقة وما ستتوصل إليه الدراسة الحالية من نتائج وتوصيات مختلفة.

• الإطار النظري للدراسة:

يشمل الإطار النظري للدراسة ثلاثة عناصر والتي تتمثل في الآتي:

- الذكاء الاصطناعي (مفهومه – سماته – أنواعه – مجالاته)
- الهيئة الوطنية للأمن السيبراني بالمملكة العربية السعودية.
- نظرية نشر الأفكار المستحدثة.

• أولا: الذكاء الاصطناعي [مفهومه – سماته – أنواعه – مجالاته]

• مفهوم الذكاء الاصطناعي:

يُعتبر الذكاء الاصطناعي **Artificial Intelligence** إحدى الركائز الأساسية التي تقوم عليها صناعة التكنولوجيا في العصر الحالي، ويُمكن تعريف مصطلح الذكاء الاصطناعي - الذي يُشار له بالاختصار **AI** بأنه قدرة الآلات والحواسيب الرقميّة على القيام بمهام مُعينة تُحاكي وتُشابه تلك التي تقوم بها الكائنات الذكيّة، كالقدرة على التفكير أو التعلم من التجارب السابقة أو غيرها من العمليات الأخرى التي تتطلب عمليات ذهنية، كما يهدف الذكاء الاصطناعي إلى الوصول إلى أنظمة تتمتع بالذكاء وتتصرف على النحو الذي يتصرف به البشر من حيث التعلم والفهم، بحيث تُقدم تلك الأنظمة لمستخدميها خدمات مُختلفة من الإرشاد والتفاعل وغير ذلك.(Verma, M. ، 2019)

• سمات الذكاء الاصطناعي:

- الاستدلال: ويعد أحد عمليات الاستنتاج المنطقي، أي استخدام القواعد والحقائق وطرق البحث المختلفة والحدس للوصول إلى استنتاج معين، وذلك عن طريق القيام بالاستدلال من خلال مطابقة الصور والأصوات وغيرها، اعتماداً على بناء قاعدة من المعرفة من خلالها يتم اكتساب الحاسوب القدرة على الاستدلال ومن ثم الاستنتاج المنطقي وإصدار الأحكام.

- تمثيل المعرفة: تمتلك أنظمة الذكاء الاصطناعي قاعدة كبيرة من المعرفة تمكنها من الربط بين الحالات والنتائج، وتمتلك هذه الأنظمة القدرة على الفصل بين هذه القاعدة وبين نظم المعالجة التي تستخدم المعرفة وتعالجها وتفسرها، وبالتالي فإن تمثيل المعرفة يعتمد على قاعدة من البيانات والتفاصيل والحقائق الواسعة، ويعتمد أيضا على نظم المعالجة وكيفية التعامل مع هذه البيانات والمعلومات والاستفادة منها على أكمل وجه.
- القدرة على التعلم: تعتبر القدرة على التعلم أحد أهم سمات الذكاء الاصطناعي بالاعتماد على استراتيجيات تعلم الآلة، حيث إنه بتحليل البيانات والمعلومات واستبعاد المعلومات غير المناسبة، وتصنيف المعلومات والاستفادة منها والتنبؤ، وأيضا تخزين هذه المعلومات للاستفادة منها في مواقف أخرى.
- البيانات المتضاربة (غير المؤكدة): حيث تمتلك أنظمة الذكاء الاصطناعي القدرة على التعامل مع البيانات المتضاربة أو المتناقضة أو التي تشوبها بعض الأخطاء وإعطاء الحلول المناسبة، كما تتمثل هذه السمة في قدرة الحواسيب الذكية على التوصل لحل المشكلات حتى في حالة عدم توفر جميع البيانات والمعلومات اللازمة لاتخاذ القرارات. (نيفين فؤاد،٢٠١٢)

- **أنواع الذكاء الاصطناعي:**

يُمكن تصنيف الذكاء الاصطناعي تِبعاً لما يتمتع به من قدرات إلى ثلاثة أنواع مُختلفة على النحو الآتي:

- الذكاء الاصطناعي المحدود أو الضيق: يُعتبر الذكاء الاصطناعي المحدود أو الضيق Weak AI or Narrow AI أحد أنواع الذكاء الاصطناعي التي تستطيع القيام بمهام مُحددة وواضحة، كالسيارات ذاتيّة القيادة، أو حتى برامج التعرُف على الكلام أو الصور، أو لعبة الشطرنج الموجودة على الأجهزة الذكية، ويُعتبر هذا النوع من الذكاء الاصطناعي أكثر الأنواع شيوعا وتوفرا في وقتنا الحالي.
- الذكاء الاصطناعي العام: General AI وهو النوع الذي يُمكن أن يَعمل بقدرة تُشابه قدرة الإنسان من حيث التفكير، إذ يُركز على جعل الآلة قادرة على التفكير والتخطيط من تلقاء نفسها وبشكل مُشابه للتفكير البشري، إلا أنه لا يوجد أيّ أمثلة عمليّة على هذا النوع، فكل ما يوجد حتى الآن مُجرد دراسات بحثيّة تحتاج للكثير من الجهد لتطويرها وتحويلها إلى واقع، وتعد طريقة الشبكة العصبيّة الاصطناعيّة Artificial Neural Network من طرق دراسة الذكاء الاصطناعي العام، إذ تُعنى بإنتاج نظام شبكات عصبيّة للآلة مُشابهة لتلك التي يحتويها الجسم البشري.
- الذكاء الاصطناعي الفائق يُعتبر الذكاء الاصطناعي الفائق Super AI النوع الذي قد يفوق مستوى ذكاء البشر، والذي يستطيع القيام بالمهام

بشكل أفضل مما يقوم به الإنسان المُتخصص وذو المعرفة، ولهذا النوع العديد من الخصائص التي لا بد أن يتضمنها؛ كالقدرة على التعلم، والتخطيط، والتواصل التلقائي، وإصدار الأحكام، إلا أن مفهوم الذكاء الاصطناعي الفائق يُعتبر مفهوما افتراضيا ليس له أي وجود في عصرنا الحالي.(Types of Artificial Intelligence، 2019)

ويُمكن أيضا تصنيف الذكاء الاصطناعي تبعا للوظائف التي يقوم بها، إذ يضُم هذا التصنيف أربعة أنواع مُختلفة كالآتي:

- الآلات التفاعليّة يُعتبر الذكاء الاصطناعي الخاص بالآلات التفاعليّة Reactive Machines أبسط أنواع الذكاء الاصطناعي؛ إذ يفتقر هذا النوع إلى القدرة على التعلم من الخبرات السابقة أو التجارب الماضيّة لتطوير الأعمال المستقبليّة، فهو يتفاعل مع التجارب الحاليّة لإخراجها بأفضل شكل مُمكن، ومن الأمثلة على هذا النوع من الذكاء الاصطناعي أجهزة Deep Blue التي تم تطويرها من شركة IBM، ونظام AlphaGo التابع لشركة جوجل.
- الذاكرة المحدودة يستطيع نوع الذكاء الاصطناعي ذو الذاكرة المحدودة Limited Memory تخزين بيانات التجارب السابقة لفترة زمنيّة محدودة، ويُعد نظام القيادة الذاتيّة من أفضل الأمثلة على هذا النوع؛ حيث يتم تخزين السرعة الأخيرة للسيارات الأخرى، ومقدار بعد السيارة عن السيارات الأخرى، والحد الأقصى للسرعة، وغيرها من البيانات الأخرى اللازمة للقيادة عبر الطرق.
- نظريّة العقل Theory of Mind يُعنى هذا النوع من الذكاء الاصطناعي بفهم الآلة للمشاعر الإنسانيّة، والتفاعل مع الأشخاص والتواصل معهم، ومن الجدير بالذكر أنه لا يوجد أيّة تطبيقات عمليّة حاليا على هذا النوع من الذكاء الاصطناعي.
- الإدراك الذّاتي: يُعتبر نوع الإدراك الذاتي Self-Awareness من التوقعات المستقبلية التي يصبو إليها علم الذكاء الاصطناعي، بحيث يتكون لدى الآلات وعي ذاتي ومشاعر خاصة، الأمر الذي سيجعلها أكثر ذكاءً من الكائن البشري، ولا يزال هذا المفهوم غير موجود على أرض الواقع.

• مجالات الذكاء الاصطناعي:

يشتمل الذكاء الاصطناعي على مجموعة واسعة من المجالات الفرعية، وفيما يلي عرض لعدد من المجالات العامة للذكاء الاصطناعي:

- تعلم الآلة Machine Learning يشير إلى مجال فرعي من الذكاء الاصطناعي يمكن فيها للبرمجية أن تتعلم أو تتكيف على غرار ما يمكن للبشر القيام به، وبصفة عامة يقوم تعلم الآلة بتحليل كميات هائلة من البيانات والبحث عن أنماط سائدة من أجل تصنيف المعلومات أو القيام بالتبوء والخروج بتوقعات. (سارة آل سعود، ٢٠١٧)

- التعلم العميق Deep Learning يقوم على أساس تطوير خوارزميات تُمكن الحاسوب من تعلم أداء المهام الصعبة التي تتطلب فهما عميقا للبيانات وطبيعة عملها من تلقاء نفسه، ويعتمد بشكل أساسي تفسير هذه البيانات على استخدام الشبكات العصبية الاصطناعية، والتي تتزايد مع مرور الوقت، وعلى مستويات متعددة من المعالجة غير الخطية للبيانات، وهذا ما يفسر قوة التعلم العميق. (Shi Dong, Ping Wang, Khushboo Abbas, 2021)
- الرؤية الحاسوبية Computer Vision يشير ذلك إلى إحدى المجالات العلمية للتخصصات التي تتناول كيفية جعل الحواسيب تكتسب مستويات عالية من الفهم خلال الصور أو الفيديوهات الرقمية، أي فهم الحواسيب لمحتوى هذه الصور ومواد الفيديو كما يفهمها الإنسان، وذلك بغرض إنتاج معلومات رقمية أو رمزية في شكل قرارات.
- معالجة اللغة الطبيعية Natural Language Processing تعتبر معالجة اللغة الطبيعية من العناصر الحاسمة والتي لا غنى عنها للذكاء الاصطناعي لأنها لا تهتم بالتفاعلات بين الحواسيب واللغات البشرية، خاصة فيما يتعلق بكيفية برمجة الحاسوب لمعالجة بيانات اللغة الطبيعية وتحليلها. (Ling Jin,2019)
- التفاعُل مع الكتابة اليدويّة Interact with handwriting وذلك من خلال تطبيقات التعرف إلى الخط المكتوب باليد سواءً كانت عمليّة الكتابة على الورق أو على شاشة الجهاز نفسه.
- الروبوتات الذكيّة smart robots تقوم الروبوتات بالكثير من الأعمال المختلفة، إذ تستطيع القيام بالأعمال التي يقوم بها البشر، وذلك لقدرتها على الإحساس بالعوامل المحيطة كالضوء، والحرارة، والصوت، أو الحركة، وذلك عبر مُستشعرات خاصة، كما أن هذه الروبوتات قادرة على التعلم من تجاربها السابقة والاستفادة من الأخطاء.
- التفاعُل مع الصوت المنطوق Interact with spoken audio إذ يُمكن استخدام بعض أنظمة الذكاء الاصطناعي للاستماع إلى الكلام وفهم معانيه، حتى لو تم النُطق به في ظل وجود بعض الضوضاء أو تم نطقه باللهجة العامية أو لغة الشارع.(Katharine Gammon,2019)

• ثانيا: الهيئة الوطنية للأمن السيبراني بالمملكة العربية السعودية.

انطلاقا من إدراك المملكة العربية السعودية لمتغيرات العصر من استقبال ثورة صناعية رابعة تقوم على تقنيات تتسم بالنمو المتسارع في قدرات المعالجة الحاسوبية وقدرات التخزين الهائلة للبيانات وتبادلها، والاستعداد للتعامل مع منتجات ومعطيات الذكاء الاصطناعي والروبوتات والأجهزة ذاتية التحكم، والتي تتطلب المواكبة الذكية، والتكييف وفق متطلبات الأمن السيبراني،

وترجمةً لنهج خادم الحرمين الشريفين الملك سلمان بن عبد العزيز وسمو ولي العهد حفظهم الله في قيادة المملكة لتكون نموذجًا ناجحًا ورائدًا في العالم على كافة الأصعدة، ولرؤية المملكة ٢٠٣٠ التي جعلت التحول نحو العالم الرقمي وتنمية البنية التحتية الرقمية ضمن مستهدفاتها، واستشعارا لأهمية البيانات والأنظمة التقنية والبنى التحتية الحساسة وارتباطها بالمصالح الوطنية، وأهمية حمايتها من أي تهديدات أو مخاطر يشهدها الفضاء السيبراني جاء تأسيس الهيئة الوطنية للأمن السيبراني وارتباطها بالملك -حفظه الله- وذلك وفق الأمر الملكي بالموافقة على تنظيمها بتاريخ ١٤٣٩/٢/١١ هـ لتكون هي الجهة المختصة في المملكة بالأمن السيبراني، والمرجع الوطني في شؤونه، والتي تهدف إلى تعزيزه، حماية للمصالح الحيوية للدولة وأمنها الوطني والبنى التحتية الحساسة والقطاعات ذات الأولوية والخدمات والأنشطة الحكومية، ولا يخلي ذلك أي جهة عامة أو خاصة أو غيرها من مسؤوليتها تجاه أمنها السيبراني بما لا يتعارض مع اختصاصات ومهمات الهيئة الواردة في تنظيمها.

وسيتم يتم التناول ذلك من حيث:

- اختصاصات ومهام الهيئة.
- الاستراتيجية الوطنية للأمن السيبراني.

- **اختصاصات ومهام الهيئة:(https://www.nca.gov.sa/about)**

- إعداد الاستراتيجية الوطنية للأمن السيبراني، والإشراف على تنفيذها، واقتراح تحديثها.
- وضع السياسات وآليات الحوكمة والأطر والمعايير والضوابط والإرشادات المتعلقة بالأمن السيبراني، وتعميمها على الجهات ذات العلاقة، ومتابعة الالتزام بها، وتحديثها.
- تصنيف وتحديد البنى التحتية الحساسة والجهات المرتبطة بها، وتحديد القطاعات والجهات ذات الأولوية بالأمن السيبراني.
- وضع أطر إدارة المخاطر المتعلقة بالأمن السيبراني، ومتابعة الالتزام بها، وتحديثها.
- إشعار الجهات المعنية بالمخاطر والتهديدات ذات العلاقة بالأمن السيبراني.
- وضع أطر الاستجابة للحوادث المتعلقة بالأمن السيبراني، ومتابعة الالتزام بها، وتحديثها.
- بناء مراكز العمليات الوطنية الخاصة بالأمن السيبراني – وما في حكمها – بكافة أنواعها، بما في ذلك مراكز التحكم والسيطرة والاستطلاع والرصد وتبادل وتحليل المعلومات، وكذلك بناء مراكز العمليات القطاعية الخاصة بالأمن السيبراني – عند الحاجة -، وبناء المنصات ذات العلاقة، والإشراف عليها، وتشغيلها.

- القيام – بنفسها أو من خلال غيرها – بالأنشطة والعمليات المتعلقة بالأمن السيبراني.
- تنظيم آلية مشاركة المعلومات والبيانات المرتبطة بالأمن السيبراني بين الجهات والقطاعات المختلفة في المملكة، والإشراف على ذلك.
- تقديم المساندة للجهات المختصة – في حال طلبها وفقا للإمكانيات المتاحة لدى الهيئة- خلال الاستدلال والتحقيق في الجرائم المتعلقة بالأمن السيبراني.
- وضع السياسات والمعايير الوطنية للتشفير، ومتابعة الالتزام بها، وتحديثها.
- وضع ما يلزم من معايير أو ضوابط للفسح والترخيص باستيراد وتصدير واستخدام الأجهزة والبرمجيات ذات الحساسية العالية للأمن السيبراني التي تحددها الهيئة، ومتابعة الالتزام بها، وتحديثها، وذلك دون إخلال بأي معايير أو ضوابط معتمدة لدى الجهات الأخرى ذات العلاقة.
- بناء القدرات الوطنية المتخصصة في مجالات الأمن السيبراني، والمشاركة في إعداد البرامج التعليمية والتدريبية الخاصة بها، وإعداد المعايير المهنية والأطر وبناء وتنفيذ المقاييس والاختبارات القياسية المهنية ذات العلاقة.
- الترخيص بمزاولة الأفراد والجهات غير الحكومية للأنشطة والعمليات المتعلقة بالأمن السيبراني التي تحددها الهيئة.
- التواصل مع الجهات المماثلة خارج المملكة والجهات الخاصة لتبادل الخبرات، وتأسيس آليات للتعاون والشراكة معها، وفقا للإجراءات المتبعة.
- تبادل الإنتاج التقني والمعرفي وتبادل البيانات والمعلومات مع الجهات المماثلة خارج المملكة.
- تمثيل المملكة في المنظمات والهيئات واللجان والمجموعات الثنائية والإقليمية والدولية ذات الصلة، ومتابعة تنفيذ التزامات المملكة الدولية الخاصة بالأمن السيبراني.
- رفع مستوى الوعي بالأمن السيبراني.
- تحفيز نمو قطاع الأمن السيبراني في المملكة، وتشجيع الابتكار والاستثمار فيه.
- إجراء الدراسات والبحوث والتطوير وعمليات التصنيع، ونقل التقنية وتطويرها في الأمن السيبراني وما يرتبط به من مجالات.
- اقتراح آليات رفع كفاءة الإنفاق في مجالات الأمن السيبراني.
- تطوير مؤشرات قياس الأداء الخاصة بالأمن السيبراني، وإعداد التقارير الدورية حول حالة الأمن السيبراني في المملكة على المستويين الوطني والقطاعي.
- اقتراح إصدار وتعديل الأنظمة واللوائح والقرارات ذات الصلة بالأمن السيبراني.

- **الاستراتيجية الوطنية للأمن السيبراني:**

تم وضع رؤية للاستراتيجية الوطنية للأمن السيبراني تعكس الطموح الاستراتيجي للمملكة وبأسلوب متوازن بين الأمان والثقة والنمو، وتتضمن الرؤية التي تسعى الهيئة إلى الوصول لها (فضاء سيبراني سعودي آمن وموثوق يمكن النمو والازدهار)

تلبي هذه الرؤية أولويات المملكة وتطلعاتها، وتؤكد على تعزيز حماية الأنظمة التقنية والتشغيلية والبنى التحتية الحساسة والقدرة على الصمود والتصدي للحوادث السيبرانية وامتصاص الأضرار والتعافي منها في الوقت المناسب، بالإضافة إلى تعزيز ثقة الجهات الوطنية والمستثمرين والأفراد في الفضاء السيبراني السعودي، وكذلك المساهمة في النمو الاقتصادي والاجتماعي للمملكة.

- **المصطلحات التي تتضمنها الرؤية الاستراتيجية:**
  - فضاء سيبراني: يشمل الفضاء السيبراني السعودي بأكمله
  - سعودي: لتلبية أولويات المملكة وتطلعاتها
  - آمن: التأكيد على حماية وصمود الأنظمة التقنية والتشغيلية والبنى التحتية الحساسة
  - موثوق: يعزز ثقة الجهات الوطنية والمستثمرين والأفراد في الفضاء السيبراني السعودي
  - يمكن النمو والازدهار: إسهام حماية الفضاء السيبراني في النمو الاقتصادي والاجتماعي للمملكة

وقد حرصت الهيئة على تصميم إطار مرجعي للأمن السيبراني خاص بالمملكة مبني على أفضل الممارسات المحلية والعالمية وأهم المستجدات والتحديات التي تواجه الأمن السيبراني، بحيث يعد نموذجًا متقدمًا يشمل الجوانب المختلفة للأمن السيبراني على مستوى الدول. ويحتوي هذا الإطار على ستة محاور تتضمن ثمانية عشر عنصرًا رئيسا من عناصر الأمن السيبراني، ويساعد هذا الإطار على تعميق الفهم لفضاء المملكة السيبراني، وتم استخدام هذا الإطار لتصميم الاستراتيجية على المستوى الوطني.

وتعرف المحاور الستة الرئيسة لهذا الإطار كما يلي:

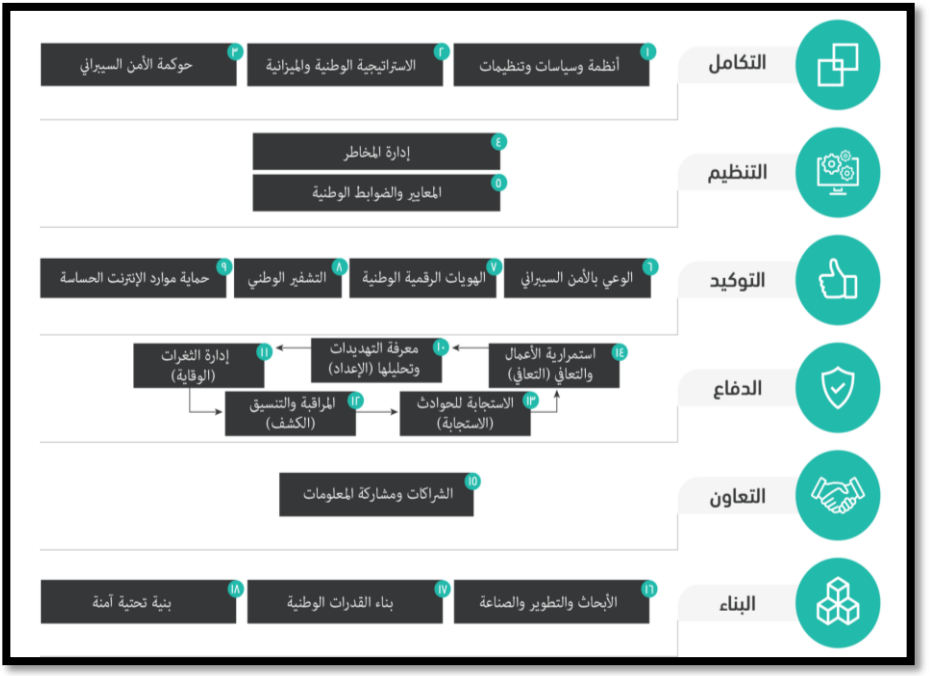
- **محور التكامل:**

يعنى هذا المحور بتكامل جميع مكونات منظومة الأمن السيبراني، ويحتوي على ثلاثة عناصر هي:

- أنظمة وسياسات وتنظيمات: الأطر والآليات اللازمة لإدارة التوجهات الاستراتيجية بالشكل المطلوب، وذلك من خلال الصلاحيات والسياسات والأنظمة والتشريعات اللازمة.
- الاستراتيجية الوطنية والميزانية: تطوير ومراجعة التوجهات الاستراتيجية الوطنية للأمن السيبراني، من خلال العمل على

إعداد ومراجعة النطاق والأهداف والمبادرات والميزانيات المتوقعة ومؤشرات الأداء لقياس مدى الالتزام بالخطة التنفيذية.

- حوكمة وإدارة الأمن السيبراني: إعداد إطار حوكمة يوضح الأدوار والمسؤوليات والصلاحيات للجهات والأفراد المعنين.



شكل (١) يوضح الإطار المرجعي للأمن السيبراني الخاص بالمملكة

- **محور التنظيم:**

يعنى هذا المحور بتحديد البنى التحتية الحساسة وإدارة المخاطر السيبرانية، ويحتوي على عنصرين:

- إدارة المخاطر السيبرانية: تقليل المخاطر من التهديدات والثغرات، عن طريق تنفيذ عمليات إدارة المخاطر التي تبدأ بتحديد البنى التحتية الحساسة، وتعريف المخاطر وتقييمها والعمل على تقليلها، انتهاءً بمراقبة المخاطر ورصدها للمساهمة بتعزيز الصمود السيبراني.
- المعايير والضوابط الوطنية: توفير نموذج مرجعي للمعايير الوطنية والضوابط السيبرانية، بحيث تعمل على تحديد نطاق الضوابط الأساسية والفرعية، ونوعيتها ومدى شموليتها وكيفية العمل على تنفيذها مع مختلف القطاعات والجهات ذات العلاقة، ووضع الآليات اللازمة للتأكد من التزام الجهات بهذه الضوابط.

- **محور التوكيد:**

يعنى هذا المحور بالتأكد من حماية الفضاء السيبراني، ويحتوي على أربعة عناصر هي:

- الوعي بالأمن السيبراني: التوعية في المجال السيبراني على المستوى الوطني عن طريق حملات التوعية والتدريب؛ مما يساهم في تحسين السلوك وتبني أفضل الممارسات وتطبيقها.
- الهويّات الرقمية الوطنية: تعزيز جوانب الأمن السيبراني في الهويات الرقمية على المستوى الوطني، مما يساهم في رفع مستوى موثوقية الهويات الرقمية في الفضاء السِيبراني للتجارة وتوفير الخدمات الحكومية وغيرها.
- التشفير الوطني: الالية الوطنية لتشفير البيانات وتشمل تطوير وتقييم أنظمة وخوارزميات ومعايير التشفير الوطنية.
- حماية موارد الإنترنت الحساسة: عن طريق تعزيز جوانب الأمن السيبراني لحماية موارد الإنترنت الحساسة وتعزيز اعتمادية الإنترنت من جوانب الأمن السيبراني.

- **محور الدفاع:**

يعنى هذا المحور بمواكبة آليات الدفاع الوطنية السيبرانية للمخاطر والتهديدات المتسارعة، ويحتوي على خمسة عناصر هي:

- معرفة التهديدات وتحليلها: رصد التهديدات السيبرانية ومشاركتها مع الجهات ذات العلاقة من القطاعين العام والخاص.
- إدارة الثغرات: تشمل العمل بشكل مشترك مع الأفراد والجهات ذات العلاقة؛ للبحث عن أي ثغرات يمكن استغلالها ومشاركة التوصيات مع الجهات المتأثرة لاتخاذ الإجراءات المناسبة.
- المراقبة والتنسيق: تعزيز مستوى الدراية الأمنية وتصنيف التهديدات واختبار خطط الاستجابة للحوادث على هجمات محددة ومن ثم احتواءها في حال حدوثها قبل أن تتسبب بأضرار كبيرة.
- الاستجابة للحوادث: آليات الاستجابة للحوادث واختبار خططها على هجمات محددة لخلق تحسينات مستمرة للتكيف مع التهديدات والمخاطر السيبرانية، ويتم تنسيق الأنشطة على المستوى الوطني لاحتواء الهجمات السيبرانية وتقليل أضرارها والحد من تكرارها.
- استمرارية الأعمال والتعافي: يشمل هذا العنصر التأكد من وجود خطط للطوارئ واختبار البنى التحتية الحساسة والخدمات الإلكترونية الهامة، وكذلك إجراءات محددة لاستعادة عملها بعد الحوادث السيبرانية، والعمل باستمرار على إجراء هذه الاختبارات للتحقق من سلامة البنى التحتية الحساسة والخدمات الهامة، وجاهزيتها مستقبلا.

• **محور التعاون:**

يعنى هذا المحور بوضع الآليات المناسبة لبناء الشراكات ومشاركة المعلومات، ويحتوي على:

- الشراكات ومشاركة المعلومات: يمكّن من وضع السياسات والآليات وأفضل الممارسات التي تتيح مشاركة المعلومات المتعلقة بالتهديدات السيبرانية مع الجهات الوطنية والدولية، وكذلك المساعدة في التنسيق والتعاون مما يسهم في رفع الجاهزية والاستعداد والوقاية وسرعة الاستجابة في حالة وقوع حادث سيبراني.

• **محور البناء:**

يعنى هذا المحور بالتأكد من وجود قاعدة وطنية متينة وآمنة، ويحتوي على ثلاثة عناصر كالتالي:

- الأبحاث والتطوير والصناعة: تشجيع الأبحاث في مجال الأمن السيبراني وفقاً لأولويات مشتركة على المستوى الوطني، ودعم الابتكار والاستثمار في مجال الأمن السيبراني لتحويل مخرجات الأبحاث والتطوير إلى منتجات وخدمات. كما يشمل تحفيز صناعة الأمن السيبراني لضمان بناء قدرات كافية.
- بناء القدرات الوطنية: يشمل هذا العنصر إعداد وتأهيل كوادر وطنية متخصصة في الأمن السيبراني وتطوير تلك الكوادر بالمحافظة عليها؛ وذلك لسد الاحتياج الوطني في هذا المجال من خلال برامج تعليم وتدريب عالية الجودة.
- بنية تحتية آمنة: العمل على تبني نهج استباقي لضمان أمن الأنظمة والأجهزة والخدمات عبر سلسلة التوريد بأكملها، بدءاً من التصميم حتى الإنتاج ومن ثم التشغيل وانتهاءً بالإتلاف، وتطوير آليات ومعايير للتقييم والاختبار والفسح لمعدات وبرامج وخدمات الأمن السيبراني؛ للتأكد من سلامتها واستعدادها. (https://www.nca.gov.sa/strategic)

• **ثالثا: نظرية نشر الأفكار المستحدثة Diffusion of Innovations theory**

تعد نظرية نشر الأفكار المستحدثة من النظريات التي وضعت لتفسير السلوك الإنساني للإقبال على تبني الأفكار أو استهلاك المنتجات الجديدة في المجتمعات الإنسانية، ووفقا لهذه النظرية فإن وجود مستحدثات جديدة يتم إدخالها إلى النظام الاجتماعي قد يكون لها قبول تدريجي مع مرور الوقت وفقا لمجموعة من المتغيرات التي تخص البيئة الاجتماعية التي يتم إدخال تلك المستحدثات إليها. (محمد العقاري، ٢٠١٩)

وقد عرف **Rogers** الانتشار بأنه العملية التي يتم من خلالها توصيل الابتكار عبر قنوات معينة مع مرور الوقت بين أعضاء النظام الاجتماعي،

والابتكار هو فكرة أو تقنية جديدة يتبناها المجتمع في ضوء بعض الخصائص المحددة لانتشاره بسرعه، كالميزة النسبية للابتكار، والتوافق مع التقاليد والقيم، والقابلية للتجريب ودرجة ظهور نتائج الابتكار للآخرين، واحتياجات المتبنين المحتملين. (بسام المشاقبة، ٢٠١٥)

وقد أكد الباحثون في هذا المجال على الأهمية الرئيسة للاتصال ولعنصر الوقت في عملية تبنى الابتكارات، ولذا صنف **Rogers** المتبنين للمستحدثات إلى المبتكرون – المتبنون الأوائل – الغالبية المبكرة – الغالبية المتأخرة – المتبنون الأواخر، ومن ثم يبدأ الابتكار بالاختراع والنشر عبر النظام الاجتماعي، إلى أن يصل إلى النهاية والتي إما أن تكون تبنياً أو رفضا، ويؤكد **Storsul & Krumsvik** أنه مع التقدم التكنولوجي أصبحت الحاجة ملحة للابتكار في صناعة الوسائل الإعلامية والاتصالية، والتي تتطلب بالضرورة إلى مهارات تقنية عالية.(**Celeste (Bishop Stein,2019**

- **تطبيق نظرية إنتشار المستحدثات أو المبتكرات على موضوع الدراسة:**

نجد أن عملية تبنى الأفكار هي العملية العقلية التي يمر خلالها الفرد من وقت سماعه أو علمه بالابتكار إلى أن ينتهي به الأمر إلى مرحلة التبني النهائية، ويمكن اختصار هذه المراحل في:

- المرحلة الأولي: مرحلة الوعي بالفكرة (Awareness stage) والتي قد تتم بشكل عفوي أو مقصود.
- المرحلة الثانية: مرحلة الاهتمام (Interest stage) وتكون هنا الرغبة في الحصول على مزيد من المعلومات حول الموضوع.
- المرحلة الثالثة: مرحلة التقييم (Evaluation stage) وهي مرحلة تقييم المعطيات وتقرير إذا كان هناك فائدة لإخضاع المسألة للتجريب العملي.
- المرحلة الرابعة: مرحلة التجريب (Trial stage) يجرب المبتكر على نطاق ضيق أو لفترة محددة.
- المرحلة الخامسة: مرحلة التبني (Adoption stage) إذا اقتنع الشخص بالموضوع فسيتبناه ويطبقه على نطاق واسع، وقد تطورت الهيئة الوطنية للأمن السيبراني منذ نشأتها إلى الآن، فلها العديد من المبادرات والإنجازات والبرامج مثل برنامج سايبرك، وكذلك العديد من البوابات مثل بوابة حصين، كما نلاحظ تطور تقنيات الذكاء الاصطناعي بسرعة كبيرة، بما يتناسب مع التقدم في مستوى حماية البنية التحتية لتكنولوجيا المعلومات للهيئة، فنجد أن الذكاء الاصطناعي سيعزز الحاجز الفاصل بين الأنظمة المختلفة والتهديدات الإلكترونية، وفقا لتقرير من شركة IBM ارتفع متوسط التكلفة الإجمالية لاختراق البيانات من ٣.٨٦ مليون دولار إلى ٤.٢٤ مليون دولار في عام ٢٠٢١م. وأصبح مجرمو الإنترنت أكثر

خبره وتقدمًا في هجماتهم مما أدى إلى هذا الارتفاع الكبير، بالإضافة إلى تركيز المجرمين على شن هجمات تصيد ضد العامل البشري للمنشأة والتي تسبب في ١٤٪ من الاختراقات الإلكترونية الناجحة في عام ٢٠٢١م. (https://maaal.com/archives/202008/152287/)

ودائما تبحث الهيئة عن طرق لحماية البيانات وأنظمة التكنولوجيا الخاصة بها، وللمؤسسات المختلفة بالمملكة مع التقدم في وسائل الهجمات الإلكترونية، وللقيام بذلك يجب عليها اعتماد نهج أكثر استباقية للتغلب على التهديدات، وبذلك يثبت الذكاء الاصطناعي (AI) قدراته، ويعنى ذلك أن الذكاء الاصطناعي هو التقدم في مجال الأمن السيبراني، وبالتالي ينطبق ذلك تماما مع نظرية انتشار المستحدثات.

ويمكن تطبيق النظرية على الدراسة الحالية من خلال قياس مدى فاعلية استخدام الهيئة الوطنية للأمن السيبراني بالمملكة العربية السعودية لتقنيات الذكاء الاصطناعي كتوجه مستقبلي، مع بيان تأثير هذه التقنيات، ومجالات استخدامها ودرجة نجاحها.

- **التعريفات الإجرائية للدراسة:**

١- الأمن السيبراني Cyber security

حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات، من أي اختراق، أو تعطيل، أو تعديل، أو دخول أو استخدام أو استغلال غير مشروع. كما يشمل هذا المفهوم أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحوها.

٢- تقنيات الذكاء الاصطناعي Artificial intelligence technologies

تقنيات تحاكي القدرات الذهنية البشرية على أداء المهام ويمكنها بشكل متكرر تحسين نفسها استنادًا إلى المعلومات التي تجمعها، مثل القدرة على التعلم والاستنتاج ورد الفعل على أوضاع لم تبرمج في الآلة.

٣- الهيئة الوطنية للأمن السيبراني National Cybersecurity Authority

هي الجهة المختصة في المملكة بالأمن السيبراني، وتعتبر المرجع الوطني في شؤونه، وتهدف إلى تعزيزه، حماية للمصالح الحيوية للدولة وأمنها الوطني والبنى التحتية الحساسة والقطاعات ذات الأولوية والخدمات والأنشطة الحكومية، وقد تم إنشاؤها عام ٢٠١٧م، وترتبط مباشرة بالملك سلمان بن عبدالعزيز آل سعود، وقد سجلت الهيئة أهم إنجازاتها في مارس ٢٠١٩م عندما صنف الاتحاد الدولي للاتصالات المملكة العربية السعودية في المرتبة ١٣ عالميا والأولى عربيًا من بين ١٧٥ دولة، من خلال المؤشر العالمي للأمن السيبراني GCI، الذي يتم قياسه بشكل دوري كل عامين بناء على خمس ركائز رئيسية، تتمثل في القانونية والتعاونية والتقنية والتنظيمية وبناء القدرات.

- **تساؤلات الدراسة:**

تجيب هذه الدراسة عن تساؤل رئيس يتعلق بمدى فاعلية استخدام الهيئة الوطنية للأمن السيبراني بالمملكة العربية السعودية لتقنيات الذكاء الاصطناعي كتوجه مستقبلي، ويتفرع عنه الأسئلة التالية:

- ما مدى اهتمام المبحوثين بتقنيات الذكاء الاصطناعي، وإدراكهم لأهميتها وفاعليتها بالهيئة الوطنية للأمن السيبراني؟
- إلى أي درجة كانت معرفة المبحوثين بتقنيات الذكاء الاصطناعي؟
- ما معدل تعرض المبحوثين لتقنيات الذكاء الاصطناعي؟
- ما الدوافع المؤدية لاعتماد المبحوثين على تقنيات الذكاء الاصطناعي مستقبلا؟
- ما مجالات توظيف تقنيات الذكاء الاصطناعي في الهيئة الوطنية للأمن السيبراني؟
- إلى أي مدى تتعدد أشكال الجرائم الإلكترونية(السيبرانية)؟
- ما مدى إدراك المبحوثين لدور تقنيات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية؟
- ما تأثير توظيف الهيئة الوطنية للأمن السيبراني لتقنيات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية؟
- ما اتجاهات المبحوثين نحو دور تقنيات الذكاء الاصطناعي في دعم وتعزيز الأمن السيبراني؟
- إلى أي مدى تكون درجة نجاح استخدام تقنيات الذكاء الاصطناعي في الهيئة الوطنية للأمن السيبراني؟
- ما أبرز أدوار الأمن السيبراني المعتمدة على تقنيات الذكاء الاصطناعي؟
- ما الفائدة المتوقعة من استخدام تقنيات الذكاء الاصطناعي في الهيئة الوطنية للأمن السيبراني؟
- ما مقترحات المبحوثين لتعزيز استخدام تقنيات الذكاء الاصطناعي بالهيئة الوطنية للأمن السيبراني؟
- ما مستقبل استخدام تقنيات الذكاء الصناعي في الهيئة الوطنية للأمن السيبراني وتأثيراتها المحتملة؟

- **فروض الدراسة:**

- الفرض الأول: توجد علاقة دالة إحصائيًا بين الفائدة المتوقعة من استخدام تقنيات الذكاء الاصطناعي في الهيئة الوطنية للأمن السيبراني وبين درجة نجاح هذا الاستخدام.
- الفرض الثاني: توجد فروق دالة إحصائيًا بين المبحوثين في مدى فاعلية توظيف تقنيات الذكاء الاصطناعي في الهيئة الوطنية للأمن السيبراني تبعا لخصائصهم الديموغرافية.

- الفرض الثالث: توجد علاقة دالة إحصائيًا بين مدى إدراك المبحوثين لدور تقنيات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية، وبين اتجاهاتهم نحو دورها في دعم وتعزيز الأمن السيبراني

- **نوع الدراسة ومنهجها:**

تنتمي هذه الدراسة إلى الدراسات الاستكشافية Exploratory, Descriptive Studies، فهي دراسة استكشافية، حيث تعد من الدراسات المبكرة التي تسهم في توفير قدر من المعلومات عن مدى فاعلية استخدام الهيئة الوطنية للأمن السيبراني بالمملكة العربية السعودية لتقنيات الذكاء الاصطناعي كتوجه مستقبلي، والتي لم تسبقها دراسة عربية في حدود علم الباحثين، إضافة إلى أن الدراسة تسعى لتحديد الفائدة المتوقعة من استخدام الهيئة الوطنية للأمن السيبراني لتقنيات الذكاء الاصطناعي، والمقترحات المقدمة لتعزيز هذا الاستخدام، والملامح المستقبلية لذلك. واعتمدت الدراسة على منهج المسح Survey Method بشقه الكمي من خلال أداة الاستبانة، عن طريق مسح عينة من المسؤولين (العاملين) بالهيئة الوطنية للأمن السيبراني، للحصول على البيانات المتصلة بالظاهرة.

- **مجتمع وعينة الدراسة:**

تم تطبيق البحث على عينة عشوائية من المسؤولين (العاملين) في الهيئة الوطنية للأمن السيبراني بالمملكة العربية السعودية، حيث تم تطبيق الدراسة على عينة قوامها ١٠٦ مفردة، لمعرفة مدى فاعلية استخدام الهيئة الوطنية للأمن السيبراني بالمملكة العربية السعودية لتقنيات الذكاء الاصطناعي كتوجه مستقبلي.

يوضح الجدول (١) الخصائص العامة لعينة الدراسة

البيانات الشخصية		الإجمالي	
		ك	٪
النوع	الذكور	76	71.7
	الإناث	30	28.3
	الإجمالي	106	100.0
السن	من ٢٥ الى ٣٤ سنة	33	31.1
	من ٣٥ الى ٤٤ سنة	48	45.3
	أكثر من ٤٥ سنة	25	23.6
	الإجمالي	106	100.0
سنوات الخبرة	من ٥ إلى ١٠ سنوات	50	47.2
	من ١٠ إلى ١٥ سنة	39	36.8
	أكثر من ١٥ سنة	17	16
	الإجمالي	106	100.0

يتبين من الجدول السابق الخصائص العامة لعينة الدراسة:

- من حيث النوع: حيث بلغت أعداد الذكور ٧٦ مفردة، في حين بلغت أعداد الاناث ٣٠ مفردة.
- من حيث السن: من ٣٥ الى ٤٤ سنة احتلت المركز الأول بنسبة ٤٥.٣٪، يليها فئة من ٢٥ الى ٣٤ سنة بنسبة ٣١.١٪، ثم الفئة أكثر من ٤٥ سنة في المركز الثالث بنسبة ٢٣.٦٪.

- من حيث سنوات الخبرة: فجاء من ٥ إلى ١٠ سنوات في المركز الأول بنسبة ٤٧.٢٪، تلاه من ١٠ إلى ١٥ سنة بنسبة ٣٦.٨٪، بينما بلغت أكثر من ١٥ سنة بنسبة ١٦٪.

وقد تم اختيار عينة الدراسة من المسؤولين (العاملين) في الهيئة الوطنية للأمن السيبراني بالمملكة العربية السعودية وذلك للآتي:

- معرفتهم التامة باختصاصات ومهام الهيئة الوطنية للأمن السيبراني، ومدى مسؤولياتها على وضع السياسات وآليات الحوكمة والأطر والمعايير والضوابط والإرشادات المتعلقة بالأمن السيبراني، وتعميمها على الجهات ذات العلاقة، ومتابعة الالتزام بها وتحديثها.
- تعزيزهم للأمن السيبراني في المملكة حمايةً للمصالح الحيوية للدولة وأمنها الوطني والبنى التحتية الحساسة والقطاعات ذات الأولوية والخدمات والأنشطة الحكومية، وبالتالي هم الأقدر بمعرفة مدى الاستفادة التامة من تقنيات الذكاء الاصطناعي.

وترجع أسباب اختيار تقنيات الذكاء الاصطناعي إلى الآتي:

- يمكنها التعامل مع عدد كبير من البيانات الضخمة.
- تحسين وتوفير المساعدة لعامل الأمن البشري.
- يساعد في التنبؤ للتهديدات المستقبلية.
- مواصلة تحسين الأتمتة.

- **متغيرات الدراسة:**

جدول (٢) متغيرات الدراسة

المتغير المستقل	المتغيرات الوسيطة	المتغير التابع
تقنيات الذكاء الاصطناعي	النوع – السن – سنوات الخبرة	الهيئة الوطنية للأمن السيبراني

- **حدود الدراسة:**

حيث تتمثل حدود الدراسة فيما يلي

- حدود موضوعية: حدد الباحثان موضوع الدراسة في التعرف على مدى فاعلية استخدام الهيئة الوطنية للأمن السيبراني بالمملكة العربية السعودية لتقنيات الذكاء الاصطناعي كتوجه مستقبلي.
- حدود بشرية: اقتصرت الدراسة الحالية على عينة قوامها ١٠٦ مفردة من المسؤولين (العاملين) بالهيئة الوطنية للأمن السيبراني.
- حدود زمنية: قام الباحثان بتوزيع الاستبانة وتجميعها خلال شهري (يناير/ فبراير ٢٠٢٣م)

- **أدوات الدراسة:**

تعتمد هذه الدراسة على استمارة الاستبانة **Questionnaire** وهو أسلوب جمع البيانات الذي يستهدف استثارة المبحوثين بطريقة منهجية (عبد المحسن القحطاني، ٢٠١٨)

- **إختبار صدق وثبات الإستبانة:**

- **اختبار الصدقReliability** : تم التأكد من صدق الاستبانة وأنه يقيس أهداف وتساؤلات وفروض الدراسة من خلال عرض الاستبانة على مجموعة من المحكمين المتخصصين في موضوع الدراسة❖❖❖، للتأكد من صلاحية الأداة لقياس متغيرات الدراسة، واتفق المحكمون بنسبة ٨٧٪ على صلاحية الأداة للتطبيق، وتم إجراء ما يلزم من تعديلات في ضوء مقترحاتهم لتصبح في شكلها النهائي.
- **اختبار الثباتValidity:** تم تطبيق اختبار قبلي على عينة قوامها ١٠٪ من إجمالي العينة، للتأكد من الفهم الصحيح للأسئلة ومدى وضوحها وترتيبها، ومن ثم ادخال بعض التعديلات المقترحة، وللتأكد من ثبات البيانات قامت الباحثتان بإعادة الاختبارTest.Retest على عينة قدرها ١٥٪ من المبحوثين بعد مرور أسبوعين من الاختبار الأول، وبلغ معامل الثبات ٩٠٪، وهي قيمة عالية تشير إلى دقة وثبات الأداة والاستقرار في نتائجها.

- **المعالجة الإحصائية للبيانات:**

تم الاستعانة ببرنامج التحليل الإحصائي (SPSS)، وتمت المعالجات الإحصائية من خلال استخدام المعاملات والاختبارات الإحصائية التالية:

- التكرارات البسيطة والنسب المئوية.
- المتوسط الحسابي والانحرافات المعيارية.
- الوزن النسبي الذي يحسب من المعادلة: الوزن المئوي = (المتوسط الحسابي x ١٠٠) ÷ الدرجة العظمى للعبارة.
- اختبار (ت) للمجموعات المستقلة (Independent-Samples T-Test) لدراسة الدلالة الإحصائية للفروق بين متوسطين حسابين لمجموعتين من المبحوثين في أحد متغيرات الفئة أو النسبة (Interval or Ratio)
- اختبار تحليل التِباين ذو البعد الواحد (Oneway Analysis of Variance) المعروف اختصارا باسم ANOVA لقياس الفروق بين المتوسطات بين أكثر من مجموعتين من المبحوثين في أحد متغيرات الفئة أو النسبة.
- اختبار كا٢ (Chi square) لدراسة معنوية الفروق بين مجموعات المتغيرات الاسمية.
- معامل ارتباط بيرسون (Pearson Correlation Coefficient) لدراسة شدة واتجاه العلاقة الارتباطية بين متغيرين من نوع الفئة أو النسبة (Interval or Ratio).

• نتائج الدراسة الميدانية

• الجزء الأول: النتائج العامة للدراسة الميدانية والمقاييس الإحصائية:

جدول (٣) يوضح مدى اهتمام المبحوثين بتقنيات الذكاء الاصطناعي

مدى اهتمام المبحوثين بتقنيات الذكاء الاصطناعي	ك	٪
دائمًا	80	75.5
أحيانًا	23	21.7
نادرًا	3	2.8
الإجمالي	106	100.0
كا٢: ٤٥٩.٥٦٠ درجة الحرية: ٣ المعنوية: ٠.٠٠٠ دال		

يتضح من بيانات الجدول السابق أن أعلى نسبة إجابة كانت من نصيب المبحوثين الذين يهتمون بتقنيات الذكاء الاصطناعي دائما حيث جاءت بنسبة ٧٥.٥٪، يلي ذلك الاهتمام أحيانا بنسبة ٢١.٧٪، ثم الاهتمام نادرا بنسبة ٢.٨٪، ويمكن تفسير ذلك في ضوء متابعة المبحوثين لكل جديد في مجال التكنولوجيا وتقنية المعلومات، ويعزو ذلك الى إدراكهم لتقنيات الذكاء الاصطناعي، والتنبؤ بإمكانية تطبيقها في مجالات الأمن السيبراني.

وتتفق هذه النتيجة مع ما تظهره المؤشرات الإحصائية المبينة أسفل الجدول من وجود فروق ذات دلالة إحصائية في معدل اهتمام أفراد العينة بتقنيات الذكاء الاصطناعي، حيث بلغت قيمة كا٢ ٤٥٩.٥٦٠ عند مستوى معنوية ٠.٠٠٠

جدول (٤) يوضح درجة معرفة المبحوثين بتقنيات الذكاء الاصطناعي

درجة معرفة المبحوثين بتقنيات الذكاء الاصطناعي	الإجمالي	
	ك	٪
معرفة متعمقة	88	83.01
معرفة إلى حد ما	18	16.99
الإجمالي	106	100.0
كا٢: ٢٩.٠٨ درجة الحرية: ١ مستوى المعنوية: ٠.٠٠٠ دال		

توضح بيانات الجدول السابق درجة معرفة المبحوثين بتقنيات الذكاء الاصطناعي، فذكروا معرفة متعمقة بنسبة ٨٣.٠١٪، ثم معرفة إلى حد ما بنسبة ١٦.٩٩٪، وتتسق هذه النتيجة مع المؤشرات المبينة أسفل الجدول، حيث تبلغ قيمة كا ٢ ٢٩.٠٨، عند درجة حرية ١، ومستوى معنوية ٠.٠٠٠، مما يعني وجود فروق دالة إحصائيًا بين المبحوثين من حيث درجة معرفتهم بتقنيات الذكاء الاصطناعي.

وترى الدراسة الحالية أن التكنولوجيا الحديثة، والتي طورت التقنيات الخاصة بالذكاء الاصطناعي، الذي يعد أهم مخرجات الثورة الصناعية الرابعة لتعدد استخداماته في كافة المجالات، ليست بعيدة عن المشهد الأمني، مع حرص المملكة الحثيث نحو الاستثمار في تفعيل تقنيات الجيل الرابع من الثورة الصناعية وعلى رأسها الذكاء الاصطناعي لتحقيق أهدافها التنموية الطموحة باعتباره لغة المستقبل التي لا محيد عن إدراك أبجدياتها والقضاء

على أميته، واعتماد العديد من القطاعات عليه مثل الصحة والإعلام والتعليم والخدمات والقطاعات الحيوية الأخرى عليه، فضلا عن تأثيراته الإيجابية في تقليل الانفاق ورفع جودة المنتجات.

جدول (٥) يوضح مدى تعرض المبحوثين لتقنيات الذكاء الاصطناعي

مدى تعرض المبحوثين لتقنيات الذكاء الاصطناعي	ك	٪
مرتفع	94	88.7
متوسط	8	7.9
منخفض	4	3.7
الإجمالي	106	100.0
كا٢: ٢٢٠.١٦٠ درجة الحرية: ٢ المعنوية: ٠.٠٠٠ دال		

يتضح من الجدول السابق ارتفاع معدل تعرض المبحوثين لتقنيات الذكاء الاصطناعي، والذي جاء بمستوى مرتفع بنسبة ٨٨.٧٪، ومستوى متوسط بنسبة ٧.٩٪، ومنخفض بنسبة ٣.٧٪، وهوما يعني حرص المبحوثين على متابعة تقنيات الذكاء الاصطناعي في المجال الأمني، وفقا لقدرات تلك التقنيات، والتي أصبحت تتفوّق في كثير من الأحيان على القدرات البشرية، في رصد الأدلة بدقة، وذلك بهدف محاولة التنبؤ بإمكانية وقوع الجرائم المشابهة، وتتفق هذه النتيجة مع ما تظهره المؤشرات الإحصائية المبينة أسفل الجدول من وجود فروق ذات دلالة إحصائية في مدى تعرض عينة الدراسة لتقنيات الذكاء الاصطناعي، حيث بلغت قيمة كا٢ ٢٢٠.١٦٠عند مستوى معنوية ٠.٠٠٠.

جدول (٦) يوضح دوافع اعتماد أفراد العينة على تقنيات الذكاء الاصطناعي مستقبلا

دوافع الاعتماد	موافق بشده		موافق الى حد ما		لا اوافق		المتوسط	الانحراف المعياري	الوزن النسبي	الترتيب
	ك	٪	ك	٪	ك	٪				
يمكنه التعامل مع عدد كبير من البيانات	105	99.05	100	94.3	3	2.8	2.94	.311	98.0	1
يقلل من وقت الاستجابة	98	92.5	80	75.5	1	.94	2.78	.524	92.7	2
يساعد في التنبؤ للتهديدات المستقبلية	98	92.5	88	83.01	1	.94	2.70	.549	90.0	3
تحسين وتوفير المساعدة لعامل الأمن البشري	87	82.07	94	88.7	3	2.8	2.37	.560	79.0	4
يساعد في تقليل التكاليف	65	61.3	56	52.8	8	7.5	2.17	.464	72.3	5

يتضح من بيانات الجدول السابق تتعدد دوافع اعتماد أفراد العينة على تقنيات الذكاء الاصطناعي في المستقبل، حيث تبين أن ٩٨.٠ منهم كان دافعهم الأساسي قدرة تقنيات الذكاء الاصطناعي التعامل مع عدد كبير من البيانات، حيث إنه من المعتاد حدوث العديد من الأنشطة على الخوادم الخاصة (بالشركات – المنشآت – الهيئات ...) وهذا يعني أنه يتم نقل كمية كبيرة من البيانات يوميًا بين الأجهزة والشبكات، فلا يمكن لمحللي الأمن السيبراني

فحص كل جزء من البيانات بحثًا عن المخاطر المحتملة، ومن ثم يعد أفضل خيار لاكتشاف هذه التهديدات التي تمر كنشاط يومي هو تقنيات الذكاء الاصطناعي، فيمكنه فرز الكثير من البيانات بالإضافة إلى تتبع حركة المرور بشكل آلي ويمكن أن يوفر تحليلا دقيقا عن أنشطة الخوادم، بالإضافة إلى ذلك لديه القدرة على التعرف على أي مخاطر قد تكون مختبئة في زخم المعلومات

وجاء في الترتيب الثاني التقليل من وقت الاستجابة بوزن نسبي ٩٢.٧، حيث تعد القدرة على اكتشاف التهديدات بسرعة أمرًا بالغ الأهمية، فالذكاء الاصطناعي قادر على مسح كميات كبيرة من البيانات في وقتٍ واحد وتحديد التهديدات الإلكترونية في نفس الوقت مما يسهل عملية تحقيق الأمان.

أما الترتيب الثالث فكان من نصيب المساعدة في التنبؤ للتهديدات المستقبلية بوزن نسبي ٩٠.٠، حيث تمر كمية كبيرة من البيانات على محللو الأمن السيبراني، مما يجعل التنبؤ بالتهديدات المستقبلية أمر صعب عليهم، ولكن مع قدرة تقنيات الذكاء الاصطناعي على التعامل مع عدد كبير من البيانات في وقت واحد، فيمكن أن يساعد في اكتشاف أي نشاط ضار أو تهديدات محتملة في وقت مبكر لمنعها، مما يعتبر مفيد للمساعدة في تقليص إضاعة الوقت واستهلاك الأيدي العاملة في غير محلها.

وجاء تحسين وتوفير المساعدة لعامل الأمن البشري بوزن نسبي ٧٩.٠، حيث نجد أن الذكاء الاصطناعي يمكن أن يساعد في تعزيز الجهد اليدوي المبذول في اكتشاف التهديدات باستخدام المعلومات التي قدمتها الأجهزة من الهجمات السابقة، وفى الترتيب الأخير جاءت المساعدة في تقليل التكاليف بوزن نسبي ٧٢.٣، حيث لاحظنا في السنوات الأخيرة تأثر العديد من المنشآت عامًا بعد الآخر من الأثر المالي لانتهاكات البيانات، وهذا الأمر لا يمكن تجاهله، وليس لدى المجرمين نية للتوقف، ووفقا (تقرير IBM Cost of Data Breach 2021)، والذى كشف أن المنشآت التي تستخدم الذكاء الاصطناعي لأغراض الأمن السيبراني تواجه فرقا بنسبة ٨٠٪ في انخفاض التكاليف، ٢.٩٠ مليون دولار مقارنة بـ ٦.٧١ مليون دولار للمنشآت التي لا تستخدم خدماتها.

جدول (٧) يوضح مدى الثقة في تقنيات الذكاء الاصطناعي في مجال الأمن السيبراني

مدى الثقة في تقنيات الذكاء الاصطناعي في مجال الأمن السيبراني	ك	٪
اثق بدرجة كبيرة	69	65.09
اثق الى حد ما	35	33.01
لا اثق على الاطلاق	2	1.9
الإجمالى	106	100.0
كا٢: ٢٦٨.٧٨١ درجة الحرية: ٢ المعنوية: ٠.٠٠٠ دال		

أوضحت نتائج الجدول السابق ان ٦٥.٠٩٪ من عينة الدراسة أظهروا ثقتهم بدرجة كبيرة في تقنيات الذكاء الاصطناعي في مجال الأمن السيبراني، في حين أوضحت نسبة ٣٣.٠١٪ من إجمالي عينة الدراسة أنهم يثقون بها إلى حد ما، أما نسبة ١.٩٪ كانت من نصيب عدم الثقة فيها. وتتفق النتيجة مع ما تظهره المؤشرات الإحصائية المبينة أسفل الجدول من وجود فروق ذات دلالة إحصائية في مدى الثقة في تقنيات الذكاء الاصطناعي في مجال الأمن السيبراني، حيث بلغت قيمة كا٢ ٢٦٨.٧٨١ عند مستوى معنوية ٠.٠٠٠

جدول (٨) يوضح مجالات توظيف تقنيات الذكاء الاصطناعي في الهيئة الوطنية للأمن السيبراني

مجالات توظيف تقنيات الذكاء الاصطناعي	موافق		موافق الى حد ما		لا اوافق		المتوسط	الانحراف المعياري	الوزن النسبي	الترتيب
	ك	٪	ك	٪	ك	٪				
أمن الشبكات	106	100	-	-	-	-	2.64	.517	88.0	1
خفض هجمات التصيّد	104	98.11	2	1.89	-	-	2.62	.516	87.3	2
إدارة الثغرات	100	94.33	6	5.66	-	-	2.59	.550	86.3	3
تحليل السلوك	90	84.90	14	13.20	2	1.89	2.56	.554	85.3	4
التحقق من الهوية	88	83.01	17	16.03	1	.94	2.55	.537	85.0	5

تتعدد مجالات توظيف تقنيات الذكاء الاصطناعي في الهيئة الوطنية للأمن السيبراني، وفقا لما أجاب به مسؤولي الهيئة عينة الدراسة، وتمثلت أولى هذه المجالات في أمن الشبكات، فجاء بوزن نسبي بلغ ٨٨، حيث يعمل الذكاء الاصطناعي على تسريع عملية إنشاء السياسات الأمنية وتحديد تصميم شبكات المؤسسات، بالإضافة إلى إدارة عدد كبير من الأجهزة وتحديثها وتصحيح الأمان فيها تلقائيا، وفي الترتيب الثاني جاء خفض هجمات التصيّد بوزن نسبي ٨٧.٣، حيث يستخدم الذكاء الاصطناعي في صنع أدوات تحدد وتتابع هجمات التصيّد وتحدّ من حدوثها بطريقة أكثر فاعلية من الإنسان، أما الترتيب الثالث فكان من نصيب إدارة الثغرات والتي جاءت بوزن نسبي بلغ ٨٦.٣، فنجد أن الذكاء الاصطناعي يتم استخدامه في تقييم الأنظمة بشكل سريع وتحديد نقاط الضعف في الأنظمة والشبكات وكذلك في تصميم أنظمة استباقية لإدارة الثغرات، وجاء تحليل السلوك بوزن نسبي ٨٥.٣ ، حيث تُصمم تقنيات الذكاء الاصطناعي خوارزميات خاصة، بطريقة تمكنها من تعلم سلوك المستخدم وخلق نمط خاص به يستفاد منه في تحليل الهجمات، وبوزن نسبي بلغ ٨٥ جاء التحقق من الهوية، حيث يساعد الذكاء الاصطناعي المطورين في رفع فاعلية التقنيات الحيوية وزيادة دقتها.

جدول (٩) يوضح الأشكال المتعددة للجرائم الإلكترونية (السايبيرية)

الأشكال المتعددة للجرائم الإلكترونية	ك	٪
التلاعب في المعلومات واتلافها	30	28.3
جرائم الاعتداء على الأموال	15	14.1
الجرائم الإلكترونية ضد الحكومات	15	14.1
الجرائم الإلكترونية ضد الأفراد	14	13.2
الإرهاب الإلكتروني	14	13.2
الجرائم الإلكترونية ضد الملكية	12	11.3
الجرائم السياسية الإلكترونية	6	5.6
الاجمالي	106	100

من المؤكد أن هجمات الذكاء الاصطناعي الإلكترونية والبرامج الضارة التي يستخدمها مجرمي الإنترنت تُشكِل تهديد كبير على أصحاب البرامج والشبكات، وتشير هذه الهجمات واختراق الأجهزة الإلكترونية إلى التطور القائم في مجال الذكاء الاصطناعي وارتباطه بالجرائم الإلكترونية، حيث يستخدم مجرمي الإنترنت الذكاء الاصطناعي في عمليات الاختراق، وعلى الجانب الآخر يساعد الذكاء الاصطناعي في اكتشاف الحملات الهجومية ويعمل على التصدي لهذه الهجمات، ويوجد مخاوف كبيرة بشأن اختراق المجرمين لأنظمة الشركات والبنوك، ولذا يجب أن يكونوا على استعداد تام لمواجهة خطر الجريمة الإلكترونية.

ويوضح الجدول السابق الصور المتعددة للجرائم الإلكترونية أو ما يطلق عليها الجرائم السايبيرية، والتي جاء في مقدمتها التلاعب في المعلومات واتلافها بنسبة بلغت ٢٨.٣٪، تلاها كل من جرائم الاعتداء على الأموال، الجرائم الإلكترونية ضد الحكومات بنفس النسبة والتي بلغت ١٤.١٪، وتدرجت العديد من أشكال الجرائم في الترتيب مثل الجرائم الإلكترونية ضد الأفراد، الإرهاب الإلكتروني بنفس النسبة والترتيب، ثم الجرائم الإلكترونية ضد الملكية، الجرائم السياسية الإلكترونية بنسبة ١١.٣٪، ٥.٦٪ على التوالي.

ويعد التلاعب في المعلومات واتلافها من أخطر أنواع الجرائم الإلكترونية، والذي يتم من خلال إدخال معلومات لا تطابق الحقيقة المطابقة للواقع، ويتم اتلافها إما عن طريق استبدالها (تزويرها)، أو محوها من خلال الدخول إلى النظام المعلوماتي وحذف كافة المعلومات كليا أو جزئيا. (رانا عبد الرازق، ٢٠٢١)

جدول (١٠) يوضح مدى إدراك المبحوثين لدور تقنيات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية

دور تقنيات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية	ك	٪
تحليل الشبكات والوصول إلى حركات المرور الخاصة بالويب	46	43.4
تنبيه الأجهزة الإلكترونية بوجود خلل ومحاولة اختراق لتقنية محددة	23	21.7
يمنع عمليات الاختراق والتطفل في نفس الوقت	22	20.8
تحليل التهديدات التي قد تتعرض لها الشركات قبل حدوثها وفقاً للتجارب الماضية	15	14.1

يساعد الذكاء الاصطناعي في اكتشاف الحملات الهجومية ويعمل على التصدي لهذه الهجمات، وله فعالية كبيرة في تحليل الشبكات والوصول إلى حركات المرور الخاصة بالويب بكل سهولة، فكلما كان اكتشاف الجرائم الإلكترونية مبكراً كلما كان الضرر أقل، ومن خلاله يمكن تنبيه الأجهزة الإلكترونية بوجود خلل ومحاولة اختراق لتقنية محددة ومن ثم بدء العمل على إصلاحها، حيث يقوم الذكاء الاصطناعي بمنع عمليات الاختراق والتطفل في نفس الوقت، وبالتالي حماية البيانات من الجرائم الإلكترونية، ويشتهر تأثير الذكاء الاصطناعي على الجريمة الإلكترونية بأنه تأثير إيجابي يتمثل في حماية البيانات، ويكون ذلك عن طريق فهم أساسيات الدفاع عن الشبكات والحفاظ على المعلومات آمنة، وهذا ما تم توضيحه من خلال

بيانات الجدول السابق، حيث جاء تحليل الشبكات والوصول إلى حركات المرور الخاصة بالويب بنسبة ٤٣.٤٪، ثم تنبيه الأجهزة الإلكترونية بوجود خلل ومحاولة اختراق لتقنية محددة بنسبة ٢١.٧٪، وبفارق بسيط جاء منع عمليات الاختراق والتطفل في نفس الوقت بنسبة ٢٠.٨٪، وأخيرا تحليل التهديدات التي قد تتعرض لها الشركات قبل حدوثها وفقا للتجارب الماضية بنسبة بلغت ١٤.١٪.

جدول (١١) يوضح تأثير توظيف الهيئة الوطنية للأمن السيبراني لتقنيات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية

تأثير توظيف تقنيات الذكاء الاصطناعي	موافق		الى حد ما		لا اوافق		المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	الترتيب
	ك	٪	ك	٪	ك	٪				
حوكمة متكاملة للأمن السيبراني على المستوى الوطني (المتعلق بالأطراف الخارجية والحوسبة السحابية)	43	44.1	27	25.7	5	4.7	2.89	.444	96.3	1
إدارة فعالة للمخاطر السيبرانية على مستوى المملكة	39	40.2	27	25.7	4	3.2	2.79	.456	93.0	2
تعزيز القدرات الوطنية في الدفاع ضد التهديدات السيبرانية	36	35	25	23.8	4	3.2	2.69	.547	89.7	3
بناء القدرات البشرية الوطنية وتطوير صناعة الأمن السيبراني في المملكة	36	35	20	19	3	2.1	2.67	.542	89.0	4
تعزيز الشراكات والتعاون في الأمن السيبراني	33	32.02	19	17.9	2	2.1	2.63	.581	87.7	5
إدارة أمن الشبكات والتشفير	32	30.02	16	15.1	1	.89	2.48	.562	82.7	6

تكشف بيانات الجدول السابق عن تأثير توظيف الهيئة الوطنية للأمن السيبراني لتقنيات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية من وجهة نظر المبحوثين، فذكروا في المقدمة حوكمة متكاملة للأمن السيبراني على المستوى الوطني (المتعلق بالأطراف الخارجية والحوسبة السحابية) بنسبة ٩٦.٣٪، ثم إدارة فعالة للمخاطر السيبرانية على مستوى المملكة بنسبة ٩٣٪، وبنسب متقاربة جاء تعزيز القدرات الوطنية في الدفاع ضد التهديدات السيبرانية، وبناء القدرات البشرية الوطنية وتطوير صناعة الأمن السيبراني في المملكة بنسبة ٨٩.٧٪، ٨٩.٠٪ على التوالي، يليها تعزيز الشراكات والتعاون في الأمن السيبراني بنسبة ٨٧.٧٪، وأخيرا إدارة أمن الشبكات والتشفير بنسبة ٨٢.٧٪.

ويمكن تفسير ذلك في ضوء وجود بنية فضاء سيبراني وطنية متكاملة وآمنة يعد أحد أهم العوامل الممكنة للنمو والازدهار، إلا أن التوسع في استخدام التقنية يفتح آفاقا جديدة للمخاطر والتهديدات السيبرانية، مما يستوجب تعزيز الأمن السيبراني لحماية الشبكات، وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات وحماية ما تقدمه من خدمات وما تحويه من بيانات من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال وكذلك لتعزيز الربط التقني الآمن بين الخدمات الحكومية ودعم الاقتصاد الرقمي السعودي، من أجل ذلك تم وضع رؤية للاستراتيجية الوطنية للأمن السيبراني تعكس الطموح الاستراتيجي للمملكة وبأسلوب متوازن بين الأمان والثقة والنمو، وتتضمن الرؤية التي تسعى الهيئة إلى الوصول لها: فضاء سيبراني سعودي آمن وموثوق يمكن النمو والازدهار، بحيث تكون هذه الرؤية شاملة للفضاء السيبراني بأكمله، وتلبي أولويات المملكة وتطلعاتها، وتؤكد على تعزيز حماية الأنظمة التقنية والتشغيلية والبنى التحتية الحساسة والقدرة على الصمود والتصدي للحوادث السيبرانية وامتصاص الأضرار والتعافي منها في الوقت المناسب، بالإضافة إلى تعزيز ثقة الجهات الوطنية والمستثمرين والأفراد في الفضاء السيبراني السعودي، وكذلك المساهمة في النمو الاقتصادي والاجتماعي للمملكة، والذى يعتبر في مقدمة أولوياتها أن يكون آمن للتأكيد على حماية وصمود الأنظمة التقنية والتشغيلية والبنى التحتية الحساسة، ويمكن تحقيق ذلك باستخدام أحدث التقنيات التكنولوجية والتي في مقدمتها تقنيات الذكاء الاصطناعي.

اتفقت نتيجة الدراسة الحالية مع نتيجة دراسة (ليلي بن برغوث،٢٠٢٣) والتي توصلت إلى الدور المهم التي يقوم به الذكاء الاصطناعي في التصدي للهجمات السيبرانية ودحض الجريمة الإلكترونية.

جدول (١٢) يوضح مدى نجاح استخدام تقنيات الذكاء الاصطناعي في الهيئة الوطنية للأمن السيبراني

مدى نجاح استخدام تقنيات الذكاء الاصطناعي	درجة كبيرة		درجة متوسطة		درجة ضعيفة		المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	الترتيب
	ك	٪	ك	٪	ك	٪				
التعامل مع البيانات الضخمة	106	100	7	1.8	10	2.5	2.93	.336	97.7	1
التعرف على بصمة الصور والصوت والعين	93	85.8	44	11.0	13	3.3	2.82	.458	94.0	2
تفسير الأنماط التي تحددها خوارزميات التعلم الآلي	89	72.3	100	40.0	12	3.0	2.70	.556	90.0	3
تحديد التهديدات الجديدة والتنبؤ بها	87	70.5	90	80.5	18	4.5	2.67	.429	84.7	4
وقت الاستجابة للتهديدات	82	57.0	105	26.3	13	3.3	2.54	.535	70.3	5
التصوير عبر Drone	78	45.0	102	25.5	9	2.3	2.11	.506	53.4	6

تكشف بيانات الجدول السابق عن درجة نجاح استخدام تقنيات الذكاء الاصطناعي في الهيئة الوطنية للأمن السيبراني من وجهة نظر المبحوثين، فذكروا في المقدمة التعامل مع البيانات الضخمة بنسبة ٩٧.٧٪، ثم التعرف على بصمة الصور والصوت والعين بنسبة ٩٤٪، ثم تفسير الأنماط التي تحددها خوارزميات التعلم الآلي بنسبة ٩٠٪، وجاء تحديد التهديدات الجديدة والتنبؤ بها، ووقت الاستجابة للتهديدات بنسبة بلغت ٨٤.٧٪، ٧٠.٣٪ على التوالي، وأخيرا جاء التصوير عبر Drone بنسبة ٥٣.٤٪.

ويمكن تفسير ذلك في ضوء أن الذكاء الاصطناعي يُعد في الأمن السيبراني مجموعة شاملة من التخصصات والأعمال مثل السابق ذكرها والتي تدل على مدى نجاح استخدام تقنيات الذكاء الاصطناعي في الهيئة الوطنية للأمن السيبراني، حيث يركز الذكاء الاصطناعي في جوهره على النجاح مع الدقة التي تحل في المرتبة الثانية بعد النجاح، وبالطبع ليس من الممكن حتى الآن للذكاء الاصطناعي المعاصر تفسير النتائج بالقدرات البشرية، خاصة مع الأعمال والتطورات التكنولوجية الجديدة، إضافة إلى أنه من مزايا تقنيات الذكاء الاصطناعي لتحليلات البيانات الضخمة، أصبحت تحليلات البيانات آلية، فأنظمة الذكاء الاصطناعي قادرة على تحليل البيانات بشكل مستقل. بناءً على نتائج التحليل، كما أصبح الوصول إلى التحليلات أسهل، حيث يمكن للمستخدمين استخدام اللغة الطبيعية للعثور على إجابات بسهولة وبساطة دون الحاجة إلى علمٍاء البيانات لاستخراج الرؤى من البيانات. كما يمكننا القول أنه نظرا لسعي المملكة العربية السعودية لتحقيق رؤية ٢٠٣٠ في التحول الرقمي والأمن السيبراني لبداية عصر جديد يتزايد ويتنوع فيه الاقتصاد، الذي يعتمد على الاستفادة من الخدمات الرقمية والمعلوماتية، ومع تزايد الهجمات الهائلة على المعلومات والبيانات الرقمية التي يصعب على أعضاء فرق الأمٍن السيبراني ملاحقتها بالدقة المتناهية المطلوبة، كان من الضروري جدا استخدام الذكاء الاصطناعي

وقدراته في تحليل كميات هائلة من البياناتٍ والمعلومات لتسريع وتيرة الاستجابة وزيادة عمليات الأمن السيبراني وايضا قدرته على التصدي لتلك التهديدات لما يتميز به الذكاء الاصطناعي من سرعة هائلة وقدرة فائقة على مراقبة البيانات والكشف عن القيم المتطرفة التي تشير إلى احتمال وجود اختراقات معلوماتية، مما جعل الذكاء الاصطناعي حليفا لبرامج الأمن السيبراني.

تتفق هذه النتيجة من حيث اهتمامها بالبيانات الضخمة مع نتيجة دراسة (Purva Grover, Arpan Kumar ,Kar & Yogesh K. Dwivedi/ 2020 Annals) حيث أشارت أن البيانات الضخمة هي النفط الجديد والذكاء الاصطناعي هو أداة التعامل مع تلك البيانات، وكذلك اتفقت معها دراسة (Anja Bachmann, Geoffrey C (Bowker,2019 والتي أوضحت كيف أثر استخدام تقنيات الذكاء الاصطناعي على إنتاج المعرفة البشرية عبر وسائل التواصل الاجتماعي لاسيما Facebook، وذلك من خلال عمل نماذج للبيانات الضخمة كطريقة لتحويل البيانات إلى معرفة قيمية، من خلال خوارزميات معدة مسبقا ومصممة تصميما خاصا لحوكمة هذه البيانات، كما اتفقت مع دراسة (Vimala Nunavath; Morten Goodwin,2018) من خلال الاهتمام بتحليلات البيانات الضخمة لإدارة الكوارث.

جدول (١٣) يوضح أبرز أدوار الأمن السيبراني المعتمدة على الذكاء الاصطناعي من وجهة نظر عينة الدراسة

أبرز أدوار الأمن السيبراني المعتمدة على الذكاء الاصطناعي	ك	٪
رفع مستوى الوعي بمخاطر أمن المعلومات	51	48.11
اكتشاف ثغرات الشبكات واحتمالية اختراقها	22	20.8
التنبؤ بالهجمات المستقبلية	12	11. 3
تحليل البرمجيات الضارة	16	15.09
تحديد هوية المهاجم	5	4.7
الاجمالي	106	100

تكشف بيانات الجدول السابق عن أبرز أدوار الأمن السيبراني المعتمدة على الذكاء الاصطناعي من وجهة نظر عينة الدراسة، فذكروا في البداية رفع مستوى الوعي بمخاطر أمن المعلومات بنسبة ٤٨.١١٪، حيث تواصل الهيئة الوطنية للأمن السيبراني جهودها في رفع مستوى الوعي بالأمن السيبراني، عبر جلساتها التوعوية المخصصة لمنسوبي الجهات الوطنية لبناء ثقافة سيبرانية عالية وتهيئة البيئة الآمنة لدعم نمو كافة القطاعات تماشيا مع أهداف الهيئة الاستراتيجية، إضافة إلى تعزيز الأمن السيبراني وأمن المعلومات في المملكة لتقليل المخاطر وتعزيز الثقة وتمكين النمو، بما يسهم في الوصول إلى فضاء سيبراني سعودي آمن وموثوق يمكن النمو والازدهار.

وفى المرتبة الثانية جاء اكتشاف ثغرات الشبكات واحتمالية اختراقها بنسبة ٢٠.٨، حيث تعد المعلومات السرية لها قيمة هائلة، وغالبًا ما يتم بيعها على الإنترنت المظلم (دارك ويب)، فعلى سبيل المثال، يمكن شراء الأسماء وأرقام بطاقات الائتمان، ثم استخدامها لأغراض سرقة الهوية أو الاحتيال،

وليس من المستغرب أن الاختراقات الأمنية يمكن أن تكلف مبالغ ضخمة من المال، وجاءت المرتبة الثالثة من نصيب التنبؤ بالهجمات المستقبلية بنسبة ١١.٣٪، وجاء تحليل البرمجيات الضارة بنسبة ١٥.٠٩٪، حيث أصبحت القدرة على تحليل البرامج الخبيثة والفيروسات من المهارات المهمة لأي مختص في أمن المعلومات أو من يقوم بالاستجابة والتعامل مع الاختراقات والحوادث عند وقوعها، أما بالنسبة لتحديد هوية المهاجم فجاءت بنسبة ٤.٧٪، حيث يمكن الذكاء الاصطناعي مراقبة جميع البيانات ورصدها باستمرار، وليس فقط أمن البيانات، للكشف عن أنماط المهاجمين التي تشير إلى وجود حوادث محتملة (حتى لو لم تتوافق هذه الحلول مع أنماط الهجوم المعروفة).

اتفقت هذه النتيجة مع نتيجة دراسة (جعفر العدوان، ٢٠٢٢) والتي حددت تسعة أدوار مهمة للأمن السيبراني المعتمد على الذكاء الاصطناعي موزعة على ٣ مراحل تشمل التقييم الآلي للثغرات الأمنية، والتوعية والتدريب، والمصادقة، واكتشاف التسلل والاختراقات الأمنية، وأيضا اكتشاف رسائل التصيد الإلكترونية المزعجة ورسائل التصيد الاحتيالي، وتحليل البرمجيات الضارة، وأتمتة المهام الروتينية، ونشر المصائد للإطاحة بالمهاجمين.

كما اتفقت هذه النتيجة مع دراسة (Bhavani Thuraisingham,2020) والتي هدفت إلى التعرف على دور كل من الذكاء الاصطناعي والأمن السيبراني في حماية أنظمة وسائل التواصل الاجتماعي من الهجمات الإلكترونية على أنظمة المعلومات، وانتهاك خصوصية الأفراد، ومشاركة المعلومات الخاطئة المعروفة باسم fake news.

جدول (١٤) يوضح اتجاهات عينة الدراسة نحو الدور الذي تقوم به تقنيات الذكاء الاصطناعي في دعم وتعزيز الأمن السيبراني

درجة الموافقة / الاتجاهات	موافق		محايد		معارض		المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	الترتيب
	ك	٪	ك	٪	ك	٪				
تمكن تقنيات الذكاء الاصطناعي من اكتشاف حالات الاختراق الشاذة داخل الشبكات بشكل أسرع من البشر	92	83	59	16.7	١	٠.٣	٢.٨٣	٠.٣٩	٩٤.٢	١
تمكن تقنيات الذكاء الاصطناعي من تحديد أنماط البيانات التي قد تشير إلى نشاط ضار	91	82.7	60	33.4	١	٠.٣	٢.٨٢	٠.٣٩	٩٤.١	٢
تساعد تقنيات الذكاء الاصطناعي قدرات التشغيل الآلي من الانتهاء من عملها في وقت أقل مثل (تحديثات البرامج – عمليات التصحيح)	76	66.6	56	30.1	٠	٠	٢.٦٦	٠.٤٧	٨٨.٨	٣
فرز رسائل البريد الإلكتروني الضارة	34	50	43	29	٠	٠	٢.٥٠	٠.٥٠	٨٣.٣	٤
تحديد البرامج الضارة وبرامج الفدية قبل وصولها إلى صندوق الوارد الخاص بالمستخدم	19	33.8	33	19	٠	٠	٢.٣٤	٠.٤٧	٧٧.٩	٥
الإجمالي	106									

تعكس بيانات الجدول الأوزان النسبية لترتيب اتجاهات المبحوثين نحو الدور الذي تقوم به تقنيات الذكاء الاصطناعي في دعم وتعزيز الأمن السيبراني، وذلك كالتالي:

يعد الذكاء الاصطناعي أداة قوية للأمن السيبراني قادرة على تحديد التهديدات والتخفيف من حدتها بسرعة، لكنها تحتاج إلى الإشراف والدعم المناسبين حتى تكون فعالة، حيث يمكن للذكاء الاصطناعي تحليل كميات كبيرة من البيانات بسرعة وبدقة، وأتمتة العمليات، والتكيف مع التهديدات الجديدة، وتوفير النطاق والسرعة اللازمين للحماية من الهجمات السيبرانية وخدع الهاكرز، وتحديد الانتهاكات المحتملة قبل حدوثها.

وفى عالمنا اليوم بدأت المنظمات والمؤسسات المختلفة في جميع أنحاء العالم بالفعل في استخدام أنظمة الذكاء الاصطناعي، وتشهد نتائج واعدة في تعزيز الأمن وتحسين الكفاءة التشغيلية نتيجة لذلك، وبناء على ذلك انفردت عناصر الجدول الحالي في توضيح اتجاهات المبحوثين نحو تقنيات الذكاء الاصطناعي ودورها في اكتشاف حالات الاختراق الشاذة داخل الشبكات بشكل أسرع من البشر، حيث جاء ذلك بوزن نسبي بلغ ٩٤.٢، حيث تعالج هذه التقنيات كميات هائلة من البيانات في غضون ثوان، وفي المرتبة التي تليها جاء تمكن تقنيات الذكاء الاصطناعي من تحديد أنماط البيانات التي قد تشير إلى نشاط ضار بوزن نسبي بلغ ٩٤.١، مما يسمح للمؤسسات بالاستجابة بسرعة وكفاءة أكبر.

وفى العادة تأخذ برامج التحديثات وقدرات التشغيل الآلي وقتاً طويلا للانتهاء من عملها، إلا أنه مع استخدام تلك التقنيات لن يتعدي الأمر ثوان معدودة، وجاء ذلك بوزن نسبي بلغ ٨٨.٨، ومن الأمور المهمة التي أضحت محل اهتمام من الجميع نجد فرز رسائل البريد الإلكتروني الضارة، وتحديد البرامج الضارة وبرامج الفدية قبل وصولها إلى صندوق الوارد الخاص بالمستخدم، وذلك بوزن نسبي بلغ ٨٣.٣، ٧٧.٩ على التوالي، حيث أصبح قراصنة العالم أيضًا أكثر تعقيداً في اختراقاتهم، حيث باتوا يستخدمون أنظمة أكثر حبكة وتعقيداً أو حتى يستندون إلى الذكاء الاصطناعي المضاد لاختراق مناطق الحماية السيبرانية، وهو ما قد ينتج مواجهات بين ذكاء اصطناعي وآخر، ووفقا لذلك تقدم التقنيات الجديدة التي تعمل وفق خوارزميات الذكاء الاصطناعي العديد من المزايا مقارنة بالتقنيات التقليدية لدرأ المخاطر والتهديدات الأمنية.

اتفقت هذه النتيجة مع نتيجة دراسة (خليل سعيدي، مرزوق بن مهدى، ٢٠٢٢) والتي اهتمت بتسليط الضوء على أهمية الذكاء الاصطناعي في تحقيق الامن السيبراني والحفاظ على البيانات والمعلومات المعرضة للاختراق، والتي توصلت إلى وجوب التفكير في توظيف تقنيات الذكاء الاصطناعي لحماية خصوصيات الأفراد والمستخدمين عبر مختلف المنصات الرقمية وعلى صعيد جميع المجالات.

جدول (١٥) يوضح الفائدة المتوقعة من استخدام تقنيات الذكاء الاصطناعي في الهيئة الوطنية للأمن السيبراني

الفائدة المتوقعة	درجة كبيرة		درجة متوسطة		درجة ضعيفة		المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	الترتيب
	ك	٪	ك	٪	ك	٪				
الاسهام في التخطيط الأمني على كافة أنحاء المملكة	85	92.8	16	4.0	13	3.3	2.89	.399	96.3	1
نشر المصائد المختلفة للإحاطة بالمهاجمين	71	85.3	43	10.8	16	4.0	2.81	.483	93.7	2
تحصين المجتمع من الجرائم الإلكترونية	40	32.5	34	63.5	16	4.0	2.29	.533	76.3	3
حظر برامج التجسس	35	21.3	29	72.3	26	6.5	2.15	.506	71.7	4
كا٢: 153.760	درجة الحرية: 1			مستوي المعنوية: ٠.٠٠٠ دال						

تكشف بيانات الجدول السابق عن الفائدة المتوقعة من استخدام تقنيات الذكاء الاصطناعي في الهيئة الوطنية للأمن السيبراني من وجهة نظر المبحوثين، فذكروا في المقدمة الاسهام في التخطيط الأمني على كافة أنحاء المملكة بنسبة ٩٦.٣٪، ثم نشر المصائد المختلفة للإحاطة بالمهاجمين بنسبة ٩٣.٦٪، وتحصين المجتمع من الجرائم الإلكترونية بنسبة ٧٦.٣٪، وأخير حظر برامج التجسس بنسبة ٧١.٧٪، والتي تعتبر شكل من أشكال العدوى السيبرانية، حيث يقوم المجرم الإلكتروني بتصميمها للتجسس على إجراءات الكمبيوتر، ونقل المعلومات إليه، وهنا يظهر الأمن السيبراني كحل مثالي لهذه الحالة؛ مثل جدار الحماية FortiGate من شركة Fortinet، والذي يمنع برنامج التجسس من الدخول والتأثير، ويحافظ على سرية المعلومات. وتتسق هذه النتيجة مع المؤشرات المبينة أسفل الجدول، حيث تبلغ قيمة كا ٢ ١٥٣.٧٦٠، عند درجة حرية، ومستوى معنوية ٠.٠٠٠، مما يعني وجود فروق دالة إحصائيًا بين المبحوثين من حيث الفائدة المتوقعة من استخدام تقنيات الذكاء الاصطناعي في الهيئة الوطنية للأمن السيبراني.

ويمكن تفسير ذلك أنه على الرغم من الإيجابيات الهائلة التي تحققت بفضل تقنية المعلومات، فإن تلك الثورة المعلوماتية المتصاعدة قد صاحبتها في المقابل جملة من الانعكاسات السلبية الخطيرة نتيجة سوء الاستخدام، ومن بين تلك الانعكاسات المستحدثة، ظاهرة الجريمة الرقمية، والتي تصاعدت مخاطرها بدورها مما أفرز نوعًا جديدًا من الجرائم العابرة للقارات، والتي لم تعد مخاطرها وأثارها محصورة في نطاق دولة بعينها مما أثار بعض التحديات القانونية أمام الأجهزة المعنية بمكافحة الجريمة، ومن هنا تظهر الفائدة المتوقعة من التقنيات المتلاحقة للذكاء الاصطناعي في حماية وتعزيز الأمن السيبراني.

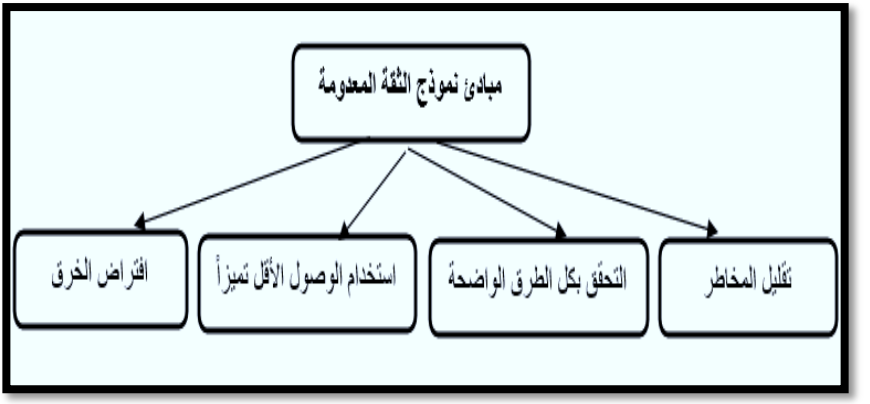
اتفقت تلك النتيجة مع نتيجة دراسة (عمار البابلي، ٢٠٢٠) والتي تناولت توظيف تقنيات الذكاء الاصطناعي في العمل الأمني، وكذلك توظيفها في التعرف على الوجه والهوية الرقمية داخل الاستنتاجات والتحليل الأمني، بما يساعد الأجهزة الأمنية في التعرف على الأشخاص المطلوبين وجمع معلومات عنهم، بغرض حفظ الأمن العام ومنع وقوع الجرائم.

جدول (١٦) يوضح المقترحات المقدمة لتعزيز استخدام تقنيات الذكاء الاصطناعي بالهيئة الوطنية للأمن السيبراني

مقترحات المبحوثين لتعزيز استخدام تقنيات الذكاء الاصطناعي بالهيئة الوطنية للأمن السيبراني	الإجمالي	
	ك	٪
عدم وضع الثقة كاملة في النظم المؤتمتة (من خلال التقنيات)	99	96.3
اعتماد استراتيجية قوية للاستثمار في البحوث والبنية التحتية لتقنيات الذكاء الاصطناعي المقترح استخدامها في الهيئة الوطنية للأمن السيبراني.	98	81.8
الاستباقية بقدر المستطاع في اكتشاف نقاط الضعف الجديدة التي تطرحها تقنيات الذكاء الاصطناعي على المجالات الحساسة للمخاطر وخاصة الأمن ومحاولة معالجتها على وجه السرعة	76	79.0
التدريب المستمر للعاملين في الهيئة الوطنية للأمن السيبراني على كيفية استخدام التقنيات المستحدثة للذكاء الاصطناعي	61	24.5
توفر عدد كاف من المبرمجين والمتخصصين في الخوارزميات	55	19.0
تقديم برامج توعوية تعنى بالأمن السيبراني بالمؤسسات الأمنية السعودية	42	10.5
حماية مؤسسات المملكة من الاختراق السيبراني داخليا وخارجيا	32	8.0
الإجمالي	106	

تكشف بيانات الجدول السابق عن مقترحات المبحوثين لتعزيز استخدام تقنيات الذكاء الاصطناعي بالهيئة الوطنية للأمن السيبراني، فذكروا في المقدمة عدم وضع الثقة كاملة في النظم المؤتمتة (من خلال التقنيات) بنسبة ٩٦,٣٪، ثم اعتماد استراتيجية قوية للاستثمار في البحوث والبنية التحتية لتقنيات الذكاء الاصطناعي المقترح استخدامها في الهيئة الوطنية للأمن السيبراني بنسبة ٨١,٨٪، تلاها بنسبة ٧٩٪ الاستباقية بقدر المستطاع في اكتشاف نقاط الضعف الجديدة التي تطرحها تقنيات الذكاء الاصطناعي على المجالات الحساسة للمخاطر وخاصة الأمن ومحاولة معالجتها على وجه السرعة، ثم التدريب المستمر للعاملين في الهيئة الوطنية للأمن السيبراني على كيفية استخدام التقنيات المستحدثة للذكاء الاصطناعي بنسبة ٢٤.٥٪، وجاء توفر عدد كاف من المبرمجين والمتخصصين في الخوارزميات بنسبة ١٩٪، وبنسب متقاربة بلغت ١٠.٥٪، ٨٪ على التوالي جاء كل من تقديم برامج توعوية تعنى بالأمن السيبراني بالمؤسسات الأمنية السعودية، وحماية مؤسسات المملكة من الاختراق السيبراني داخليا وخارجيا.

ويمكننا تفسير المقترح الذي جاء في مقدمة المقترحات والمتمثل في عدم وضع الثقة كاملة في النظم المؤتمتة (من خلال التقنيات)، حيث نجد الآن تبني نهج أمان استباقي من خلال نموذج الثقة المعدومة، حيث نجد أن مؤسسات اليوم تحتاج إلى نموذج أمان جديد يتكيف بشكل أكثر فاعلية مع تعقيد البيئة الحديثة، والذي يعد من أهم مبادئه الآتي:



شكل (٢) يوضح مبادئ نموذج الثقة المعدومة

ويمكن تفسير تلك النموذج بناء على النقاط التالية:

- محاولة سد الثغرات الأمنية بكافة الطرق الممكنة.
- التحقق من هوية المستخدم والموقع وصحة الجهاز والخدمة وتصنيف البيانات.
- حماية البيانات السرية وتأمين الوصول إليها.
- الحد من هجمات الوصول المنهالة على القطاعات، والتحقق من التشفير التام، وتعزيز اكتشاف التهديدات وتحسين الدفاعات.

جدول (١٧) يوضح الملامح المستقبلية لاستخدام تقنيات الذكاء الاصطناعي في الهيئة الوطنية للأمن السيبراني وتأثيراتها المحتملة

الملامح المستقبلية	موافق		الي حد ما		لا اوافق		المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	الترتيب
	ك	٪	ك	٪	ك	٪				
زيادة الاعتماد على تقنيات الذكاء الاصطناعي لمواجهة التهديدات السيبرانية	100	98.3	4	1.0	15	3.8	2.92	.391	97.3	1
التوجه المبكر للاستفادة من البيانات	91	87.8	27	6.8	22	5.5	2.82	.507	94.0	2
المرونة والديناميكية في استخدام تقنيات الذكاء الاصطناعي	89	74.8	85	21.3	16	4.0	2.71	.536	90.3	3
ميزة تقنية وتنافسية	88	77.3	32	58.0	20	5.0	2.32	.564	77.3	4
التوجه المبكر وفرق متعددة للتخصصات	63	37	12	78.0	25	6.3	2.09	.460	69.7	5
تنمية رأس المال البشري	60	34	71	17.8	20	5.0	2.72	.549	54.4	6

يكشف تحليل البيئة الأمنية الدولية أنّ هناك اتجاهًا خطيًا تصاعديًا في جهود وأدوات تحقيق الأمن السيبراني، حيث يحاول كل الفاعلين، سواء كانوا دولًا أو مؤسسات وشركات أو أفرادًا، الوصول إلى أفضل الطرق لتحقيق الأهداف والغايات المرجوة في مجال أمن الفضاء السيبراني، فمع تسارع التقدم التكنولوجي والترابط العالمي بشكل كبير في إطار الثورة الصناعية الرابعة، يختبر العالم تزايدًا متواصلًا في التهديدات السيبرانية

بكافة أنواعها من جرائم سيبرانية وإرهاب وتجسس سيبراني وحروب سيبرانية، وتقوض المخاطر والتهديدات الأمنية النظامية غير المسبوقة الثقة والنمو على المستويين الوطني والكوني، وفي ظل التدافع بين تنامي مهددات الأمن السيبراني وجهود تحقيقه، هناك دائمًا يقين واحد، يتمثل في أنّ عالم الأمن السيبراني يواجه دائمًا بالمزيد من محاولات الاختراق والتهديد التي تتطلب الاستعداد للتصدي لها.

ومن أهم طرق الاستعداد هذه زيادة الاعتماد على تقنيات الذكاء الاصطناعي لمواجهة التهديدات السيبرانية، والتي جاءت في مقدمة الملامح المستقبلية لاستخدام تقنيات الذكاء الاصطناعي في الهيئة الوطنية للأمن السيبراني، وذلك بوزن نسبي ٩٧.٣، حيث نجد اقتراب المشاريع المستقبلية في قطاع التكنولوجيا والاتصالات إلى الرقمنة لتتماشى مع الواقع الجديد الذي يعتمد على تقنية التشغيل وإنترنت الأشياء والبنية التحتية الرقمية، وفي ظل هذا الواقع القائم، تتنامى تهديدات الأمن السيبراني.

أما الترتيب الثاني فكان من نصيب التوجه المبكر للاستفادة من البيانات، وذلك بوزن نسبي بلغ ٩٤، وهذا يعنى دفاع سيبراني قائم على البيانات، حيث لم تعد الأساليب والممارسات الدفاعية التقليدية التي تعتمد على المؤشرات المعروفة أو على مهام يدوية كافية لإحباط الهجمات السيبرانية، فالهجمات الإلكترونية تزداد تعقيدا، كما أن منتهكو الأمن السيبراني يتبنون المزيد من قدرات الذكاء الاصطناعي في مناوراتهم دون الكشف عن هويتهم، أو لفت الأنظار إليهم.

وجاء في الترتيب الثالث المرونة والديناميكية في استخدام تقنيات الذكاء الاصطناعي بوزن نسبي بلغ ٩٠.٣، ويمكننا القول في ذلك أنه لمواجهة التحديات الحالية والمستقبلية، لابد من مواكبة التطورات التقنية، وذلك عن طريق تسخير قدرات الذكاء الاصطناعي، بل وإنتاج قدرات مصممة خصيصا حسب الاحتياج المطلوب له، ومن ثم يمكن الانتقال إلى وسيلة دفاع سيبراني تنبؤية، يمكنها التفاعل مع البيانات الضخمة.

وفى الترتيب الرابع جاء ميزة تقنية وتنافسية، وذلك بوزن نسبى بلغ ٧٧.٣، والتي تعتبر منصة البيانات الضخمة بالأمن السيبراني، والت تعمل على تحويل وإرسال كميات كبيرة من البيانات إلى نماذج الذكاء الاصطناعي، والتي يتم انتاجها بمواصفات خاصة تتناسب مع أعمال الهيئة الوطنية للأمن السيبراني.

وجاء التوجه المبكر وفرق متعددة للتخصصات، بوزن نسبي بلغ ٦٩.٧، ونعني بالتوجه المبكر هذا هو دعم الابتكار في جميع مجالات الأمن السيبراني، والذي يتطلب إنتاج نماذج متخصصة لتحديد الثغرات، وإدخال أفكار متنوعة وتعاون جماعي لتصور حلول مبتكرة للدفاع السيبراني، أما بالنسبة لفرق متعددة التخصصات لتحليلات الأمن السيبراني، والتي ترتبط ارتباطا كاملا

بتقنيات الذكاء الاصطناعي، حتى يصبح الذكاء الاصطناعي وتعليم الآلات أمرا معتادا بين موظفي الأمن السيبراني بالهيئة، أما الترتيب الأخير فكان من نصيب تنمية رأس المال البشري، وذلك بوزن نسبي ٥٤.٤، حيث تتماشى استراتيجية استقطاب الكفاءات المتميزة مع بناء فرق متمكنة من تقنيات الذكاء الاصطناعي. والأمن السيبراني.

تتفق نتيجة الدراسة الحالية مع دراسة (ماجد الفتلاوى، حسن الأعسم، ٢٠٢٢) والتي كان من أهم توصياتها تشجيع روح الابتكارات لدى الموارد البشرية في مجال تقنيات الذكاء الاصطناعي.

- **الجزء الثاني: نتائج إختبار الفروض**
- **الفرض الأول: توجد علاقة دالة إحصائيًا بين الفائدة المتوقعة من إستخدام تقنيات الذكاء الاصطناعي في الهيئة الوطنية للأمن السيبراني وبين درجة نجاح هذا الاستخدام.**

جدول (١٨) يوضح معامل ارتباط بيرسون لقياس العلاقة بين الفائدة المتوقعة من استخدام تقنيات الذكاء الاصطناعي في الهيئة الوطنية للأمن السيبراني وبين درجة نجاح هذا الاستخدام.

الفائدة المتوقعة من استخدام تقنيات الذكاء الاصطناعي /	معامل ارتباط بيرسون	مستوي المعنوية	الدلالة
درجة نجاح هذا الاستخدام	٠.٠٧٩	٠.٠٠٠	دال
ن = العينة	١٠٦		

تشير بيانات الجدول السابق إلى وجود علاقة دالة إحصائيًا بين الفائدة المتوقعة من استخدام تقنيات الذكاء الاصطناعي في الهيئة الوطنية للأمن السيبراني، وبين درجة نجاح هذا الاستخدام، حيث بلغت قيمة معامل ارتباط بيرسون ٠.٠٧٩، عند مستوى معنوية ٠.٠٠٠، مما يعني أن ارتفاع الفائدة المتوقعة من استخدام تقنيات الذكاء الاصطناعي في مواقع التواصل الاجتماعي، تؤثر على درجة نجاح هذا الاستخدام، وبذلك ثبت صحة الفرض الأول.

- **الفرض الثاني: توجد فروق دالة إحصائيًا بين المبحوثين في مدى فاعلية توظيف تقنيات الذكاء الاصطناعي في الهيئة الوطنية للأمن السيبراني تبعا لخصائصهم الديموغرافية.**

جدول (١٩) يوضح مدى وجود فروق بين المسؤولين (العاملين) في مدى فاعلية توظيف تقنيات الذكاء الاصطناعي بالهيئة الوطنية للأمن السيبراني

مدى فاعلية توظيف تقنيات الذكاء الاصطناعي / المتغيرات الديموغرافية		العدد	المتوسط	الانحراف المعياري	مؤشرات إحصائية: الاختبار	درجة الحرية	مستوي المعنوية
النوع	ذكور	76	2.9846	.12345	ت= ٣.٥٧٤	٣٩٨	٠.٠٠٠ دال
	اناث	30	2.9079	.29110			
السن	من ٢٥ الى ٣٤ سنة	33	2.9670	.17954	ف= ٠.٦٤٦	٣ ٣٩٦	٠.٥٨٦ غير دال
	من ٣٥ الى ٤٤ سنة	48	2.9741	.15927			
	أكثر من ٤٥ سنة	25	2.9529	.21302			
سنوات الخبرة	من ٥ إلى ١٠ سنوات	50	2.9780	.14702	ف= ٣.٢٧٣	٢ ٣٩٧	٠.٠٣٩ دال
	من ١٠ إلى ١٥ سنة	39	2.9808	.13778			
	أكثر من ١٥ سنة	17	2.9194	.27451			

يتضح من خلال بيانات الجدول السابق ما يلي:

- بالنسبة للنوع: ثبت وجود فروق ذات دلالة احصائية بين المبحوثين في مدى فاعلية توظيف تقنيات الذكاء الاصطناعي بالهيئة الوطنية للأمن السيبراني وفقا النوع، حيث بلغت قيمة ت ٣.٥٧٤، عند مستوى معنوية ٠.٠٠٠، وكانت الفروق لصالح الذكور ثم الإناث.
- بالنسبة للسن: ثبت عدم وجود فروق ذات دلالة احصائية بين المبحوثين في مدى فاعلية توظيف تقنيات الذكاء الاصطناعي بالهيئة الوطنية للأمن السيبراني وفقا للسن، حيث بلغت قيمة ف ٠.٦٤٦، عند مستوى معنوية ٠.٥٨٦.
- بالنسبة لسنوات الخبرة: ثبت وجود فروق ذات دلالة احصائية بين المبحوثين في مدى فاعلية توظيف تقنيات الذكاء الاصطناعي بالهيئة الوطنية للأمن السيبراني، وفقا لسنوات الخبرة، حيث بلغت قيمة ف ٣.٢٧٣ عند مستوى معنوية ٠.٠٣٩، مما يعني وجود فروق دالة إحصائيًا بين المبحوثين في مدى فاعلية توظيف تقنيات الذكاء الاصطناعي بالهيئة الوطنية للأمن السيبراني، طبقا لمتغيري النوع وسنوات الخبرة، في حين لا توجد فروق دالة إحصائيًا بين المبحوثين طبقا لمتغير السن، وبذلك ثبت صحة الفرض الثاني جزئيا.

- **الفرض الثالث: توجد علاقة دالة إحصائيًا بين مدى إدراك المبحوثين لدور تقنيات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية، وبين اتجاهاتهم نحو دورها في دعم وتعزيز الأمن السيبراني.**

جدول (٢٠) يوضح معامل ارتباط بيرسون لقياس العلاقة بين إدراك المبحوثين لدور تقنيات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية، وبين اتجاهاتهم نحو دورها في دعم وتعزيز الأمن السيبراني

إدراك المبحوثين لدور تقنيات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية / اتجاهاتهم نحو دورها في دعم وتعزيز الأمن السيبراني	معامل ارتباط بيرسون	مستوى المعنوية	الدلالة
ن = العينة	٠.٧٩٥**	0.000	دال
	106		

تشير بيانات الجدول السابق إلى وجود علاقة دالة إحصائيًا بين إدراك المبحوثين لدور تقنيات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية، وبين اتجاهاتهم نحو دورها في دعم وتعزيز الأمن السيبراني، حيث بلغت قيمة معامل ارتباط بيرسون ٠.٧٩٥**، عند مستوى معنوية ٠.٠٠٠، مما يعني أنه كلما ارتفعت أدراك المبحوثين لدور تقنيات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية، ارتفع اتجاهاتهم نحو دورها في دعم وتعزيز الأمن السيبراني، وبذلك ثبت صحة الفرض الثالث.

- **النتائج العامة للدراسة والتوصيات والمقترحات:**
- **أولا: مناقشة النتائج العامة للدراسة:**

- نعيش اليوم في زمن الابتكارات العلمية والتقنيات غير المسبوقة وآفاق نمو غير محدودة، ويمكن لهذه التقنيات الجديدة مثل الذكاء الاصطناعي في

حال تم استخدامها على النحو الأمثل أن تجنب العالم الكثير من المضار وتجلب للعالم الكثير من الفوائد الضخمة، ويمثل الذكاء الاصطناعي أهم مخرجات الثورة الصناعية الرابعة لتعدد استخداماته في المجالات المختلفة، ويتوقع له أن يفتح الباب لابتكارات لا حدود لها وأن يؤدي إلى مزيد من الثورات الصناعية بما يحدث تغييرا جذريا في حياة الانسان، إذ أنه مع التطور التكنولوجي الهائل والمتسارع وما يشهده العالم من تحولات في ظل الثورة الصناعية الرابعة سيكون الذكاء الصناعي محرك التقدم والنمو والازدهار خلال السنوات القليلة القادمة، وبإمكانه وما يتبعه من ابتكارات أن يؤسس لعالم جديد قد يبدو الآن بعيدا، ولكن البوادر الحالية تؤكد على أن خلق هذا العالم بات قريبا.

- ويعتبر اليوم اتخاذ التدابير اللازمة لتحقيق الأمن السيبراني تحدياً كبيراً ومطلبا أساسيا على مستوى الأفراد والشركات والدول نظرا لوجود عدد أجهزة يفوق أعداد الأشخاص واعتماد البشرية بشكل شبه رئيسي على التكنولوجيا وعلى الصعيد الآخر أيضا أصبح المهاجمون والمتلصصون أكثر ابتكارا، ويُساعد الأمن السيبراني على صد هجمات السرقة باستخدام برامج الدفاع الإلكترونية، ومنع احتمالية استخدام المعلومات بشكل غير مصرح به وإحداث الضرر، ومنع حدوث محاولات ابتزاز تُضر بالفرد، كما يُحافظ على كيان المجتمع بحماية معلوماته الخاصة بالخدمات المالية، والمستشفيات، ومؤسسات الرعاية الصحية الأخرى، ومحطات الطاقة، وغيرها.
- وقد أصبحت الهجمات السيبرانية متطورة بمستوى يتفوق على قدرات وسائل الحماية التقليدية التي أصبحت ضعيفة أمام التهديدات المنفذة بواسطة خوارزمياتٍ الذكاء الاصطناعي، وأصبح الذكاء الاصطناعي في عالم اليوم سلاحا ذو حدين، فعاي الجانب السلبي، يمكن للمجرمين استخدام الذكاء الاصطناعي في دعم هجماتهم الذكية للإضرار بالمنظمات، وعلى الجانب الإيجابي، توجهت العديد من المنظمات والهيئات لتعزيز الأمن السيبراني بتقنيات وأدوات الذكاء الاصطناعي بهدف مواكبة مستويات المخاطر المحتملة وتحقيق الحماية الشاملة.
- استنادا لنظرية نشر الأفكار المستحدثة، اختبرت الدراسة الحالية فاعلية استخدام الهيئة الوطنية للأمن السيبراني بالمملكة العربية السعودية لتقنيات الذكاء الاصطناعي كتوجه مستقبلي، واتجاهاتهم نحو تلك التقنيات كبديل للعنصر البشرى في ظل ما أثارته ثورة الذكاء الاصطناعي من جدل واسع حول التأثيرات الإيجابية والسلبية لها على مستقبل الأمن السيبراني، وكذلك استفادتها من تلك الثورة، ورصد العوامل المؤثرة على مدى نجاح استخدام تقنيات الذكاء الاصطناعي في الهيئة الوطنية للأمن السيبراني، بالإضافة إلى تحديد الملامح المستقبلية لهذا الاستخدام.

- طبقت الدراسة على عينة عشوائية بسيطة قوامها (١٠٦) مفردة من المسؤولين (العاملين) بالهيئة الوطنية للأمن السيبراني، من ذوي سنوات الخبرة والأعمار المختلفة، لرصد التأثيرات المتوقعة لفاعلية استخدام تقنيات الذكاء الاصطناعي في الهيئة، في ضوء ظهور مؤشرات عديدة للاستغناء عن العنصر البشرى والاعتماد على الآلة في مجالات متعددة في الأمن السيبراني، والتعامل مع البيانات الضخمة والعملات الرقمية والربوتات وغيرها.
- وأظهرت النتائج وجود علاقة دالة إحصائيًا بين الفائدة المتوقعة من استخدام تقنيات الذكاء الاصطناعي في الهيئة الوطنية للأمن السيبراني، وبين درجة نجاح هذا الاستخدام، كما أظهرت النتائج أيضا وجود علاقة دالة إحصائيًا بين إدراك المبحوثين لدور تقنيات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية، وبين اتجاهاتهم نحو دورها في دعم وتعزيز الأمن السيبراني.
- ثبت وجود فروق ذات دلالة احصائية بين المبحوثين في مدى فاعلية توظيف تقنيات الذكاء الاصطناعي بالهيئة الوطنية للأمن السيبراني وفقا النوع، وسنوات الخبرة، في حين لم تثبت أي فروق وفقا للسن.
- أوضحت نتائج الدراسة أن أعلى نسبة إجابة كانت من نصيب المبحوثين الذين يهتمون بتقنيات الذكاء الاصطناعي دائما، حيث أكدوا على أن السيناريو المرجعي (الثبات) هو السيناريو الأكثر ترجيحا لتبني تقنيات الذكاء الاصطناعي في المستقبل، ويمكن تفسير ذلك، كانعكاس حقيقي وملموس للواقع الذي يعايشه العالم اليوم لتطبيقات الذكاء الاصطناعي حيث لوحظ أن معظم الخدمات ارتبطت بالتعامل مع البيانات الضخمة، والأدوات الأكثر ذكاءا.
- وجاء معرفة عينة الدراسة بتقنيات الذكاء الاصطناعي، بدرجة متعمقة بنسبة كبيرة، ويمكن للدراسة الحالية تفسير ذلك بناء على أوجه تقنيات الذكاء الاصطناعي المنتشرة، والمتمثلة في تقنيات الترجمة الآلية للغات الأخرى، واستخدام الروبوت، واستخدام الـ BOTS الدردشة الآلية للرد على استفسارات، وتعلم الآلة، وأمن الشبكات، وغيرها.
- وأوضحت النتائج كذلك ارتفاع معدل تعرض المبحوثين لتقنيات الذكاء الاصطناعي، حيث دمجت تقنيات الذكاء الاصطناعي بشكل متزايد في أماكن العمل عبر مختلف المجالات، ولها تأثير يُعتقد أنه سيكون كبيراً على عمليات إنتاجها، حيث يساعد على تحسين الكفاءة وخفض التكاليف وتعزيز الدقة.
- جاء دافع قدرة تقنيات الذكاء الاصطناعي على التعامل مع عدد كبير من البيانات في المرتبة الأولى من حيث دوافع اعتماد أفراد العينة على تقنيات الذكاء الاصطناعي في المستقبل، حيث يبسط الذكاء الاصطناعي من عملية تحليل البيانات الضخمة من خلال أتمتة وتعزيز مهام تحضير البيانات، بالإضافة إلى تصوير البيانات والنماذج التنبؤية وغيرها من مهام

تحليلية أخرى معقدة تستهلك الكثير من الوقت والموارد البشرية والأموال، كما يساعد الذكاء الاصطناعي المستخدمين على العمل مع رؤى قابلة للتنفيذ ومعالجتها وإبرازها بشكل أسرع من خلال معالجة مجموعات البيانات الضخمة المعقدة، وبفضل تقنيات الذكاء الاصطناعي المتطورة أصبحت تحليلات البيانات: أكثر كفاءة بفضل الأتمتة - يمكن الوصول إليها بشكل أكبر بفضل تحسين واجهة المستخدم - أكثر قوة، حيث أصبح بالإمكان تحليل النصوص والفيديوهات بسهولة؛ وهو ما لم يكن متاحًا من قبل.

- بينت النتائج أن نسبة كبيرة من عينة الدراسة أظهروا ثقتهم بدرجة كبيرة في تقنيات الذكاء الاصطناعي في مجال الأمن السيبراني، فكان أحد أهم مجالات التحول السيبراني في عام ٢٠٢٢، وما قبله، هو إدراك العديد من الدول والمؤسسات، بأن القدرات السيبرانية باتت مجالًا مهمًا لممارسة النفوذ وتحقيق التفوق والتنافس، حيث لم تعد ترسانات الأسلحة التقليدية هي المعيار الأساسي لقياس القوة الشاملة للدولة، بعد الثورة الصناعية الرابعة وما صاحبها من تجليات الذكاء الاصطناعي، وفي هذا الإطار قامت العديد من الدول بوضع سياسات واستراتيجيات وطنية لمواكبة قفزات التطور في الثورة الصناعية الرابعة، لاسيما بعد تصاعد الصراعات الدولية في الفضاء السيبراني التي باتت جزءًا لا يتجزأ من التفاعلات الدولية مع تنامي معدلات الهجمات والمخاطر الإلكترونية بشكل لافت للنظر.
- أشارت نتائج الدراسة إلى تعدد مجالات توظيف تقنيات الذكاء الاصطناعي في الهيئة الوطنية للأمن السيبراني، وفقا لما أجاب به مسؤولي الهيئة عينة الدراسة، وتمثلت أولى هذه المجالات في أمن الشبكات، الذى هو عبارة عن نشاط يتم تصميمه لحماية استخدام وسلامة الشبكة (الخاصة – العامة) والبيانات، ويشمل هذا المجال كلا من تكنولوجيا الأجهزة والبرمجيات، ويدير أمن الشبكات الفعال إمكانية الوصول إلى الشبكة ويستهدف مجموعة متنوعة من التهديدات ويمنعها من الانتشار.
- وجاء التلاعب في المعلومات واتلافها في مقدمة الجرائم الإلكترونية المنتشرة، حيث أدت ثورة المعلومات والاتصالات إلى ظهور جريمة الاحتيال الإلكتروني، حيث أحدثت تغيرات جذرية ونوعية في مختلف مناحي الحياة الاقتصادية والسياسية والقانونية، وأدت الثورة المعلوماتية إلى ظهور من يسيء استخدام الأنظمة المعلوماتية بشكل غير مشروع، ما أدى إلى ظهور فضاء الجرائم الإلكترونية المعلوماتية وبالأخص جريمة الاحتيال الإلكتروني، ويهدف البروتوكول السعودي إلى ضبط وتنظيم المعاملات والتوقيعات الإلكترونية وتوفير إطار تنظيمي لها بما يؤدي إلى وضع قواعد تنظيمية موحدة لاستخدام المعاملات والتوقيعات الإلكترونية ،وتسهيل تطبيقها في القطاعين العام والخاص من خلال سجلات إلكترونية موثوقة، كما تشمل طرق حماية المعلومات الدخول غير المشروع إلى

المواقع الإلكترونية والأجهزة الإلكترونية، والحصول غير الشرعي على معلومات منها، أو استبدال تلك المعلومات بأخرى.

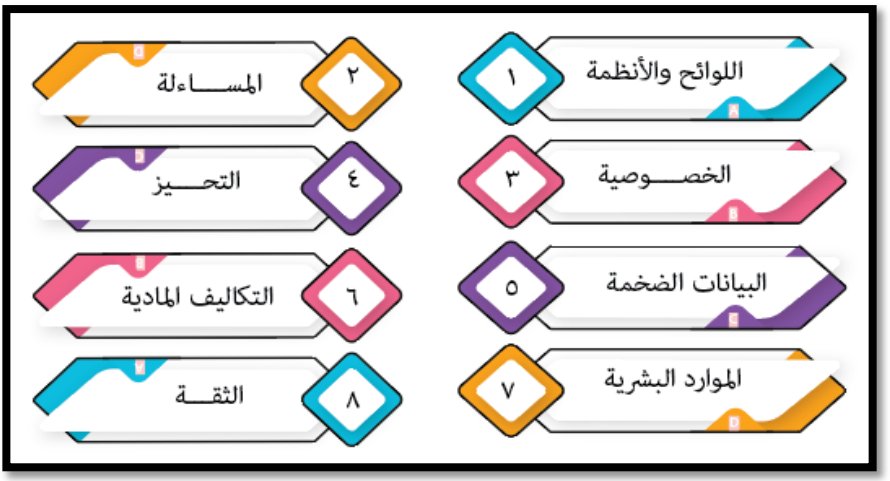
- كما أكدت النتائج على دور الذكاء الاصطناعي في مكافحة الجرائم الالكترونية، حيث جاء تحليل الشبكات والوصول إلى حركات المرور الخاصة بالويب في مقدمة أدوار الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية، حيث تعد التهديدات الأمنية الإلكترونية أكثر التحديات التي تواجهها الأجهزة الأمنية، ويشكل استخدام أحدث تقنيات الحماية المعقدة وتعزيز أنظمة البنية التحتية لأمن المعلومات أزمة كبيرة على الاقتصاد لما تكلفه من مبالغ ضخمة، ويعتبر حجم الاستثمار في أمن المعلومات ومكافحة الجرائم الإلكترونية من أهم اولويات الحكومات في مختلف دول العالم، لذا يجب أن يكون هناك العديد من الاستراتيجيات لحمياتها وحماية مختلف شبكاتها من التهديدات الحقيقية لأمن المعلومات، إضافة لذلك أن المخاطر الإلكترونية تتغير باستمرار والجرائم الإلكترونية تتسم بطابع دولي، من هنا تظهر الحاجة إلى بناء أنظمة ذكية مبنية على تقنيات الذكاء الاصطناعي و منهاجياتها لتدعم عمليات التحكم و المراقبة و اتخاذ القرارات الدقيقة من قبل الخبراء و دعم عمليات إدارة أمن المعلومات و اكتشاف عمليات التلاعب و التجسس، والتشفير وكافة أشكال الجرائم الإلكترونية الأخرى.
- كشفت النتائج عن درجة نجاح استخدام تقنيات الذكاء الاصطناعي في الهيئة الوطنية للأمن السيبراني من وجهة نظر المبحوثين، وذكروا في المقدمة التعامل مع البيانات الضخمة، حيث تعد البيانات الضخمة هي الوقود الذي تعمل به الذكاء الاصطناعي، فكمية البيانات الضخمة المتنوعة هي ما تمكن تطبيقات التعلم الآلي من اكتساب وإتقان المهارات، و كلما كانت كمية البيانات المتاحة أكبر للذكاء الاصطناعي، كلما تمكن من تعلم وتحسين قدراته على التعرف على الأنماط، كما أصبحت تحليلات البيانات أكثر قوة، فأصبحت المؤسسات الآن تعتمد على التعلم الآلي، واستخدام التقنيات الإحصائية لتمكين أجهزة الكمبيوتر من تحديد وتعلم الأنماط في البيانات المعينة، بدلا من أن تتم برمجتها بشكل صريح لوظيفة معينة.
- أشارت نتائج الدراسة الحالية إلى أبرز أدوار الأمن السيبراني المعتمدة على الذكاء الاصطناعي، حيث جاء في بدايتها رفع مستوى الوعي بمخاطر أمن المعلومات، حيث أصبح أمن المعلومات السيبراني (الإلكتروني) في العصر الحاضر من أهم المواضيع الأكثر نقاشًا في الأوساط الأكاديمية والحكومية والصناعية لما يتعلق به من مخاطر متعددة تهدد مختلف المؤسسات والقطاعات التي أصبحت اليوم متصلة بالشبكة العنكبوتية العالمية (الانترنت)، وأوضحت العديد من الدراسات والأبحاث أن كثير من التهديدات والاختراقات المعلوماتية تأتي من داخل المنشأة بسبب ضعف الوعي بأمن المعلومات لدى كثير من الموظفين الذين يعتبرون الحلقة

الأضعف في النظام المعلوماتي حتى مع وجود أنظمة الحماية المتطورة، ومن ثم يستغل المهاجمون المحترفون هذه الثغرة لاختراق الأجهزة، والوصول إلى الشبكة، ثم التمكن من سرقة البيانات، أو تدمير الأنظمة المعلوماتية الحساسة.

- كما أوضحت النتائج اتجاهات المبحوثين نحو تقنيات الذكاء الاصطناعي ودورها في اكتشاف حالات الاختراق الشاذة داخل الشبكات بشكل أسرع من البشر، وهي ما يطلق عليها قرصنة الشبكات اللاسلكية War Driving والتي تعد اختراق للشبكات اللاسلكية أي بدون تصريح أو دراية لصاحب الشبكة، لأسباب كثيرة لا يقوم أصحاب تلك الشبكة بحمايتها، إما عن جهل أو إهمال، وفي أحوال أخرى تكون أساليب الحماية بدائية سهلة الكسر، ما يسهل تسلل أي شخص على دراية بكيفية الولوج، من التطفل واستغلال المعطيات والثغرات والمعلومات المتوفرة على الشبكة، ومن ثم أصبح لتقنيات الذكاء الاصطناعي دورا كبيرا في اكتشاف مثل تلك الحالات.
- كشفت النتائج عن الفائدة المتوقعة من استخدام تقنيات الذكاء الاصطناعي في الهيئة الوطنية للأمن السيبراني من وجهة نظر المبحوثين، فذكروا في البداية الاسهام في التخطيط الأمني على كافة أنحاء المملكة، حيث سعت المملكة إلى وضع إستراتيجية البرمجيات الحكومية الحرة ومفتوحة المصدر، والتي تعمل على تعزيز الريادة في التقنيات المستقبلية، وتحويل مشهد الإنفاق على تقنية المعلومات، وبناء منظومة "المحيط الأزرق" للتقنيات الحديثة، وتهدف إلى تحفيز إنشاء المؤسسات التي يمكنها بناء قيمة مستدامة آمنة للمملكة، والمساهمة في الاقتصاد الرقمي الآمن، وتشجيع تطوير منتجات البرمجيات، وبناء منصات تقنية آمنة ومستدامة وعالية القيمة.

- **ثانيا: توصيات ومقترحات الدراسة:**

- تنمية وتطوير الكفاءات العلمية المتخصصة والقدرات المحلية في مجال الذكاء الاصطناعي، وخلق ثقافة الذكاء الاصطناعي لدى فئات المجتمع لتسهيل انتشار استخدام التطبيقات التي تعتمد على هذه التقنيات وخلق المواطن الرقمي القادر على التعامل معها، وتعزيز تضافر جهود المؤسسات الحكومية والتعليمية والإعلامية للتوعية بأساسيات هذا المجال، مع إطلاق استراتيجية خاصة بتقنيات الذكاء الاصطناعي.
- تكثيف البرامج التوعوية الموجهة لأفراد المجتمع، ورفع الوعي بالمخاطر والتهديدات الأمنية، والتعريف بأفضل الممارسات الكفيلة بجعل الذكاء الاصطناعي بيئة آمنة الاستخدام، لا سيما في مجال مكافحة الجرائم وتعزيز الأمن السيبراني.
- ضرورة وضع أولوية خاصة لكيفية معالجة تحديات الأمن السيبراني المعتمدة على تقنيات الذكاء الاصطناعي، والمتمثلة في:



شكل (٣) يوضح تحديات الأمن السيبراني المعتمدة على تقنيات الذكاء الاصطناعي

- توحيد الجهود الوطنية والمبادرات الخاصة في البيانات والذكاء الاصطناعي والأمن السيبراني على كافة الأصعدة، ويكون ذلك ضمن توجه وطني لتحقيق الاستفادة المثلى، ومن هذا المنطلق لابد من توحيد جهود الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) مع الهيئة الوطنية للأمن السيبراني.
- تطوير القوى العاملة في الهيئة الوطنية للأمن السيبراني ببناء مورد مستدام للكفاءات الوطنية في مجال تقنيات وتطبيقات الذكاء الاصطناعي.

شكر وتقدير: تم تمويل هذا المشروع من قبل عمادة البحث العلمي (DSR) جامعة الملك عبد العزيز، جدة – السعودية تحت منحة رقم (IFPAS: 56-848-1443)، كما يتقدم الباحثان بالشكر لعمادة البحث العلمي على الدعم التقني والمادي للبحث.

• مراجع الدراسة:

١- الفتلاوي، ماجد جبار غزاي، والأعسم، حسن علاء محمد جواد. (٢٠٢٢). اسهامات تقنيات الذكاء الاصطناعي في الريادة الاستراتيجية: دراسة وصفية تحليلية في مطار النجف الأشرف الدولي ٢٠٢١، *مجلة الغري للعلوم الاقتصادية والإدارية، مج ١٨ ، ع ١*، ١٥٧ – ١٧٩.

٢- عبد الرازق، مي مصطفى. (٢٠٢٢). تقنيات الذكاء الاصطناعي في الإعلام: الواقع والتطورات المستقبلية: دراسة تطبيقية على القائمين بالاتصال بالوسائل الإعلامية المصرية والعربية.المجلة المصرية لبحوث الإعلام، ع٨١، ص ١- ٧٤

٣- سالم، دعاء فتحى (٢٠٢١). فاعلية استخدام تقنيات الذكاء الاصطناعي في مواقع التواصل الاجتماعي من وجهة نظر طلاب الإعلام التربوي: الفيس بوك أنموذجا، المجلة المصرية لبحوث الرأي العام، ج١، ع ٣، ص ١-٦١.

3- Anja Buchmann, Geoffrey C Bowker, Unsupervised by any other name: Hidden layers of knowledge production in artificial intelligence

on social media, Big Data & Society/ January–June 2019/pp1-11, Published IN
inhttps://journals.sagepub.com/doi/full/10.1177/2053951718819569# □
4-Vimala Nunavath ;Morten Goodwin, The Role of Artificial Intelligence in Social Media Big data Analytics for Disaster Management -Initial Results of a Systematic Literature Review, Publisher: IEEE.□
Published in: **2018 5th International Conference on Information and Communication Technologies for Disaster Management (ICT-DM)**
5- Purva Grover, Arpan Kumar Kar & Yogesh K. Dwivedi/ Annals, Understanding artificial intelligence adoption in operations management: insights from the review of academic literature and social media discussions, 16 June 2020.
Published in **https:// link.springer.com/article/10.1007/s10479-020-03683-9**□
6- Luis Fernandez-Muhammad Imran, Humanitarian health computing using artificial intelligence and social media: A narrative literature review, International Journal of Medical Informatics, Vol 114, June 2018, P. 136-142/Google Scholar.
https://www.sciencedirect.com/science/article/abs/pii/S1386505618300212?via%3Dihub.
7- Amir Hussain,Aziz Sheikh, Opportunities for Artificial Intelligence–Enabled Social Media Analysis of Public Attitudes Toward Covid-19 Vaccines, February 5, 2021.
https://catalyst.nejm.org/doi/full/10.1056/CAT.20.0649.
8- Bhavani Thuraisingham, The Role of Artificial Intelligence and Cyber Security for Social Media, Publisher: IEEE.
Published in: 2020 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW), Conference on New Orleans, LA, USA.
9- Feyza AltunbeyOzbay, BilalAlatas, Fake news detection within online social media using supervised artificial intelligence algorithms, Vol.540, 15 February 2020, 123174Google Scholar/Elsevier/pp.1-17.
https://www.sciencedirect.com/science/article/abs/pii/S0378437119317546?via%3Dihub.
10- F.A.H. Ambreen, Varsha D. Jadhav, Novel Model for Detection of Cyber-Aggressive Comments on Social Media Platforms a Review, Publisher: IEEE.
Published in: 2020 International Conference on Aurangabad, India, on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC)
11- Rana Mohamed Eisa, Merna Labib; Amr ElMougy, SOS: Save Our Social Network Accounts, Publisher: IEEE, Published in:

2019 International Conference on Herlany, Slovakia, Symposium on Applied Machine Intelligence and Informatics (SAMI)

١٢- البابلي، عمار ياسر محمد زهير. (٢٠٢٠). توظيف تقنيات الذكاء الاصطناعي في العمل الأمني: دراسة تطبيقية "الشرطة التنبؤية – أزمة فيروس كورونا بووهان الصينية". مجلة الأمن والقانون، مج ٢٨ ، ع ١، ٣ – ٨٦

١٣- دولي، لخضر، وناصري، نفيسة. (٢٠١٨). دور الذكاء الاصطناعي في مواجهة الجرائم الإلكترونية. مجلة المؤشر للدراسات الاقتصادية، مج ٢، ع ٢، ٥٢ – ٦٧.

١٤- سعيدي خليل .بن مهدي مرزوق (٢٠٢٢). الذكاء الاصطناعي كتوجه حتمي في حماية الامن السيبراني (واقع اليوم ورهان الغد)، مجلة السلام للعلوم الإنسانية و الاجتماعية، مج٦،ع١، ص٢٥-٣٧.

١٥- الخضري، جيهان سعد محمد، سلامي، هدى جبريل علي، كليبي، نعمة ناصر مدبش(٢٠٢٠). الأمن السيبراني والذكاء الاصطناعي في الجامعات السعودية: دراسة مقارنة، مجلة تطوير الأداء الجامعي، جامعة المنصورة - مركز تطوير الأداء الجامعي، مج١٢، ع١، ص ٢١٧ -٢٣٣

١٦- العدوان، جعفر أحمد عبد الكريم(٢٠٢٢).أدوار وتحديات الأمن السيبراني المعتمد على الذكاء الاصطناعي: دراسة حالة، المجلة الأردنية في إدارة الأعمال، الجامعة الأردنية ، عمادة البحث العلمي، مج١٨، ع٣، ص ٤٣٧ - ٤٥٦

١٧- أحمد، فاطمة علي إبراهيم، ويوسف، رحاب فايز أحمد، والسيد، وليد محمود (٢٠٢٢) .(الأمن السيبراني والنظافة الرقمية. المجلة المصرية لعلوم المعلومات، مج٩ ،ع٢ ،٣٩٠ - ٤٢٢

١٨- بن برغوث، ليلي. (٢٠٢٣) الأمن السيبراني وحماية خصوصية البيانات الرقمية في الجزائر في عصر التحول الرقمي والذكاء الاصطناعي: التهديدات، التقنيات، التحديات، وآليات التصدي، المجلة الدولية للاتصال الاجتماعي، مج١٠ ،ع١ ،٤٤٣ - ٤٥٧

١٩- الدمرداش، نانسي صابر (٢٠٢٢). أثر تفاعل العناصر الافتراضية المدعومة بالذكاء الاصطناعي وأدوات إدارة المعرفة في تنمية مهارات الأمن السيبراني وحل المشكلات لدى طلاب الحاسبات والذكاء الاصطناعي، مجلة البحوث في مجالات التربية النوعية، جامعة المنيا - كلية التربية النوعية، ع٤١، ص ١٣٣١ – ١٤٢٧

٢٠- عبد العزيز، سوزي محمد رشاد (٢٠٢٢). التهديدات الأمنية الهجين في العلاقات الدولية: السيبرانية والذكاء الاصطناعي نموذجا، مجلة وادي النيل للدراسات والبحوث الإنسانية والاجتماعية والتربوية، جامعة القاهرة - فرع الخرطوم - كلية الآداب، مج٣٣، ع٣٣، ص ٦٦٣ – ٧٠٠

٢١- الداغر، مجدي محمد عبد الجواد (٢٠٢١). اتجاهات النخبة نحو توظيف الإعلام الأمني لتطبيقات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية وانعكاساته على دعم وتعزيز الأمن السيبراني في مصر: دراسة ميدانية، المجلة العربية لبحوث الإعلام والاتصال، جامعة الأهرام الكندية، ع٣٣، ص ٤ - ١١٠

٢٢- الزهراني، عبد الله بن يحي، والشهري، حسن بن أحمد(٢٠٢٠). استراتيجيات الأمن السيبراني في ضوء التقنيات والتحديات الحديثة: دراسة مقارنة، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، كلية العلوم الاستراتيجية.

23-Verma, M. **Artificial intelligence and its scope in different areas** with special reference to the field of education, Artificial intelligence,3(1), p.6.

24- B.J. Copeland, "Artificial intelligence", **www.britannica.com**, Retrieved 7-10-2019.

٢٥- فؤاد، نيفين فاروق(٢٠١٢). الآلة بين الذكاء الطبيعي والذكاء الاصطناعي: دراسة مقارنة، **مجلة البحث العلمي في الآداب**، مج٣، ع.١٣، ص ٤٨١: ٥٠٤.

26- Types of Artificial Intelligence, **www.javatpoint.com**, Retrieved 7-10-2019

٢٧- آل سعود، سارة (٢٠١٧) . التطبيقات التربوية للذكاء الاصطناعي في الدراسات الاجتماعية، **مجلة البحث العلمي في الآداب**، مج ٣، ع٣، ص١٣٣-١٦٣

28- Shi Dong, Ping Wang, Khushnood Abbas,(2021) A survey of Deep Learning and Its Applications: A New paradigm to Machine Learning Archives of Computational Methods in Engineering,p.1, Computer Science Review,Volume 40, https://doi.org/10.1016/j.cosrev.2021.100379

29- Ling Jin,(2019) Investigation on Potential Application of Artificial Intelligence in Preschool Children's Education, Journal of Physics Conference ,(Vol.1288.No.1.P.2)

30- Katharine Gammon,(2019) "5 Ways Artificial Intelligence Will Change the World by 2050, news.usc.edu, www.javatpoint.com.

31- https://www.nca.gov.sa/about.

32- https://www.nca.gov.sa/strategic

٣٣- العقاري، محمد على (٢٠١٩). **نظريات الاتصال: رؤى فلسفية وتطبيقات عملية**، الرياض، ط١، مكتبة الرشد، ص١٠٤.

٣٤- المشاقبة، بسام عبد الرحمن(٢٠١٥). **نظريات الاتصال**، الأردن، ط١، دار أسامة للنشر والتوزيع، ص ١٧٧.

35- Celeste Bishop Stein, The Future of the Newsroom in the Age of New Media: A Survey on Diffusion of Innovations in American Newsrooms, unpublished dissertation Doctorate, **School of Communication and the Arts**, Regent University,2019, pp.48-58.

-(https://maaal.com/archives/202008/152287/)

٣٦- القحطاني، عبد المحسن عايض(٢٠١٨). **تصميم البحوث: الكمية – النوعية – المزجية**، دار المسيلة للنشر والتوزيع، ص ٢٧٩

٣٧- (تقرير IBM Cost of Data Breach 2021)

٣٨- عبد الرازق، رانا مصباح عبد المحسن (٢٠٢١). تأثير الذكاء الاصطناعي على الجريمة الإلكترونية، المجلة العلمية لجامعة الملك فيصل - العلوم الإنسانية والإدارية، مج٢٢ ،ع١ ،ص ٤٣٣.

◆◆◆السادة محكمي الاستبانة:

أ.د/ جيهان يسري. الأستاذ بقسم الإذاعة والتليفزيون/ كلية الإعلام جامعة القاهرة، وعميدة كلية الإعلام سابقا

أ. د/ السيد عزت. أستاذ الإعلام/ كلية التربية النوعية جامعة المنصورة.

أ.م. د/ خلود ملياني. أستاذ الإعلام المشارك بكلية الاتصال والإعلام جامعة الملك عبد العزيز، ووكيلة كلية الاتصال والإعلام.