المجلة الأردنية في إدارة الأعمال، المجلّد **18**، العدد **3**، **2022**
DOI: https://doi.org/10.35516/jjba.v18i3.196

Roles and Challenges of AI-Based Cybersecurity: A Case Study

Jaffar Ahmad Abdulkarim Alalwan [1]

ABSTRACT

Nowadays, organizations face complex cyber-attacks that are difficult to counter with traditional protections. Therefore, many modern organizations tend to use AI-based cybersecurity systems to secure their assets and infrastructure and to reduce the level of potential risks.

Because of the lack of clarity of the AI roles in cybersecurity and the ambiguity of the related challenges, this study aims to explore the most prominent roles of AI-based cybersecurity related to information security in the prevention phase, the detection phase and the response phase. The study also aims to determine the most prominent challenges facing AI-based cybersecurity.

To achieve the goals of this study, we adopt a case-study methodology that origins from the general framework which is information security and ends with the specific framework which is AI-based cybersecurity. After designing a matrix to analyze the case study, the study concludes nine important roles for AI-based cybersecurity distributed over the three phases. Three roles are in the prevention phase, which are automated assessment of security vulnerabilities, awareness and training and authentication. Two roles are in the detection phase; namely, detection of intrusion and security breaches and detection of spams and phishing and four rules are in the response stage, which are analyzing malware, automating routine tasks, deploying traps and topple attackers and isolating important assets.

The study also identifies eight elements that represent the most prominent challenges facing AI-based cybersecurity: regulations and principles, trust, accountability, privacy, bias, training datasets, human resources and financial costs. In conclusion, the study presents a set of recommendations drawn from the results.

Keywords: Cybersecurity, Artificial intelligence, Accountability, Bias, Intrusion detection.

1 Associate Professor, Institute of Public Administration, Dammam, Kingdom of Saudi Arabia. alwanj@ipa.edu.sa

Received on 14/12/2020 and Accepted for Publication on 12/4/2021.

أدوار وتحديات الأمن السيبراني المُعتمد على الذكاء الاصطناعي: دراسة حالة

***جعفر أحمد عبد الكريم العلوان*[1]**

ملخص

تواجه المنظمات في عصرنا الحديث هجمات إلكترونية مُعقدة تصعب مواجهتها بوسائل الحماية التقليدية. ولذلك تتجه الكثير من المنظمات المعاصرة لاستخدام أنظمة الأمن السيبراني المُعتمد على الذكاء الاصطناعي لتأمين أصولها وبنيتها التحتية وتقليل مستوى المخاطر المحتملة.

ونظراً لعدم وضوح أدوار الذكاء الاصطناعي في الأمن السيبراني وغموض التحديات التي تواجهها، هدفت هذه الدراسة لاستكشاف أبرز أدوار الأمن السيبراني المُعتمد على الذكاء الاصطناعي المنبثقة من أمن المعلومات والمرتبطة بمرحلة الوقاية ومرحلة الاكتشاف ومرحلة الاستجابة. كذلك هدفت الدراسة لمعرفة أبرز التحديات التي تواجه الأمن السيبراني المُعتمد 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 المُعتمد على الذكاء الاصطناعي. وبعد تصميم مصفوفة لتحليل دراسة الحالة، توصلت الدراسة إلى وجود تسعة أدوار هامة للأمن السيبراني المُعتمد 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 تُمثل أبرز التحديات التي تواجه الأمن السيبراني المُعتمد على الذكاء الاصطناعي، وهي: اللوائح والأنظمة، والثقة، والمساءلة، والخصوصية، والتحيز، ومجموعات البيانات التدريبية، والموارد البشرية، والتكاليف المالية. وفي الختام، قدمت الدراسة بعضاً من التوصيات المستخلصة من النتائج.

الكلمات الدالة: الأمن السيبراني، الذكاء الاصطناعي، المساءلة، التحيز، كشف التسلل.

المقدمة

مع التطورات المتسارعة في تقنيات المعلومات والاتصالات، تواجه منظمات اليوم هجمات سيبرانية متطورة تستهدف بياناتها وأصولها الثمينة. وتتسم هذه التهديدات الجديدة بظهورها المستمر وقدرتها على تصميم هجمات يمكنها التحايل على وسائل الحماية المعروفة والتغلب على سيناريوهات الاستجابة التقليدية. ونظراً لقلة مرونة أنظمة الحماية الأمنية التقليدية، فإن قدراتها على التغير والتكيف آلياً وفقاً للتغيرات المحيطة بها تكون محدودة وبطيئة وغير كافية حتى مع وجود التفاعل البشري (Jean-Philippe, 2018; Rehman and Saba, 2014).

لقد أصبحت الهجمات السيبرانية متطورة بمستوى يتفوق على قدرات وسائل الحماية التقليدية التي أصبحت ضعيفة أمام التهديدات المُنفذة بواسطة خوارزميات الذكاء الاصطناعي. وفي الواقع، أصبح الذكاء الاصطناعي في مجال الأمن السيبراني سلاحاً ذا حدين. فعلى الجانب السلبي، يمكن للمجرمين استخدام الذكاء الاصطناعي في دعم هجماتهم الذكية للإضرار بالمنظمات وتحقيق أهدافهم الدنيئة. وعلى الجانب الإيجابي، توجهت الكثير من المنظمات لتعزيز الأمن السيبراني بأدوات

1 أستاذ إدارة الأعمال المشارك، معهد الإدارة العامة، الدمام، المملكة العربية السعودية. alwanj@ipa.edu.sa; alwanj1@gmail.com

تاريخ استلام البحث 2020/12/14 وتاريخ قبوله 2021/4/12.

الذكاء الاصطناعي بهدف مواكبة مستويات المخاطر المُحتملة وتحقيق الحماية الشاملة. على سبيل المثال، تُشير إحدى الدراسات الحديثة التي تضمنت 850 من رؤساء الأمن السيبراني وأمن تقنية المعلومات في عشر دول مختلفة إلى ضرورة تصميم دفاعات الأمن السيبراني بواسطة الذكاء الاصطناعي؛ لأن مهاجمي الإنترنت يستخدمون هذه التقنية في الوقت الحالي. وقد أشار 75% من المشاركين في هذه الدراسة إلى أن الذكاء الاصطناعي يُتيح لمنظماتهم الاستجابة للخروقات بشكل أسرع (Capgemini Research Institute, 2019).

إن الأهمية البالغة لموضوع الأمن السيبراني المُعتمد على الذكاء الاصطناعي تدل على وجود أدوار فاعلة تقوم بها هذه التقنيات لدعم الحماية الأمنية للمنظمات. إضافة إلى ذلك فإن تبني التقنيات الحديثة يصاحبه في الغالب عدة تحديات يمكن أن تؤثر على كفاء التقنيات الحديثة وفاعليتها. ونظراً لعدم وضوح كل من الأدوار والتحديات وغموضها، تهدف هذه الدراسة لتكون خطوة أولية لاستكشاف أبرز أدوار وتحديات الأمن السيبراني المُعتمد على الذكاء الاصطناعي.

مشكلة الدراسة

أثبتت أنظمة الحماية التقليدية في مجال أمن المعلومات، كأنظمة كشف التسلل (Intrusion Detection Systems)، أنها أدوات مهمة للأمن السيبراني. وتتمثل مواصفاتها المرغوبة في الأداء المثالي، والحماية القصوى، وتقليل الأخطاء. وبالرغم من أهميتها، يعتقد بعض الباحثين أنها لم تعد قادرة على الوفاء بهذه المتطلبات نظراً لمُعدل اكتشاف الهجمات المُنخفض، والإنتاجية البطيئة، ومحدودية مرونتها، وصعوبة أتمتتها (Ravi and Ramachandran, 2020). إن عدم الدقة في تحديد الأنماط الطبيعية أو غير الطبيعية لسلوك الشبكة والنظام قد يؤدي إلى معدل اكتشاف منخفض في نظام كشف التسلل، كما أن التغير المستمر لبيئة الشبكة تجعل من هذه المهمة أكثر تعقيداً. ويمكن أن تؤدي الأخطاء في تحديد الأنماط غير الطبيعية إلى معدلات اكتشاف سلبية خاطئة بحيث لا يتم اكتشاف الأنشطة الإجرامية على الشبكة في الوقت المناسب بسبب افتراض أن سلوك الشبكة غير إجرامي. وفي المقابل، فإن التعريف الخاطئ للأنماط الطبيعية يمكن أن يؤدي إلى معدلات اكتشاف موجبة خاطئة، مما يؤدي إلى تصنيف أنشطة الشبكة غير الاجرامية على أنها أنشطة إجرامية.

وفي مقابل نُقاط الضعف المُحتملة في أنظمة الحماية التقليدية، تؤكد الأدبيات أنه بإمكان أنظمة الذكاء الاصطناعي تحسين الأداء الأمني وتقديم حماية أفضل ضد التهديدات المتزايدة، وذلك مع التطور الملحوظ في آليات تعلم الآلة والشبكات العصبية الاصطناعية، وشبكات الحوسبة السحابية الموزعة، والنمو المُطرد في القدرات الحاسوبية، والبيانات الضخمة القادرة على تدريب نُظم تعلم الآلة. على سبيل المثال، أثبتت بعض الدراسات فاعلية الذكاء الاصطناعي وتفوقه على وسائل الحماية التقليدية في التحليل الآلي للثغرات الأمنية (Feng et al., 2014)، واكتشاف الاختراقات الأمنية(Bisio et al., 2017)، وعزل الأصول الهامة (Goosen et al., 2018). من جهة أخرى، يُعتبر الذكاء الاصطناعي أداة تساعد مجرمي الإنترنت على تطوير هجماتهم التخريبية. فكما يمكن استخدام الذكاء الاصطناعي لتحديد الهجمات السيبرانية وإيقافها، فإنه يمكن لمجرمي الإنترنت القيام بهجمات سيبرانية معقدة باستخدام أنظمة الذكاء الاصطناعي.

وتتجسد مشكلة هذه الدراسة في شقين؛ الشق الأول يتعلق بعدم وضوح أدوار الأمن السيبراني المُعتمد على الذكاء الاصطناعي في مرحلة الوقاية ومرحلة الاكتشاف ومرحلة الاستجابة. فبالرغم من كثرة الأدبيات التي أبرزت دور الذكاء الاصطناعي في الأمن السيبراني، فإن أغلبها يفتقر إلى التركيز على توضيح هذه الأدوار من خلال النظر في عدسة المراحل الثلاث لأمن المعلومات. أما الشق الثاني لمشكلة الدراسة فيتعلق بعدم وضوح التحديات التي يمكن أن تؤثر سلباً على كفاءة الذكاء الاصطناعي في الأمن السيبراني، حيث تؤكد الأدبيات على أن أدوار التقنيات الذكية وقدراتها محدودة وأنها تواجه الكثير من التحديات التي يمكن أن تُقلل من كفاءة الأمن السيبراني وفاعليته. على سبيل المثال، قد تتضمن البيانات المستخدمة في الخوارزميات نوعاً من التحيز، مما يؤثر سلباً على القرارات الصادرة من هذه الأنظمة الذكية، كما يمكن أن يكون لتحليل البيانات الضخمة المرتبطة بتقنيات الذكاء الاصطناعي والأمن السيبراني أثر سلبي على خصوصية الأفراد والمنظمات. إن معرفة مثل هذه التحديات أمر ضروري لمعالجتها، وبالتالي

ضمان إدارة فاعلة للأمن السيبراني من خلال الذكاء الاصطناعي.

أهداف الدراسة

تهدف هذه الدراسة لتسليط الضوء على أبرز أدوار الأمن السيبراني المعتمد على الذكاء الاصطناعي في مرحلة الوقاية ومرحلة الاكتشاف ومرحلة الاستجابة، كما تهدف الدراسة لمعرفة أبرز التحديات التي يواجهها الأمن السيبراني المُعتمد على الذكاء الاصطناعي.

أسئلة الدراسة

تتسق أسئلة الدراسة مع أهدافها، حيث تركز الدراسة على سؤالين رئيسين. السؤال الرئيسي الأول هو: ما أبرز أدوار الأمن السيبراني المعتمد على الذكاء الاصطناعي؟ وتتفرع من هذا السؤال الأسئلة التالية:

- ما أبرز أدوار الأمن السيبراني المعتمد على الذكاء الاصطناعي في مرحلة الوقاية؟
- ما أبرز أدوار الأمن السيبراني المعتمد على الذكاء الاصطناعي في مرحلة الاكتشاف؟
- ما أبرز أدوار الأمن السيبراني المعتمد على الذكاء الاصطناعي في مرحلة الاستجابة؟

أما السؤال الرئيسي الثاني لهذه الدارسة فهو: ما أبرز التحديات التي يواجهها الأمن السيبراني المُعتمد على الذكاء الاصطناعي؟

أهمية الدراسة

لهذه الدراسة أهمية في الجانبين التطبيقي والعلمي. في الجانب التطبيقي، تتمثل أهمية هذه الدراسة في القاء نظرة على الأدوار المختلفة للأمن السيبراني المُعتمد على الذكاء الاصطناعي في مرحلة الوقاية ومرحلة الاكتشاف ومرحلة الاستجابة. وبالتالي فإن نتائج هذه الدراسة تلفت نظر المسؤولين والمهتمين بهذه التقنيات الذكية إلى الإمكانات المختلفة لتقنيات الذكاء الاصطناعي في الأمن السيبراني في مراحل أمن المعلومات الثلاث. إن مُخرجات هذه الدراسة والأدبيات التي في سياقها والمتمثلة في معرفة الإمكانات الموضوعية للأمن السيبراني المُعتمد على الذكاء الاصطناعي يُمكن أن تُعتبر مُدخلاً هاماً للتفكير في اتخاذ القرار نحو تبني مثل هذه التقنيات الحديثة.

أما الإضافة التطبيقية لهذه الدراسة فتتمثل في تحديد أبرز التحديات التي يواجهها الأمن السيبراني المُعتمد على الذكاء الاصطناعي. إن تحديد مثل هذه التحديات يلفت نظر مُتخذي القرار إلى أهمية تحديات الذكاء الاصطناعي في الأمن السيبراني والنظر إلى قدراتها على أنها تعمل في أُطر معينة وليست بلا حدود. كما يساعد تحديد هذه التحديات في فهمها وتقديم التوصيات العملية لمعالجتها ووضع الاستراتيجيات الملائمة للتعامل معها، وبالتالي رفع كفاء الأمن السيبراني المُعتمد على الذكاء الاصطناعي في المنظمات.

وفي الجانب العلمي، نجد أن قلة من الأدبيات ربطت بين دور أمن المعلومات ودور الذكاء الاصطناعي في الأمن السيبراني والمراحل الثلاث لعمليات أمن المعلومات (مرحلة الوقاية، ومرحلة الاكتشاف، ومرحلة الاستجابة). لذا تتمثل الإضافة العلمية لهذه الدراسة في تحديد دور الأمن السيبراني المُعتمد على الذكاء الاصطناعي من خلال مصفوفة خاصة تربط بين المراحل الثلاث لإدارة أمن المعلومات من جهة، وبين دور أمن المعلومات ودور الأمن السيبراني المعتمد على الذكاء الاصطناعي من جهة أخرى. لذا يؤمل أن تمثل هذه الدراسة إضافة مميزة للجانب المعرفي بشكل عام، وللمكتبة العربية بشكل خاص.

الإطـار النظـري

يستعرض هذا القسم الإطار النظري الخاص بأمن المعلومات والأمن السيبراني، والذكاء الاصطناعي وأبرز تقنياته، والأدبيات ذات العلاقة بالأمن السيبراني المُعتمد على الذكاء الاصطناعي، والأدبيات ذات العلاقة بتحديات الذكاء الاصطناعي في الأمن السيبراني.

أمن المعلومات والأمن السيبراني

يُعتبر أمن المعلومات والأمن السيبراني من أهم قضايا الفضاء السيبراني في عصرنا الراهن (Wu et al., 2018). ويرى بعض الباحثين أن هناك ترادفاً بين مصطلح أمن المعلومات

ومصطلح الأمن السيبراني، بينما يعتقد باحثون آخرون أن هناك اختلافاً بينها. على سبيل المثال، يعتقد البعض أن الاختلاف بين أمن المعلومات والأمن السيبراني هو كالاختلاف بين المفهوم العام والمفهوم الخاص؛ إذ يُنظر للأمن السيبراني على أنه مجموعة فرعية من أمن المعلومات (von Sloms and von Sloms, 2018). ويمكن تعريف أمن المعلومات (Information Security) بأنه "حماية كل من المعلومات ونظم المعلومات من الأعمال غير المصرح بها، كالوصول أو الاستخدام أو الافشاء أو الإخلال أو التعديل أو التدمير، وذلك لضمان التكامل، والخصوصية، والجاهزية" (الموقع الإلكتروني لمدونة قانون الولايات المتحدة الأمريكية). كذلك يمكن تعريفه بأنه "حماية المعلومات المختلفة والأدوات التي تتعامل معها وتعالجها، من منظمة وغرف تشغيل أجهزة وأجهزة ووسائط تخزين وأفراد، من السرقة أو التزوير أو التلف أو الضياع أو الاختراق باتباع إجراءات وسياسات وقائية" (الحميد ونينو، 2007: 37). أما الأمن السيبراني فيمكن تعريفه بأنه "المنهج والإجراءات المرتبطة بعمليات إدارة المخاطر الأمنية التي تتبعها المنظمات والدول لحماية سرية وتكامل وجاهزية البيانات والأصول المستخدمة في الفضاء السيبراني" (Schatz et al., 2017:66).

ويُعتبر أمن المعلومات والأمن السيبراني ركيزة أساسية لأمن المنظمات وجزءاً لا يتجزأ من أمن المجتمع والأمن الوطني للدولة ككل (صادق والفتال، 2019). فعلى مستوى المنظمات، تبرز أهمية خصوصية معلومات الموظفين والمستفيدين، وأهمية سلامة تلك المعلومات من التعديل، ومدى ضمان الوصول للمعلومات في الوقت المطلوب. أما على مستوى المجتمع والدولة، فتؤدي الكثير من الهجمات المرتبطة بأمن المعلومات إلى حدوث أضرار سياسية واقتصادية وخيمة (القحطاني، 1435هـ) (اللوزي، 2010). وتختلف الأدبيات في تحديد مراحل عمليات الأمن السيبراني وأمن المعلومات. فالبعض يعتقد بأن عمليات الأمن السيبراني تتكون من خمس مراحل هي: التحديد، والوقاية، والاكتشاف، والاستجابة، والاستعادة (NIST, 2018)، ويعتقد بعض الباحثين بأن عمليات أمن المعلومات تمر بثلاث مراحل هي: مرحلة الوقاية، ومرحلة الاكتشاف، ومرحلة الاستجابة (La Piedra, 2002; Ahmad et al., 2014).

وتهدف مرحلة الوقاية للحماية الشاملة للأصول المعلوماتية قبل حدوث الهجمات الأمنية. وتهتم هذه المرحلة بوضع سياسات أمن المعلومات التي ينبغي أن تتضمن أهداف أمن المعلومات وأسس توجيه جميع الأنشطة ذات العلاقة بأمن المعلومات. وينبغي أن تكون مسؤوليات المنظمة والموظفين والإدارة واضحة في هذه السياسات؛ بمعنى أن يتم تحديد المسؤوليات العامة والخاصة لإدارة أمن المعلومات وتحديد الأدوار (Abdelwahed et al., 2017). وتهتم هذه المرحلة أيضاً بتثقيف الموظفين بأهمية أمن المعلومات من خلال برامج الوعي بأمن المعلومات. فإذا لم يكن الموظف مدركاً لمسؤوليات أمن المعلومات، فإن ذلك قد يسبب ضرراً كبيراً للمنظمة. وينبغي تقديم التدريب والتعليم المتعلق بإجراءات وسياسات أمن المعلومات في المنظمة، وذلك على أساس دوري (Antonucci, 2017). وتهتم هذه المرحلة كذلك بالتحكم في الوصول الذي يهدف لتقييد الوصول للمعلومات وضمان وصول المستخدم المصرح له فقط إلى النظام والخدمات الإلكترونية ومنع المستخدم غير المصرح له من الوصول (Evans, 2016; Al-Khuri and Al-Qudah, 2006).

وبخصوص مرحلة الاكتشاف، تؤكد أدبيات أمن المعلومات أنه لا يمكن حماية أي نظام إلكتروني حماية كاملة بنسبة 100%؛ بمعنى أنه مهما بالغنا في حماية الأنظمة الإلكترونية تظل هناك نسبة ولو بسيطة لحدوث ثغرة يمكن للمهاجم من خلالها القيام بالهجوم الالكتروني (بانقا، 2019). ويعتبر الاكتشاف السريع للاختراق من جهة، وإشعار مسؤولي أمن المعلومات بحدوث هذا الاختراق من جهة أخرى، من أهم العناصر الحرجة في هذه المرحلة. ولهذا الهدف يتم استخدام أنظمة كشف التسلل (Intrusion Detection Systems)، وهي برمجيات أو أجهزة تراقب النظام أو الشبكة بحثاً عن أي خروقات أو أنشطة مشبوهة. ويمكن تصنيف هذه الأنظمة إلى ثلاث فئات: أنظمة كشف التسلل المعتمدة على التوقيعات، وأنظمة كشف التسلل المعتمدة على الانحرافات، وأنظمة كشف التسلل الهجينة التي تشمل الأنظمة المعتمدة على التوقيعات والأنظمة المعتمدة على الانحرافات. وتعتمد أنظمة كشف التسلل المعتمدة على التوقيعات على قواعد البيانات الحالية للتهديدات المعروفة لاكتشاف الهجمات السيبرانية؛ أي أن النظام يقارن توقيع البيانات الواردة بقاعدة البيانات المُتضمنة توقيعات البرمجيات الخبيثة التي تم تحديدها مسبقاً. وإذا كانت حزمة البيانات تتوافق مع

التوقيع، يفترض النظام أنه تم اكتشاف حالة اختراق. أما أنظمة كشف التسلل المعتمدة على الانحرافات، فإنها تكشف عمليات التسلل من خلال تقييم سلوك الشبكة، حيث تراقب هذه التقنية سلوك الشبكة العادي وسلوك النظام الفعلي وتحدد الاختلافات على أنها انحرافات عن السلوك الطبيعي (Ravi and Ramachandran, 2020).

أما مرحلة الاستجابة، فتؤكد على وجود خطة لمرحلة الاستجابة لحوادث أمن المعلومات ووجود فريق للاستجابة لحوادث أمن المعلومات له أدوار ومسؤوليات واضحة. وتهدف هذه المرحلة للقضاء على سبب الحادث واستعادة النظام. كذلك ينبغي اتخاذ إجراءات تحقيق معقولة لتحديد المهاجم أو المنظمة التي عرضت الأنظمة للخطر من خلال جمع الأدلة الجنائية أو احتواء الهجوم أو استعادة الأنظمة المخترقة. وينبغي أن يوضع في الاعتبار أيضاً أن هناك أطرافاً رئيسية خارج المنظمة، مثل منظمات إنفاذ القانون ووكالات النيابة العامة ووسائل الإعلام. وينبغي إقامة العلاقات مع هذه الأطراف الخارجية خلال مرحلة التخطيط للعمليات الأمنية. ومن الضروري تقييم الأضرار واحتواء الحادث وإجراء تحليل ما بعد الحادث، وذلك لتوثيق الدروس المستفادة وتعزيز دور أمن المعلومات في الحوادث الأمنية المستقبلية (Ahmad et al., 2014; La Piedra, 2002).

مما سبق، يمكن تلخيص المراحل الثلاث لعمليات أمن المعلومات وأهم أدوارها كما هو مبين في الشكل (1).

الشكل (1)

أهم مراحل عمليات أمن المعلومات وأبرز أدوارها

الذكاء الاصطناعي وأبرز تقنياته

يُعد الذكاء الاصطناعي فرعاً من فروع علوم الحاسب الآلي التي تستخدم الخوارزميات الرياضية المعقدة لمحاكاة التفكير البشري. ولا يوجد تعريف واحد متفق عليه لمُصطلح الذكاء الاصطناعي، وذلك بالرغم من كثرة تداول هذا المصطلح خلال العقود الأخيرة (موسى وبلال، 2020؛ Grosz et al., 2016). وبشكل عام، يمكن تعريف الذكاء الاصطناعي بأنه البرمجيات القادرة على التعلم والتكيف والابداع وحل المشكلات (Rosa et al., 2016). وفي تعريف آخر، نجد أن الذكاء الاصطناعي هو النظام الذي يمكنه تعلم وتكرار الأداء البشري مع إمكانية تجاوز هذا الأداء في مجموعة متكاملة من القدرات المعرفية والفكرية (Adams et al., 2012). وفي تعريف ثالث، يُنظر إلى الذكاء الاصطناعي على أنه دراسة كيفية جعل أجهزة الحاسب الآلي تقوم بالأشياء التي يفعلها الناس حالياً، بشكل أفضل (Rich et al., 2009).

ووفقاً للمجس الوطني للعلوم والتقنية التابع للبيت الأبيض (2016)، فإن جذور الذكاء الاصطناعي ترجع للأربعينات من القرن الماضي. لكن البعض يعتقد أن فكرة الذكاء الاصطناعي بدأت في التبلور عام 1950 بواسطة الباحث (Alan Turing)، وذلك من خلال دراسته (Computing Machinery and Intelligence)، حيث كان السؤال الرئيسي المطروح في هذه الدراسة: هل تستطيع الآلات التفكير؟ (Luger & Chakrabarti,

(2017. ويعتقد البعض أنه لم تتم صياغة مصطلح الذكاء الاصطناعي إلا في عام 1956 (Anand et al., 2019). وفي البداية كان الذكاء الاصطناعي يُستخدم لحل المسائل الرياضية والألعاب والألغاز. وفي الستينات من القرن الماضي، ازداد الطلب على البرمجيات التي تقوم ببعض المهام الفكرية مثل إنشاء الشبكات الدلالية (Matthias, 2004) .أما طفرة الذكاء الاصطناعي فقد بدأت في الثمانينات، وذلك من خلال مشروع أنظمة الجيل الخامس لأجهزة الحاسب الآلي في اليابان عام 1982، وبرنامج (ESPRIT) في أوروبا عام 1983 (Kurzweil et al., 1990). وتعود التطورات الحديثة في التعلم الآلي لعوامل كثيرة أبرزها تطور الخوارزميات، وزيادة الدعم المالي، والنمو الهائل في البيانات التي يتم انشاؤها وحفظها بواسطة الأنظمة الرقمية، وزيادة القوة الحاسوبية، وتوسع الحوسبة السحابية (Anand et al., 2019).

وقد أصبحت للذكاء الاصطناعي أولوية قصوى، ليس فقط على مستوى المنظمات، بل على مستوى الدول أيضاً. على سبيل المثال، أصدر مجلس الدولة الصيني توجيهاته باستثمار 147,8 مليار دولار حتى تصبح الصين مُبتكراً عالمياً في مجال الذكاء الاصطناعي بحلول 2030 (State Council of the People's Republic of China, 2017). وفي عام 2016، أنفقت الولايات المتحدة الأمريكية ما يقارب 1,2 مليار دولار في مجال البحوث والتطوير فيما يتعلق بتقنيات الذكاء الاصطناعي (Holdren and Smith, 2016). وبشكل مماثل، أنفقت أوروبا ما يقارب 700 مليون جنيه على علم الروبوتات والشراكة بين القطاع العام والخاص المتعلقة بالذكاء الاصطناعي (Ansip, 2017). ومن المتوقع أن يصل الاستثمار العالمي في الذكاء الاصطناعي إلى 35,8 مليار دولار عام 2019، وأن يصل إلى 79,2 مليار عام 2022 (IDC, 2019).

وبشكل عام، يمكن تصنيف تقنيات الذكاء الاصطناعي إلى ست تقنيات هي (قمورة وآخرون، 2018؛ Soni, 2020): تقنيات الأنظمة الخبيرة (Expert Systems)، وتقنيات معالجة اللغة الطبيعية (Natural Language Processing)، وتقنيات التعرف على الكلام (Speech Recognition)، وتقنيات الروبوتات (Robotics) وتقنيات رؤية الآلة (Machine Vision)، وتقنيات تعلم الآلة (Machine Learning) التي تندرج تحتها تقنيات التعلم العميق (Deep Learning). وتُعد تقنيات تعلم الآلة (machine learning) أكثر أشكال الذكاء الاصطناعي استخداماً، وهي مجموعة جزئية من الذكاء الاصطناعي، ويُقصد بها تطوير النظم الذكية لتحسين أدائها في مهمة معينة مع مرور الوقت من خلال التجربة. وقد ساهمت تقنيات تعلم الآلة في تطور العديد من الابتكارات، مثل السيارات ذاتية القيادة، والتعرف على الكلام، والترجمة الآلية.

الأدبيات ذات العلاقة بالأمن السيبراني المُعتمد على الذكاء الاصطناعي

نظراً لتطور الهجمات السيبرانية الخبيثة وتبنيها أساليب تقنية متطورة، برز الأمن السيبراني المعتمد على الذكاء الاصطناعي بهدف تقديم حلول أمنية فاعلة للمنظمات. فكما يمكن للمنظمات أن تستخدم الذكاء الاصطناعي لأتمتة العمليات وتحسينها، يستطيع المهاجمون استغلال تقنيات الذكاء الاصطناعي بهدف أتمتة تحديد الثغرات واختراقها.

ويمكن تعريف الأمن السيبراني المعتمد على الذكاء الاصطناعي بأنه مجموعة من القدرات التي تُتيح للمنظمات التنبؤ بالتهديدات السيبرانية واكتشافها والاستجابة لها في الوقت الفعلي باستخدام الخوارزميات المرتبطة بتقنيات الذكاء الاصطناعي المختلفة (Capgemini Research Institute, 2019). ويتميز الأمن السيبراني المعتمد على الذكاء الاصطناعي بالاستجابة السريعة، في أجزاء من الثانية، للهجمات السيبرانية التي قد يستغرق اكتشافها الكثير من الوقت للعنصر البشري؛ أي أن الأمن السيبراني المعتمد على الذكاء الاصطناعي يتميز بقدرته على تطوير تحليل الجرائم السيبرانية ودراستها وفهمها، وتطوير تقنيات مكافحة الجرائم السيبرانية، وتوسيع أفق حلول الأمن السيبراني الحالية، وإنشاء حلول جديدة للأمن السيبراني. وبالتالي فإن نُظم الذكاء الاصطناعي قادرة على التغلب على نقاط الضعف الموجودة في الأدوات الحالية للأمن السيبراني بسبب مرونتها وقدرتها الهائلة على التكيف (Dilek et al., 2015). ويؤكد بعض الباحثين أن الميزة الرئيسية لهذه التقنية هي قدرتها على اكتشاف ليس فقط الهجمات القديمة المعروفة سابقاً، بل أيضاً اكتشاف الهجمات الجديدة غير المعروفة، بما في ذلك الهجمات التي لم تتم كتابتها أو تصورها. وهذه هي قوة تقنيات

تعلم الآلة لتوقع المستقبل (Winder, 2016).

ففي مرحلة الوقاية من المخاطر السيبرانية، تسعى المنظمات للاستفادة من تقنيات الذكاء الاصطناعي في حماية مواردها التقنية وبناها التحتية من الهجمات المُمكنة. على سبيل المثال، هدفت دراسة (Feng et al., 2014) لتطوير نموذج لتحليل المخاطر قادر على تحديد الثغرات وإعطائها أولوية بشكل استباقي باستخدام نموذج تحليل المخاطر لشبكة (Bayesian) وخوارزمية مستعمرة النمل (Ant Colony Optimization)، وذلك لتمثيل عوامل الخطر ومسارات انتشار الثغرات المحددة بناءً على المعرفة من الخبرات والحالات التي تمت ملاحظتها. ووفقاً لدراسة (Poolsappasit et al., 2012)، فقد تم تطوير نموذج يُدعى (Bayesian Attack Graph) من خلال نمذجة هجمات الشبكة وعلاقاتها السببية. ويتضمن هذا النموذج خصائص كل هجمة مع احتمالية الحدوث والتدابير الأمنية ذات الصلة. ويمكن استخدام هذا النموذج في البيئات الجديدة غير المعروفة، في حين أن التحديد الكمي يمكن أن يساعد في بناء إدارة أمنية وخطط فعالة لمعالجة التهديدات. أما دراسة (Damopoulos et al., 2012) فقد عرضت تقنية لاكتشاف الثغرات الأمنية المعروفة والمتنوعة للأجهزة المحمولة، خاصة في مجال الشبكات اللاسلكية وشبكات الاتصالات. واستخدمت هذه التقنية مجموعة من أربع خوارزميات لتعلم الآلة هي: (Random Forest)، و(Bayesian Networks)، و(K-Nearest Neighbours)، و(Radial Basis Function). وقد حققت هذه المجموعة دقة كبيرة في تحديد البرمجيات الضارة والثغرات الخلفية ((Back-doors). وكانت الخصائص المُستخدمة لتدريب الخوارزميات مرتبطة بالمكالمات الهاتفية والرسائل النصية وخدمات الويب.

ولتعزيز مرحلة الوقاية، يدعم الذكاء الاصطناعي عملية المصادقة التي يقوم فيها المستخدم بإثبات أنه مالك للهوية التي يتم استخدامها. وتتم عملية المصادقة عادة من خلال أنظمة المصادقة المعتمدة على القياسات الحيوية كبصمة الإصبع ومسح قزحية/شبكية العين وصورة الوجه (Almuairfi et al., 2013)، بالإضافة إلى أنظمة المصادقة القائمة على القياسات الحيوية السلوكية، مثل طريقة المشي وطريقة التعامل مع لوحة المفاتيح وشاشات اللمس (Gupta et al., 2019). وفي مجال الأمن السيبراني لإنترنت الأشياء، على سبيل المثال، تؤكد الدراسات أن التوقيت الزمني لضغط مفاتيح لوحة المفاتيح والطباعة باللمس من الخصائص المميزة التي يمكن من خلالها التعرف على المستخدم (Buriro et al., 2015)، كما تؤكد الأدبيات أن طبيعة استخدام الفأرة يمكن استخدامها في عملية المصادقة (Zheng et al., 2016)، ويمكن أيضاً تحديد هوية المستخدمين وإتمام عملية المصادقة من خلال تحليل أنماط المشي (Meng et al., 2014). وفي سياق رفع الوعي بالمخاطر السيبرانية، يمكن للألعاب الرقمية الجادة المعتمدة على الذكاء الاصطناعي أن تُسهم في تنمية مهارات الأمن السيبراني ورفع مستوى الوعي بمخاطر أمن المعلومات (Troussas et al., 2020). على سبيل المثال، ركزت اللعبة المقترحة في دراسة (Carlton and Levy, 2015) على تنمية ثلاثة أنواع من مهارات الأمن السيبراني هي: مهارات الأمن السيبراني المرتبطة بأنظمة العمل، ومهارات الأمن السيبراني المرتبطة بمعلومات التعريف الشخصية، ومهارات الأمن السيبراني المرتبطة بالبرمجيات الخبيثة.

أما في مرحلة اكتشاف المخاطر السيبرانية، فتساعد أنظمة الذكاء الاصطناعي على اكتشاف الهجمات والخروقات الأمنية. ففي سياق أنظمة كشف التسلل في الشبكات، واعتماداً على تقنيات التعلم العميق، قامت دراسة (Kim et al., 2016) بتطبيق هيكلة (Long Short Term Memory) على خوارزمية الشبكة العصبية العميقة المتكررة (Recurrent Deep Neural Network)، كما قامت بتدريب النموذج المقترح باستخدام مجموعة بيانات (KDD Cup 1999). ومن خلال اختبار الأداء، أكدت النتائج فاعلية النموذج المقترح. وفي دراسة مشابهة (Alom et al., 2015)، هدف الباحثون لاكتشاف إمكانيات خوارزمية (Deep Belief Networks) من خلال سلسلة من التجارب التي تعتمد على تدريب الخوارزمية على مجموعة بيانات (NSL-KDD). واستطاع النظام المقترح اكتشاف الهجمات وتصنيفها في خمس مجموعات مع دقة في تحديد وتصنيف نشاط الشبكة بناءً على مصادر بيانات محدودة وغير مكتملة. وحقق النظام المقترح دقة بلغت 97% في اكتشاف التسلل.

وتساعد أنظمة كشف التسلل الحديثة أيضاً في اكتشاف شبكات الروبوت، وهي عبارة عن شبكات من الأجهزة المصابة التي يسيطر عليها المهاجمون ويُساء استخدامها للقيام بأنشطة

متعددة غير مشروعة. ويهدف اكتشاف شبكات الروبوت إلى تحديد الاتصالات بين الأجهزة المُصابة داخل الشبكة المُراقبة، وكذلك تحديد خوادم القيادة والتحكم، حيث تؤكد الدراسات أن حقيقة استمرار تطور شبكات الروبوتت تعني أن أساليب الكشف التقليدية متأخرة نسبياً. وفي هذا السياق، هدفت دراسة (Torres et al., 2016) اعتماداً على تقنيات التعلم العميق لتقديم تحليل لجدوى خوارزمية الشبكة العصبية العميقة المتكررة (Recurrent Deep Neural Network) لاكتشاف سلوك حركة المرور في الشبكة، وتم تقييم الأداء من خلال أمرين هامين هما: عدم توازن حركة مرور الشبكة، والطول الأمثل للتسلسلات. وكشفت النتائج الأولية أن الخوارزمية قادرة على تصنيف حركة المرور بمعدلات دقيقة.

كذلك تساعد أنظمة كشف التسلل الذكية في اكتشاف ما يُعرف بـ (خوارزميات إنشاء النطاق) التي تقوم تلقائياً بإنشاء أسماء النطاقات وغالباً ما يستخدمها الجهاز المُصاب للتواصل مع خادم خارجي من خلال إنشاء أسماء مُضيفة جديدة بشكل دوري. وتمثل هذه الخوارزميات تهديداً حقيقياً للمنظمات لأنه من خلال خوارزميات إنشاء النطاق التي تعتمد على تقنيات معالجة اللغة، فإنه من الممكن تجنب الدفاعات اعتماداً على القوائم السوداء الثابتة لأسماء النطاقات. وقد اقترحت الأدبيات خوارزميات عدة للتعامل مع هذه المشكلة. ومن ذلك دراسة (Bisio et al., 2017) التي تقدم خوارزمية فعالة للكشف عن خوارزميات إنشاء النطاق اعتماداً على مراقبة شبكة واحدة. وتقوم الخوارزمية المقترحة باكتشاف الروبوت الذي يبحث عن البنية التحتية للقيادة والتحكم ومن ثم تحليل طلبات نظام أسماء المجالات (DNS) في الفترة الزمنية نفسها. وتشير اختبارات النظام إلى قدرة الخوارزمية المقترحة على اكتشاف خوارزميات إنشاء النطاق مع انخفاض معدل الإنذارات الكاذبة التي يتسبب فيها النظام.

بالإضافة إلى ذلك، يساعد الذكاء الاصطناعي في اكتشاف الرسائل الإلكترونية المزعجة (Spam) والتصيد الاحتيالي (Phishing). وتعتبر الرسائل الإلكترونية المزعجة ورسائل التصيد الاحتيالي إحدى الطرق المفضلة للمهاجمين لتأمين دخولهم غير النظامي إلى شبكات المنظمات، حيث تتضمن تلك الرسائل برمجيات خبيثة أو روابط إلى مواقع إلكترونية مخترقة. وبالرغم من وجود مجموعة كبيرة من التقنيات الهادفة إلى تقليل مخاطر الرسائل الإلكترونية المزعجة ورسائل التصيد الاحتيالي، فإن اكتشاف مثل هذا النوع من الرسائل يزداد صعوبة بسبب استراتيجيات المراوغة المتقدمة التي يستخدمها المهاجمون لتجاوز الأدوات الأمنية التقليدية. وهنا يبرز دور الذكاء الاصطناعي في تحسين عملية اكتشاف الرسائل الإلكترونية المزعجة والتصيد الانتحالي. على سبيل المثال، تم في دراسة (Mi et al., 2015) تطبيق الخوارزمية المعروفة بـ (Stacked Auto-encoder)، وهي أحد الأنواع الرئيسية لخوارزميات الشبكات العميقة، بهدف اكتشاف رسائل البريد الإلكتروني المزعجة، ومقارنة أداء هذه الخوارزمية بشكل شامل مع تقنيات تعلم الآلة السائدة والشائع استخدامها في تصفية البريد الإلكتروني المزعج. وقد أظهرت النتائج التجريبية أن خوارزمية (Stacked Auto-encoder) تعمل بشكل أفضل وبدقة عالية من الخوارزميات التالية: (Naive Bayes)، (Support Vector Machine)، (Decision Tree)، (Boosting)، (Random Forest)، (Artificial Neural Network).

وفي مرحلة الاستجابة، يدعم الذكاء الاصطناعي القضاء على أسباب الهجمات الإلكترونية واستعادة النظام في وقت قياسي. ويدعم الذكاء الاصطناعي في هذه المرحلة أيضاً تحليل البرمجيات الضارة (Malware Analysis). فقد تطورت البرمجيات الضارة في عصرنا الحالي بحيث أصبح بإمكانها إنشاء متغيرات جديدة آلياً لها نفس التأثيرات الضارة، لكنها تظهر كملفات مُختلفة تماماً عن الملفات الأصلية. إن هذه الأشكال المختلفة والخصائص المتعددة للبرمجيات الضارة تتغلب عادة على أدوات أمن المعلومات التقليدية، لكن استخدام تقنيات الذكاء الاصطناعي يساعد في تحليل متغيرات البرمجيات الضارة ويعمل على تصنيفها ووضعها بشكل صحيح في عائلة البرمجيات الضارة المناسبة لها. على سبيل المثال، اقترحت دراسة (Pascanu et al., 2015) نظاماً يعتمد على تقنيات التعلم العميق، وبالأخص يعتمد على نمذجة اللغة الطبيعية. وهذا النظام قادر على تعلم لغة البرمجيات الضارة من خلال التعليمات المنفذة واستخراج خصائص النطاق الزمني. ويستخدم النظام المقترح خوارزمية الشبكة العصبية العميقة المتكررة (Recurrent Deep Neural Network) وشبكات (Echo- state) في مرحلة استخراج

الخصائص. وتشير نتائج اختبار النظام المقترح إلى دقة عالية في تصنيف البرمجيات الضارة.

وفي مرحلة الاستجابة أيضاً، تساعد تقنيات الذكاء الاصطناعي على إعادة توجيه الجهود البشرية إلى الأنشطة الأكثر أهمية، وذلك من خلال تقليل أعباء العمل على محللي الأمن السيبراني. فبواسطة تقنيات الذكاء الاصطناعي، يمكن أتمتة المهام الروتينية التي يؤديها عادة محللو الأمن السيبراني، وكذلك تحديد أولويات مجالات المخاطر للتركيز عليها (Goosen et al., 2018). ومن خلال تقنيات الذكاء الاصطناعي، يمكن أيضاً تفعيل "الاستجابة الذكية" من خلال نشر "مصائد" تعمل كبيئة مستقلة ومكررة من البيئة الفعلية بهدف إيهام المهاجم بأنه يسير في مساره المقصود، وبعد ذلك يتم تحديد هوية ذلك المهاجم (Heinl, 2014). كما يمكن أيضاً لأنظمة الاستجابة المدعومة بالذكاء الاصطناعي إعادة توجيه المهاجمين بعيداً عن الأصول الهامة، أو فصل الشبكات بهدف عزل الأصول الهامة وجعلها في مكان آمن (Goosen et al., 2018).

ويلخص الجدول (1) أبرز أدوار الأمن السيبراني المُعتمد على الذكاء الاصطناعي ومراحله المستهدفة.

الجدول (1)

أبرز أدوار الأمن السيبراني المعتمد على الذكاء الاصطناعي ومراحله المستهدفة

الأدبيات	أبرز أدوار الأمن السيبراني المُعتمد على الذكاء الاصطناعي	المرحلة المستهدفة
(Feng et al., 2014)	• تحليل المخاطر المُحتملة	مرحلة الوقاية
(Poolsappasit et al., 2012)	• حساب احتمالية اختراق الشبكات	
(Damopoulos et al., 2012)	• اكتشاف ثغرات الشبكات	
(Almuairfi et al., 2013)	• المصادقة المعتمدة على القياسات الحيوية	
(Gupta et al., 2019)	• المصادقة المعتمدة على القياسات الحيوية السلوكية	
(Buriro et al., 2015)	• المصادقة من خلال طبيعة استخدام لوحة المفاتيح	
(Zheng et al., 2016)	• المصادقة من خلال طبيعة استخدام الفأرة	
(Meng et al., 2014)	• المصادقة من خلال تحليل أنماط المشي	
(Troussas et al., 2020)	• رفع مستوى الوعي بمخاطر أمن المعلومات	
(Carlton and Levy, 2015)	• تنمية مهارات الأمن السيبراني	
(Winder, 2016)	• التنبؤ بالهجمات المستقبلية	
(Kim et al., 2016)	• كشف التسلل في الشبكات	مرحلة الاكتشاف
(Alom et al., 2015)	• اكتشاف وتصنيف الهجمات	
(Torres et al., 2016)	• اكتشاف شبكة الروبوتات	
(Bisio et al., 2017)	• اكتشاف خوارزميات انشاء النطاق	
(Mi et al., 2015)	• اكتشاف رسائل البريد الإلكتروني المزعجة	
(Pascanu et al., 2015)	• تحليل البرمجيات الضارة	مرحلة الاستجابة
(Heinl, 2014)	• تحديد هوية المهاجم	
(Goosen et al., 2018)	• عزل الأصول الهامة	
(Goosen et al., 2018)	• أتمتة المهام الروتينية	

مما سبق، يمكن استنتاج أن الأمن السيبراني المُعتمد على الذكاء الاصطناعي لديه القدرة على التعامل مع المخاطر

السيبرانية بفاعلية من خلال الوقاية من المخاطر والثغرات المُحتملة، واكتشاف الهجمات في وقت قياسي، وتقديم الاستجابة المناسبة لكل هجوم حتى تتمكن المنظمة من استعادة النظام بأقل خسائر ممكنة. كذلك يمكن مما سبق استنتاج أن أبرز أدوار الأمن السيبراني المُعتمد على الذكاء الاصطناعي في مراحل عمليات أمن المعلومات الثلاث هي: تقييم الثغرات الأمنية، ورفع الوعي الأمني للمستخدمين، واكتشاف حالات التسلل، وتحليل البرمجيات الضارة، وعزل الأصول المهمة. وتتضح من هذا القسم أيضاً قلة الدراسات السابقة، وبالأخص الدراسات العربية، التي تُلقي نظرة شمولية على الأدوار المختلفة للأمن السيبراني المُعتمد على الذكاء الاصطناعي في المراحل الثلاث لعمليات أمن المعلومات على الرغم من أهمية هذه النظرة الشمولية.

الأدبيات ذات العلاقة بتحديات الذكاء الاصطناعي في الأمن السيبراني

إن إمكانات الذكاء الاصطناعي في الأمن السيبراني تواجه العديد من التحديات التي يمكن أن تُعيق من عملها وتؤثر على فاعليتها. ومن هذه التحديات الحاجة للمزيد من القوانين واللوائح المُنظمة للذكاء الاصطناعي في مجال الأمن السيبراني (Liu et al., 2020; Stahl et al., 2010). وهنا تبرز ضرورة صياغة السياسات واللوائح المتعلقة بهذا المجال ودعمها لآليات حوكمة مناسبة تعالج نقاط الضعف وتقلل من المخاطر المحتملة وتدعم آليات الرقابة على قرارات وأنشطة أنظمة الذكاء الاصطناعي في مجال الأمن السيبراني والخوارزميات ذات العلاقة لضمان المتطلبات الأساسية، مثل الشفافية والقابلية للتوضيح والثقة.

وتعتبر الثقة مهمة ليس فقط في التفاعل الاجتماعي البشري، بل هي مهمة أيضاً للعلاقة بين العنصر البشري وأتمتة الأنظمة، لأن مدى نجاح الأمن السيبراني المعتمد على الذكاء الاصطناعي يعتمد على مدى الثقة في هذه التقنيات الحديثة (Soni, 2020). وما زال هناك الكثير من التساؤلات حول مستوى قبول هذه التقنيات الحديثة نظراً لاعتبار الأتمتة جزءاً متأصلاً في الكثير من تطبيقات الذكاء الاصطناعي. وفي الواقع، فإن تأسيس ثقة المستخدمين والمستفيدين في الأنظمة الذكية وتعزيزها يعتبر عنصراً مهماً لتحقيق المنافع والمزايا الاجتماعية والاقتصادية لهذه الأنظمة (Winfield and Jirotka, 2018). وبشكل عام، يمكن الوثوق في التقنية إذا كانت هناك فوائد ملموسة وكانت التقنية آمنة ومنظمة في الوقت ذاته (Winfield and Jirotka, 2018). على سبيل المثال، يمكن تعزيز الثقة عند وجود الشفافية في طريقة عمل الخوارزميات (ibid). كما يمكن بناء الثقة المطلوبة في الذكاء الاصطناعي من خلال عدة منهجيات، بدءاً من تلك الموجودة على مستوى الأنظمة الفردية ومجالات التطبيقات (Robinette et al., 2013) وصولاً إلى تلك الموجودة على المستوى المؤسسي (Mulgan, 2016).

بالإضافة إلى ذلك، تُعد المساءلة تحدياً هاماً من تحديات الأمن السيبراني المُعتمد على الذكاء الاصطناعي. إن قدرة الذكاء الاصطناعي على أتمتة مجموعة كبيرة من الأنشطة قد أدت إلى تغييرات جذرية في نطاق الأعمال ونطاق الحياة الشخصية (Davis, 2016). ومن بين أبرز تلك التغييرات عدم اكتفاء الذكاء الاصطناعي بدعم اتخاذ القرارات، بل سعيه أيضاً لتقديم النصائح والتوصيات التي يمكن أن تنطوي على مخاطر كبيرة (Parnas, 2017). وللتعامل مع هذه المخاطر، توكد الأدبيات على أهمية القدرة على توضيح أسباب اتخاذ القرار أو السلوك المعين وتقديم معلومات حول البيانات والمعارف المستخدمة ومعالجتها وتوضيح ذلك لأصحاب المصلحة، وهذه الخاصية في أنظمة الذكاء الاصطناعي تُسمى المساءلة (Anthes, 2018).

ويُعتبر الجيل الجديد من الخوارزميات المعتمد على تقنيات التعلم العميق أكثر غموضاً بسبب تعقيد عمليات المعالجة والحجم الضخم للبيانات المُكتسبة والناتجة (Guidotti et al., 2019). على سبيل المثال، إذا تم اتخاذ قرار غير دقيق بواسطة أنظمة الذكاء الاصطناعي، كاتخاذ قرار خطأ بتصنيف معين لخوارزميات خبيثة معينة أو تحديد خطأ لهوية مهاجم مُشتبه فيه، وأدى هذا القرار إلى عواقب سلبية على المنظمة، فمن المسؤول في هذه الحالة؟ وللإجابة عن هذا التساؤل الهام، ينبغي توخي الوضوح في موضوع المسؤولية والمساءلة ومقدار نسبتها لكل طرف من الأطراف، سواء كان المسؤول مصمم الأجهزة أو مصمم البرمجيات أو المورد أو غيرهم.

كذلك يخشى الكثير من المتعاملين مع أنظمة الذكاء الاصطناعي على خصوصية بياناتهم التنظيمية؛ فخوارزميات الذكاء الاصطناعي تحتاج غالباً إلى بيانات ضخمة تتعلق بسلوك الأمن السيبراني للمنظمات العامة والخاصة، مما يثير القلق لدى

المسؤولين حول قضايا تتعلق بالبيانات لم يتم حسمها في أغلب الأحيان، مثل: ماهية البيانات التي يتم استخدامها في هذه الأنظمة الذكية، وكيفية استخدام البيانات، وأسباب استخدام تلك البيانات، والنتائج التي تم التوصل إليها من تلك البيانات (Simonit, 2016). وتواجه أنظمة الأمن السيبراني المُعتمد على الذكاء الاصطناعي تحدياً آخر يتعلق بالتحيز المُحتمل من الأنظمة الذكية. فهناك اعتقاد يتمثل في أن أنظمة الذكاء الاصطناعي لا تعمل بعدالة مع جميع المستفيدين. ويرجع ذلك للتحيز المتأصل في البيانات التي تستخدمها أنظمة الذكاء الاصطناعي. على سبيل المثال، قد يتم اعتماد تصاميم الأنظمة المُدربة على نماذج مُعتمدة على بيانات تُمثل شريحة معينة من الفئة المستهدفة ولا تعكس المجتمع بأكمله. كما يعتقد البعض أن التحيز في أنظمة الذكاء الاصطناعي يعود لندرة فحص حلول الذكاء الاصطناعي من قبل البشر أو محاولة منافستها (Crawford and Calo, 2016).

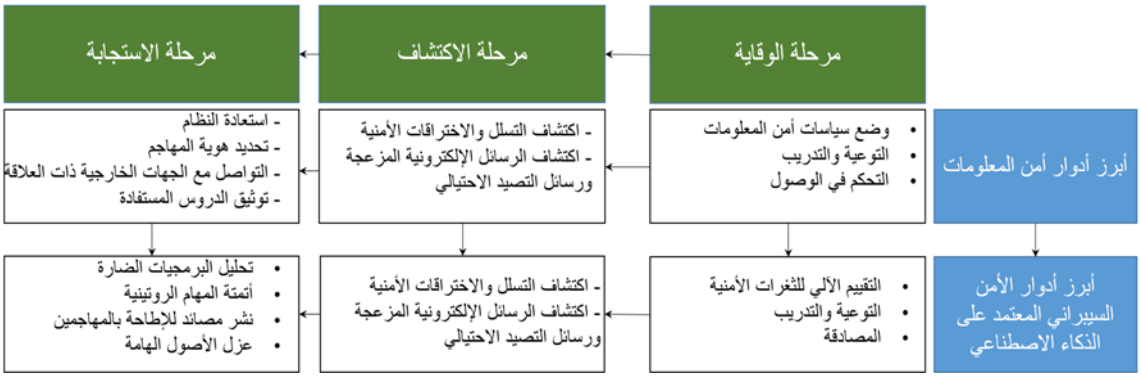
وبشكل عام، يُعتبر توفر مجموعات البيانات اللازمة لتدريب الخوارزميات بمواصفات محددة أحد التحديات في هذا المجال. فالذكاء الاصطناعي في سياق الأمن السيبراني يحتاج إلى كمية كبيرة من البيانات بهدف تدريب الخوارزميات، وكذلك اختبارها والتحقق من نتائجها. ويُفترض أن تتسم هذه البيانات بخصائص معينة حتى يمكن استخدامها كمدخلات للخوارزميات. على سبيل المثال، ينبغي أن تكون هذه البيانات متنوعة بحيث يتم جمعها من العديد من القطاعات والجهات لضمان تعميم النظام على مجموعات متنوعة من المنظمات، وهذا أمر يصعب تحقيقه (Massaro, 2020).

من جهة أخرى، تتطلب الاستفادة من الذكاء الاصطناعي في مجال الأمن السيبراني موارد بشرية ذات تخصصات علمية يتميز بعضها بالندرة في سوق العمل بحيث تدمج تلك التخصصات بين علوم البيانات وعلوم أمن المعلومات. كذلك فإن التعامل مع تقنيات الذكاء الاصطناعي في هذا المجال يتطلب خبرات ومهارات خاصة. فالنمو المتسارع لتقنيات الذكاء الاصطناعي في هذا المجال يتطلب خبرات ومهارات داعمة لتطور الذكاء الاصطناعي. وبشكل عام، هناك نقص في خبرات ومهارات الذكاء الاصطناعي، مما يؤثر سلباً على تنفيذ مشاريع الذكاء الاصطناعي ذات العلاقة بهذا المجال (Reim et al., 2020). إن ندرة التخصصات العملية ذات العلاقة بالذكاء الاصطناعي والأمن السيبراني من جهة، ومحدودية الخبرات والمهارات ذات العلاقة من جهة أخرى، يمكن أن تؤدي إلى صعوبات في تدريب الكادر البشري وتأهيلهم لفهم هذه التقنيات الحديثة والتعامل معها.

وكنتيجة طبيعية لندرة التخصصات العلمية والمهارات العملية، فإن هناك ارتفاعاً في التكاليف المادية للتعليم والتدريب في هذا المجال. على سبيل المثال، يتطلب التعاقد مع الخبراء في هذا المجال مميزات مالية ورواتب عالية. إضافة إلى ذلك، يتطلب الاستثمار في البنية التحتية للذكاء الاصطناعي والأمن السيبراني، التي تُعتبر في غاية التعقيد، مبالغ مالية كبيرة. وهذه التكاليف المالية، سواءً في التدريب والتعليم أو البنية التحتية، قد تكون عائقاً لتطوير تقنيات الذكاء الاصطناعي، خصوصاً في بعض المجتمعات النامية (Terzi et al., 2014).

منهجية الدراسة

تؤكد أدبيات هذه الدراسة على اعتبار موضوع الأمن السيبراني المُعتمد على الذكاء الاصطناعي مجموعة جزئية من الموضوع العام، وهو موضوع أمن المعلومات (von Sloms and von Sloms, 2018). لذا فإن اتباع منهجية دراسة الحالة القائمة على التسلسل من الإطار العام إلى الإطار الخاص والمقترحة في (Trochim and Donnelly, 2001)، واستنتاج المعلومات بناءً على هذا التسلسل يعتبر أمراً منطقياً للإجابة عن السؤال الرئيسي الأول لهذه الدراسة. ولضمان ترابط محاور دراسة الحالة، تم التحليل اعتماداً على مصفوفة تتكون من بعد أفقي وبعد عمودي، كما هو موضح في الشكل (2). وتم تصميم هذه المصفوفة استناداً إلى ما هو متاح من أدبيات أمن المعلومات وأدبيات الأمن السيبراني المعتمد على الذكاء الاصطناعي التي تم استعراضها في الإطار النظري لهذه الدراسة. وستتم مناقشة هذه المصفوفة بالتفصيل في قسم نتائج الدراسة.



الشكل (2)

مصفوفة أدوار ومراحل أمن المعلومات والأمن السيبراني

ويتكون البعد الأفقي للمصفوفة من المراحل الثلاث لعمليات أمن المعلومات والأمن السيبراني، وهي: مرحلة الوقاية، ومرحلة الاكتشاف، ومرحلة الاستجابة. أما البعد الآخر فينتقل عمودياً من النطاق العام لدور إدارة أمن المعلومات إلى النطاق الخاص لدور الأمن السيبراني المعتمد على الذكاء الاصطناعي. وجدير بالذكر أن الأسهم العمودية والأسهم الأفقية الموجودة في المصفوفة لا تُشير إلى توجه الدارسة لاختبار أي علاقة تأثيرية أو علاقة ارتباطية بين الأجزاء المختلفة للمصفوفة، بل جاءت الأسهم لتُشير إلى الانتقال من مرحلة إلى أخرى أفقياً، وكذلك الانتقال من الدور العام إلى الدور الخاص عمودياً. أما السؤال الرئيسي الثاني للدراسة المتعلق بالتحديات، فقد تمت الإجابة عنه اعتماداً على الأدبيات ذات العلاقة بتحديات الأمن السيبراني المُعتمد على الذكاء الاصطناعي.

نتائج الدراسة

في هذا القسم، نُجيب عن أسئلة الدراسة كما يلي:

ما أبرز أدوار الأمن السيبراني المعتمد على الذكاء الاصطناعي؟

اعتماداً على المصفوفة المقترحة في هذه الدراسة والموضحة في الشكل (2)، تمت الإجابة عن هذا السؤال من خلال مناقشة أسئلته الفرعية كما يلي:

ما أبرز أدوار الأمن السيبراني المُعتمد على الذكاء الاصطناعي في مرحلة الوقاية؟

ينبغي التأكيد على أن السياق العام لهذه المرحلة هو عدم وجود أي هجوم أو تسلل فعلي حالياً، لكن ينبغي العمل الجاد من خلال إدارة الأمن السيبراني والذكاء الاصطناعي لرفع جاهزية المنظمة وأخصائيي الأمن السيبراني والكادر البشري لحدوث أي هجوم محتمل. ووفقاً لهذه المصفوفة، يتمثل دور الأمن السيبراني المعتمد على الذكاء الاصطناعي في ثلاثة أدوار هي: التقييم الآلي للثغرات الأمنية، وتقديم الوعي والتدريب الذي يساعد على تنمية مهارات الأمن السيبراني، وتقديم المصادقة الآمنة.

ففي مرحلة الوقاية، تسعى المنظمات لحماية مواردها التقنية وبناها التحتية من الهجمات المُمكنة. ويتم ذلك عادة بواسطة التقييمات الدورية للثغرات الأمنية. وتساعد تقنيات الذكاء الاصطناعي على بناء نماذج تنبؤية لتصنيف الثغرات الأمنية وتجميعها وترتيبها. كذلك يساعد الذكاء الاصطناعي، من خلال الألعاب الرقمية الجادة مثلاً، في تنمية مهارات الأمن السيبراني ورفع الوعي بأهمية أمن المعلومات. ونظراً لأهمية مصادقة المستخدم في الوقاية من الجرائم السيبرانية، يسعى الباحثون لتطوير طرق مُعقدة للتحقق من هوية المستخدم والتعرف عليها، وتقنيات الذكاء الاصطناعي تُقدم طرق مصادقة مختلفة عن الطرق التقليدية، وأبرزها الطرق التي تعتمد على القياسات الحيوية والقياسات الحيوية السلوكية.

وبالنظر إلى دور أمن المعلومات في هذه المرحلة، تؤكد المصفوفة على ضرورة اتساق دور الأمن السيبراني المُعتمد على الذكاء الاصطناعي مع الدور العام لأمن المعلومات. وبعبارة أخرى، ينبغي أن يكون تقييم الثغرات الأمنية وجهود التوعية

والتدريب والمصادقة الآمنة المعتمدة على الذكاء الاصطناعي متسقة مع سياسات أمن المعلومات وسياسات التدريب وسياسات التحكم في الوصول، وألا يكون هناك أي تعارض بينها.

ما أبرز أدوار الأمن السيبراني المعتمد على الذكاء الاصطناعي في مرحلة الاكتشاف؟

السياق العام لهذه المرحلة هي أن هناك هجوماً أو تسللاً فعلياً في الشبكات أو الأجهزة، وأنه ينبغي العمل بأقصى كفاءة لاكتشافه في زمن قياسي حتى لا تكون الأضرار على المنظمة فادحة. وبالتحديد، فإن هناك دورين رئيسيين للأمن السيبراني المعتمد على الذكاء الاصطناعي في مرحلة الاكتشاف، وهما: اكتشاف التسلل بشتى أنواعه سواء كان اكتشاف شبكات الروبوت أو اكتشاف خوارزميات إنشاء النطاق، واكتشاف الرسائل الإلكترونية المزعجة ورسائل التصيد الاحتيالي.

فكشف التسلل يهدف إلى اكتشاف الأنشطة غير المشروعة داخل جهاز الحاسب الآلي أو داخل الشبكة من خلال أنظمة كشف التسلل. وقد أتاح الذكاء الاصطناعي، وبالتحديد أنظمة كشف التسلل المعتمدة على الذكاء الاصطناعي، تغييراً جذرياً في اكتشاف التهديدات والانتقال من الاكتشاف المعتمد على التوقيعات و/أو الانحرافات إلى طرق اكتشاف تتسم بالمرونة وقابلة للتحسين بشكل مستمر لفهم نشاط الشبكة والنظام. كما أتاحت تقنيات الذكاء الاصطناعي التغلب على استراتيجيات المراوغة للرسائل الإلكترونية المزعجة ورسائل التصيد الانتحالي وتطوير عملية اكتشافها.

وبالنظر إلى أبرز أدوار أمن المعلومات في هذه المرحلة، يلاحظ أن الأدبيات أكدت على وجود تطابق بين هذه الأدوار وبين أدوار الأمن السيبراني المُعتمد على الذكاء الاصطناعي. فكل من أمن المعلومات والأمن السيبراني المُعتمد على الذكاء الاصطناعي يسعى لاكتشاف الاختراقات من جهة، كما يسعى لاكتشاف الرسائل الإلكترونية المزعجة ورسائل التصيد الاحتيالي من جهة أخرى. إلا أن الأمن السيبراني المُعتمد على الذكاء الاصطناعي يؤكد على المرونة والديناميكية في أدوات الاكتشاف، بينما أمن المعلومات يركز بشكل عام على هذين الدورين بجميع الوسائل المتاحة، سواء كانت تقليدية أو حديثة.

ما أبرز أدوار الأمن السيبراني المُعتمد على الذكاء الاصطناعي في مرحلة الاستجابة؟

السياق العام لهذه المرحلة هي أن هناك هجوماً أو تسللاً فعلياً في الشبكات أو الأجهزة، وأنه ينبغي العمل بأقصى كفاءة للقضاء على أسبابه بأقل خسائر ممكنة وإعادة الأمور إلى مسارها الطبيعي في أسرع وقت ممكن. وتؤكد المصفوفة أن أدوار أمن المعلومات في هذه المرحلة تتجسد في أربعة أدوار هي: القضاء على أسباب الحوادث الأمنية واستعادة النظام، والمساعدة في مجرى التحقيقات المرتبطة بتحديد المهاجم، والتواصل مع الجهات الخارجية الأمنية والإعلامية ذات العلاقة بحوادث أمن المعلومات، واجراء تحليلات ما بعد الحادث وتوثيق الدروس المستفادة.

أما أدوار الأمن السيبراني المُعتمد على الذكاء الاصطناعي في هذه المرحلة، فجاءت مُنبثقة من أدوار أمن المعلومات وفي سياقها. وهي أربعة أدوار كما يلي: تحليل البرمجيات الضارة، وأتمتة المهام الروتينية لأخصائيي الأمن السيبراني، ونشر المصائد للإطاحة بالمهاجمين، وعزل الأصول الهامة. فالذكاء الاصطناعي يساعد على تحليل الأشكال المتحورة من البرمجيات الضارة التي يصعب تحليلها بالوسائل الأمنية التقليدية. وبواسطة تقنيات الذكاء الاصطناعي، يمكن أيضاً أتمتة المهام الروتينية التي يؤديها عادة محللو الأمن السيبراني، مما يتيح لهم مجالاً أكبر للتركيز على أولويات المخاطر الاستراتيجية. كذلك يدعم الذكاء الاصطناعي الاستجابة الذكية التي تساعد في مجرى التحقيقات المرتبطة بمثل هذه الهجمات وتمهد الأرضية المناسبة لاكتشاف المهاجمين وملاحقتهم قضائياً. بالإضافة إلى ذلك، يساعد الأمن السيبراني المُعتمد على الذكاء الاصطناعي في حماية الأصول الهامة للمنظمة من خلال عزلها وإبعادها عن المهاجمين.

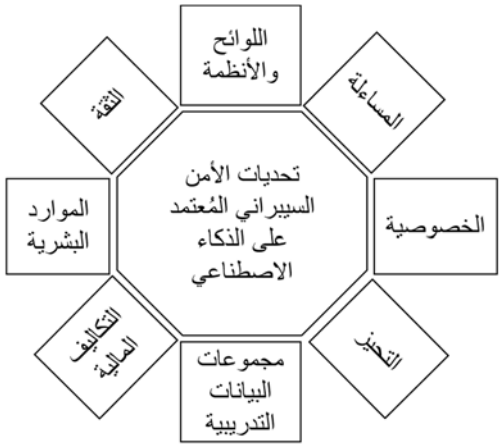
ما أبرز التحديات التي يواجهها الأمن السيبراني المُعتمد على الذكاء الاصطناعي؟

يناقش الإطار النظري لهذه الدراسة ثمانية من أبرز التحديات التي يواجهها الذكاء الاصطناعي في الأمن السيبراني، وهي: اللوائح والأنظمة، والثقة، والمساءلة، والخصوصية، والتحيز، ومدى توفر مجموعات البيانات التدريبية، والموارد البشرية، والتكاليف المادية.

فقد أشارت الأدبيات إلى الحاجة للمزيد من الأطر التنظيمية المرتبطة بسياسات ولوائح الأمن السيبراني المُعتمد على الذكاء الاصطناعي. إن وجود مثل هذه التنظيمات ودعمها يُعتبر الحجر الأساس لضمان الحوكمة المناسبة وتقليل المخاطر المُحتملة في هذا المجال. كذلك أكدت الأدبيات على عنصر الثقة في الذكاء الاصطناعي المرتبط بالأمن السيبراني واعتبرته عنصراً حاسماً لتحقيق الاستفادة من التقنيات الحديثة. وهنا تبرز أهمية التأسيس السليم للثقة في الخوارزميات الذكية والعمل على استدامتها على المدى البعيد.

ونظراً لقدرة الأمن السيبراني المُعتمد على الذكاء الاصطناعي على اتخاذ قرارات وتقديم توصيات قد تنطوي على بعض المخاطر، برزت المساءلة كأحد التحديات في هذا المجال. وتؤكد الأدبيات في هذا السياق أهمية معرفة أسباب اتخاذ القرارات الهامة وتوضيحها لأصحاب المصلحة. كما أن هذا النوع من التقنيات الحديثة يعتمد على جمع البيانات بشكل كبير، مما يُثير بعض المخاوف حول خصوصية البيانات التنظيمية نظراً لعدم وضوح كيفية استخدام تلك البيانات وما هو مصيرها بعد انتهاء التحليل.

إضافة إلى ذلك، يعتقد البعض أن هذه الأنظمة الذكية لا تخلو من التحيز في اتخاذ قراراتها بسبب اعتمادها على بيانات متحيزة في الأصل. إضافة إلى ذلك، فإن الأنظمة الذكية تحتاج إلى مجموعات بيانات بمواصفات معينة حتى يتم تدريب الخوارزميات، لكن قلة توفر مثل هذه المجموعات يُعتبر أيضاً من التحديات. ومن بين التحديات أيضاً نُدرة التخصصات العلمية التي تجمع بين مجال أمن المعلومات ومجال علوم البيانات، وكذلك ضعف المهارات والخبرات العملية واللازمة للعمل والإبداع في هذا المجال. إن التكاليف المادية المرتبطة بمجال الأمن السيبراني المعتمد على الذكاء الاصطناعي، كتكاليف البنى التحتية وتكاليف التعليم والتدريب وغيرها، تعتبر أيضاً من التحديات التي يواجهها هذا المجال. ويلخص الشكل (3) أبرز التحديات التي يواجهها الأمن السيبراني المُعتمد على الذكاء الاصطناعي.



الشكل (3)

أبرز تحديات الأمن السيبيراني المُعتمد على الذكاء الاصطناعي

الخلاصة والتوصيات

لا يزال الأمن السيبراني إحدى القضايا الهامة التي تؤرق الجهات المختلفة وتستهلك جزءاً لا يُستهان به من الموار التنظيمية والبشرية والمالية للمنظمات. ولم تعد أساليب الحماية الأمنية التقليدية قادرة على كبح جماح الهجمات السيبرانية المتطورة، مما أدى إلى ظهور أشكال متطورة من الأمن السيبراني، ومنها ما يُعرف بالأمن السيبراني المُعتمد على الذكاء الاصطناعي. ونظراً لغموض أدوار هذه التقنية الأمنية الحديثة في الأدبيات الحالية، هدفت هذه الدراسة لتسليط الضوء على أبرز أدوار الأمن السيبراني المُعتمد على الذكاء الاصطناعي المنبثقة من أمن المعلومات والمرتبطة بمرحلة الوقاية ومرحلة الاكتشاف ومرحلة الاستجابة. كما هدفت الدراسة لمعرفة أبرز التحديات التي تواجه الأمن السيبراني المُعتمد 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 المُعتمد على الذكاء الاصطناعي. وقد تم الاعتماد في دراسة الحالة على مصفوفة يختص بعدها الأفقي بالمراحل (مرحلة الوقاية، ومرحلة

الاكتشاف، ومرحلة الاستجابة)، بينما يختص بعدها العمودي بالأدوار (دور أمن المعلومات، ودور الأمن السيبراني المُعتمد على الذكاء الاصطناعي).

وخلصت الدراسة إلى وجود تسعة أدوار هامة للأمن السيبراني المُعتمد على الذكاء الاصطناعي، وهذه الأدوار موزعة على المراحل الثلاث (الشكل 2) كما يلي. في مرحلة الوقاية، توصلت الدراسة إلى أن أبرز الأدوار هي: التقييم الآلي للثغرات الأمنية، والتوعية والتدريب، والمصادقة. كما خلصت الدراسة إلى دورين هامين لهذه التقنية الحديثة في مرحلة الاكتشاف، وهما: اكتشاف التسلل والاختراقات الأمنية، واكتشاف رسائل التصيد الإلكترونية المزعجة ورسائل التصيد الاحتيالي. أما بخصوص أبرز الأدوار في مرحلة الاستجابة، فخلصت الدراسة إلى أربعة أدوار هي: تحليل البرمجيات الضارة، وأتمتة المهام الروتينية، ونشر المصائد للإطاحة بالمهاجمين، وعزل الأصول الهامة. وتوصلت الدراسة أيضاً إلى تحديد ثمانية تحديات تواجه الأمن السيبراني المُعتمد على الذكاء الاصطناعي، وهي: اللوائح والأنظمة، والثقة، والمساءلة، والخصوصية، والتحيز، ومجموعات البيانات التدريبية، والموارد البشرية، والتكاليف المالية (الشكل 3).

وفي الختام، نقدم بعضاً من التوصيات المستخلصة من نتائج الدراسة. تؤكد مُخرجات الدراسة على ضرورة الاهتمام بأدوار أمن المعلومات، وبالأخص أدوار الأمن السيبراني المُعتمد على الذكاء الاصطناعي المرتبطة بمرحلة الوقاية ومرحلة الاكتشاف ومرحلة الاستجابة. إن النظرة الشمولية لهذه الأدوار في المراحل الثلاث تعطي معلومات موضوعية عن أبرز القدرات المُمكنة لهذه التقنية الحديثة. كذلك يجدر تأكيد أن تبني الأمن السيبراني المُعتمد على الذكاء الاصطناعي لم يعد ترفاً لبعض المنظمات دون أخرى، بل أصبح ضرورة تُمليها القدرات المتنامية للهجمات السيبرانية المُتطورة. ومع الأهمية المتزايدة لهذه التقنية الحديثة ولأنها أصبحت ضرورة في مُعظم المنظمات، ينبغي النظر إلى الأدوار المتعددة التي تمت مناقشتها في ثنايا هذه الدراسة نظرة موضوعية دون مبالغة أو تقليل من شأنها. ويعني ذلك أن هذه الأدوار ليست بلا حدود، بل ما زالت ضمن أُطر محددة ينبغي فهمها جيداً قبل المُضي قدماً نحو تبني هذه التقنيات الحديثة. وينبغي أيضاً الاهتمام بتحديات الأمن السيبراني المُعتمد على الذكاء الاصطناعي والتعامل معها ضمن خطة استراتيجية شمولية، والابتعاد عن الخطط الجزئية التي تعالج بعضاً من التحديات وتُهمل البعض الآخر. وأخيراً، ينبغي التوجه بشكل أكبر نحو تفعيل التعاون البحثي بين المتخصصين في المجالات ذات العلاقة بالأمن السيبراني والذكاء الاصطناعي، وذلك لرفع كفاءة هذه التقنيات الحديثة والتغلب على تحدياتها.

المراجع

المراجع العربية

اللوزي، موسى سلامة، 2010، الصعوبات التي تواجه تطبيق الخدمات الإلكترونية كما يراها العاملون في أجهزة الخدمة المدنية في الأردن. ***المجلة الأردنية في إدارة الأعمال***، العدد 1، ص 1-55

بانقا، علم الدين، 2019، ***مخاطر الهجمات الإلكترونية (السيبرانية) وآثارها الاقتصادية: دراسة حول دول مجلس التعاون الخليجي***. المعهد العربي للتخطيط

الحميد، محمد دباس، نينو، ماركو إبراهيم، 2007، ***حماية أنظمة المعلومات***. عمان، دار الحامد للنشر والتوزيع.

صادق، دلال، والفتال، حميد ناصر، 2019، ***أمن المعلومات***. دار اليازوي العلمية للنشر والتوزيع، الأردن.

القحطاني، عادل محمد، 1435هـ، ***تصور استراتيجي لتطوير أمن المعلومات تعزيزاً للأمن الوطني في المملكة العربية السعودية بالتطبيق على شركة سابك***. رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، كلية العلوم الاستراتيجية، قسم الدراسات الاستراتيجية.

قمورة، سامية شهيي، ومحمد، باي، وكروش، حيزية، 2018، ***الذكاء الاصطناعي بين الواقع والمأمول: دراسة تقنية***

وميدانية. الملتقى الدولي: الذكاء الاصطناعي تحد جديد للقانون، الجزائر.

موسى، عبدالله، وبلال، أحمد حبيب، 2020، ***الذكاء الاصطناعي ثورة في تقنيات العصر***. شركة كتاب للنشر والتوزيع.

المراجع العربية باللغة الإنجليزية

Al-Hamid, Muhammad Dabbas and Nino, Marco Ibrahim. 2007. ***Information Systems Protection***. Amman, Al-Hamid House for Publishing and Distribution.

Al-Lawzi, Musa Salameh. 2010. Difficulties Facing the Application of Electronic Services as Seen by Workers in Civil Service Agencies in Jordan. ***Jordanian Journal of Business Administration***, (1): 1-55.

Al-Qahtani, Adel Muhammad. 1435 (AH). ***A Strategic Vision for Developing Information Security in Order to Enhance National Security in the Kingdom of Saudi Arabia Based on SABIC***. Master Thesis, Naif Arab University for Security Sciences, College of Strategic Sciences, Department of Strategic Studies.

Banaqa, Alumedeen. 2019. ***The Risks of Cyber Attacks and Their Economic Impacts: A Study on the Countries of the Gulf Cooperation Council***. Arab Planning Institute.

Musa, Abdullah and Bilal, Ahmed Habib. 2020. ***Artificial Intelligence, A Revolution in the Technologies of the Era***. Kitab Company for Publishing and Distribution.

Qamoura, Samia Chahi, Mohamed, Bay and Krouche, Hayziah. 2018. Artificial Intelligence between Reality and Expectations: Technical and Field Study. ***The International Forum on Artificial Intelligence: A New Challenge to Law***, Algeria.

Sadiq, Dalal and Al-Fattal, Hamid Nasir. 2019. ***Information Security***. Al-Yazwi Scientific Publishing and Distribution House, Jordan.

USA Code of Law website, Legal Information Institute, https://www.law.cornell.edu/uscode/text/44/3542.

المراجع الأجنبية

Abdelwahed, A.S., Mahmoud, A.Y. and Bdair, R.A. 2017. Information Security Policies and Their Relationship with the Effectiveness of Management Information Systems of Major Palestinian Universities in the Gaza Strip. ***International Journal of Information Science & Management***, 15 (1).

Adams, S., Arel, I., Bach, J., Coop, R., Furlan, R., Goertzel, B., Hall, J.S., Samsonovich, A., Scheutz, M., Schlesinger, M., Shapiro, S.C. and Sowa, J. 2012. Mapping the Landscape of Human-level Artificial General Intelligence. ***AI Magazine***, 33 (1): 25-42.

Ahmad, A., Maynard, S.B. and Park, S. 2014. Information Security Strategies: Towards an Organizational Multi-strategy Perspective. ***Journal of Intelligent Manufacturing***, 25 (2): 357-370.

Al-Khuri, R.S. and Al-Qudah, K.A. 2006. Problems Facing Owners and Managers Operating in the Qualifying Industrial Zones in Jordan. ***Jordan Journal of Business Administration***, 2 (1), 134-146.

Almuairfi, S., Veeraraghavan, P. and Chilamkurti, N. 2013. A Novel Image-based Implicit Password Authentication System (IPAS) for Mobile and Non-mobile Devices. ***Math. Comput. Model.***, 58 (1-2): 108-116.

Alom, M.Z., Bontupalli, V. and Taha, T.M. 2015. Intrusion Detection Using Deep Belief Networks. In: ***2015 National Aerospace and Electronics Conference (NAECON)***, 339-344, IEEE.

Anand, S., Sinha, A., Tiwari, U. and Ray, S. 2019. ***Artificial Intelligence-Literature Review***. Retrieved from: https://cis-india.org/internet-governance/files/artificial-

الموقع الإلكتروني لمدونة قانون الولايات المتحدة الأمريكية، معهد المعلومات القانونية، https://www.law.cornell.edu/uscode/text/44/3542

intelligence-literature-review

Ansip, A. 2017. ***Making the Most of Robotics and Artificial Intelligence in Europe***. Edited by European Commission. https://ec.europa.eu/commission/commissioners/2014-2019/ansip/blog/making-mostrobotics-and-artificial-intelligence-europe_en

Anthes, G. 2017. Artificial Intelligence Poised to Ride a New Wave. ***Commun. ACM***, 60 (7): 19-21. https://doi.org/10.1145/3088342

Antonucci, D. 2017. Human Resources Security. ***The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities***, 369-374.

Bisio, F., Saeli, S., Lombardo, P., Bernardi, D., Perotti, A. and Massa, D. 2017. Real-time Behavioral DGA Detection through Machine Learning. In: ***2017 International Carnahan Conference on Security Technology (ICCST)***, 1-6, IEEE.

Buriro, A., Crispo, B., Del Frari, F. and Wrona, K. 2015. Touchstroke: Smartphone User Authentication Based on Touch-typing Biometrics. In: ***International Conference on Image Analysis and Processing,*** 27-34, Springer, Cham.

Capgemini Research Institute. 2019. ***Reinventing Cybersecurity with Artificial Intelligence.*** https://www.capgemini.com/wp-content/uploads/2019/07/AI-in-Cybersecurity_Report_20190711_V06.pdf

Carlton, M. and Levy, Y. 2015. Expert Assessment of the Top Platform Independent Cybersecurity Skills for Non-IT Professionals. In: ***Southeast Con.***, 2015, 1-6. IEEE.

Crawford, K. and Calo, R. 2016. There Is a Blind Spot in Al. ***Nature Comment***, 538 (7625).

Damopoulos, D., Menesidou, S.A., Kambourakis, G., Papadaki, M., Clarke, N. and Gritzalis, S. 2012. Evaluation of Anomaly-based IDS for Mobile Devices Using Machine Learning Classifiers. ***Security and Communication Networks***, 5 (1): 3-14.

Davis, A. 2016. ***How Artificial Intelligence Has Crept into our Everyday Lives***. IEEE Special Report. http://theinstitute.ieee.org/static/special-report-artificial-intelligence

Dilek, S., Çakır, H. and Aydın, M. 2015. Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review. ***Arxiv preprint arXiv:***1502.03552.

Evans, L. 2016. Protecting Information Assets Using ISO/IEC Security Standards. ***Information Management***, 50 (6): 28.

Feng, N., Wang, H.J. and Li, M. 2014. A Security Risk Analysis Model for Information Systems: Causal Relationships of Risk Factors and Vulnerability Propagation Analysis. ***Information Sciences***, 256: 57-73.

Goosen, R., Rontojannis, A., Deutscher, S., Rogg, J., Bohmayr, W. and Mkrtchian, D. 2018. ***Artificial Intelligence Is a Threat to Cybersecurity. It's Also a Solution***. The Boston Consulting Group.

Grosz, B.J., Mackworth, A., Altman, R., Horvitz, E., Mitchell, T., Mulligan, D. and Shoham, Y. 2016. ***Artificial Intelligence and Life in 2030: One Hundred Years Study on Artificial Intelligence***. Edited by Stanford University.

Guidotti, R., Monreale, A. and Pedreschi, D. 2019. The AI Black Box Explanation Problem. ***ERCIM News***, 116: 12-13.

Gupta, S., Buriro, A. and Crispo, B. 2019. Driverauth: A Risk-based Multi-modal Biometric-based Driver Authentication Scheme for Ride-sharing Platforms. ***Computers & Security***, 83: 122-139.

Heinl, C.H. 2014. Artificial (intelligent) Agents and Active Cyber Defence: Policy Implications. ***2014 6th International Conference on Cyber Conflict (CyCon 2014)***, 53-66. IEEE.

Holdren, J. and Smith, M. 2016. ***Preparing for the Future of Artificial Intelligence***. Edited by Executive Office of the President National Science and Technology Council, Committee on Technology. Washington, DC. https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf

IDC. 2019. ***Worldwide Spending on Artificial Intelligence***

Systems Will Grow to Nearly $35.8 Billion in 2019, According to New IDC Spending Guide. https://www.idc.com/getdoc.jsp?containerId=prUS44911419

Jean-Philippe, R. 2018. ***Enhancing Computer Network Defense Technologies with Machine Learning and Artificial Intelligence***. Utica College.

Kim, J., Kim, J., Thu, H.L.T. and Kim, H. 2016. Long Short Term Memory Recurrent Neural Network Classifier for Intrusion Detection. In: ***2016 International Conference on Platform Technology and Service (PlatCon)***, 1-5, IEEE.

Kurzweil, R., Richter, R. and Schneider, M.L. 1990. ***The Age of Intelligent Machines***, (Vol. 579). MIT Press Cambridge, MA.

La Piedra, J. 2002. ***The Information Security Process: Prevention, Detection and Response***. *SANS Institute*.

Liu, H.Y., Maas, M., Danaher, J., Scarcella, L., Lexer, M. and Van Rompaey, L. 2020. Artificial Intelligence and Legal Disruption: A New Model for Analysis. ***Law, Innovation and Technology***, 1-54.

Luger, G.F. and Chakrabarti, C. 2017. From Alan Turing to modern AI: Practical Solutions and an Implicit Epistemic Stance. ***AI & Society***, 32 (3): 321-338.

Massaro, A. 2020. Advanced Multimedia Platform based on Big Data and Artificial Intelligence Improving Cybersecurity. ***International Journal of Network Security & Its Applications (IJNSA)***, 12.

Matthias, A. 2004. The Responsibility Gap: Ascribing Responsibility for the Actions of Learning Automata. ***Ethics and Information Technology***, 6 (3): 175-183.

Meng, W., Wong, D.S., Furnell, S. and Zhou, J. 2014. Surveying the Development of Biometric User Authentication on Mobile Phones. ***IEEE Communications Surveys & Tutorials***, 17 (3): 1268-1293.

Mi, G., Gao, Y., and Tan, Y. 2015. Apply Stacked Auto-encoder to Spam Detection. In: ***International Conference on Swarm Intelligence***, 3-15. Springer, Cham.

Mulgan, G. 2016. ***A Machine Intelligence Commission for the UK: How to Grow Informed Public Trust and Maximise the Positive Impact of Smart Machines, February 2016***. London, UK: Nesta.https://www.nesta.org.uk/documents/692/a_machine_intelligence_commission_for_the_uk_-_geoff_ mulgan.pdf.

NIST, National Institute of Standards and Technology. 2018. ***Cybersecurity Framework***. https://www.nist.gov/cyberframework/online-learning/five-functions

Noyes, K. 2016. ***A.I + Humans = Serious Cybersecurity***. Computerworld, www.computerworld.com/ articles/ 3057590/security/ai-humans-serious-cybersecurity.html

Parnas, D.L. 2017. The Real Risks of Artificial Intelligence. ***Commun. ACM***, 60 (10): 27-31. https://doi.org/10.1145/3132724

Pascanu, R., Stokes, J.W., Sanossian, H., Marinescu, M. and Thomas, A. 2015. Malware Classification with Recurrent Networks. In: ***2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)***, 1916-1920, IEEE.

Poolsappasit, N., Dewri, R., and Ray, I. 2012. Dynamic Security Risk Management Using Bayesian Attack Graphs. ***IEEE Transactions on Dependable and Secure Computing***, 9 (1): 61-74.

Ravi, N. and Ramachandran, G. 2020. A Robust Intrusion Detection System Using Machine-learning Techniques for MANET. ***International Journal of Knowledge-based and Intelligent Engineering Systems***, 24 (3): 253-260.

Reim, W., Åström, J. and Eriksson, O. 2020. Implementation of Artificial Intelligence (AI): A Roadmap for Business Model Innovation. ***AI***, 1 (2): 180-191.

Rich, Elaine, Knight, Kevin and Nair, Shivashankar B. 2009. ***Artificial Intelligence***. Third Edition. New Dehli, India: Tata McGraw-Hill.

Robinette, P., Wagner, A.R. and Howard, A.M. 2013. Building and Maintaining Trust between Humans and Guidance Robots. in an Emergency. In: ***Trust and Autonomous Systems: 2013 AAAI Spring Symp.***, Stanford, CA, 25-27 March, 78-83. Palo Alto, CA: AAAI Press.

Rosa, A., Feyereisl, J. and Team, T. G. 2016. A Framework for Searching for General Artificial Intelligence. ***CoRR abs.,***/1611.00685, 1-54.

Schatz, D., Bashroush, R. and Wall, J. 2017. Towards a More Representative Definition of Cyber Security. ***Journal of Digital Forensics, Security and Law***, 12 (2): 8.

Simonit, T. 2016. Microsoft and Google want to Let Artificial Intelligence Loose on Our Most Private Data. ***MIT Technology Review.com***/s/601294/microsoft-and-google-want-to-let-artificial-intelligence-loose-on-our-most-private-data/

Soni, V.D. 2020. ***Challenges and Solution for Artificial Intelligence in Cybersecurity of the USA***. *Available at SSRN 3624487*.

Stahl, B., Elizondo, D., Carroll-Mayer, M., Zheng, Y. and Wakunuma, K. 2010. Ethical and Legal Issues of the Use of Computational Intelligence Techniques in Computer Security and Computer Forensics. In: ***The 2010 International Joint Conference on Neural Networks (IJCNN)***, 1-8, IEEE.

State Council of the People's Republic of China. 2017. ***China Issues Guideline on Artificial Intelligence Development***. http://english.gov.cn/policies/latest_releases/2017/07/20/content_281475742458322.htm

Terzi, R., Yavanoglu, U., Sinanc, D., Oguz, D. and Cakir, S. 2014. An Intelligent Technique for Detecting Malicious Users on Mobile Stores. In: ***2014 13th International Conference on Machine Learning and Applications***, 470-477, IEEE.

Torres, P., Catania, C., Garcia, S. and Garino, C.G. 2016. An Analysis of Recurrent Neural Networks for Botnet Detection Behavior. In: ***2016 IEEE Biennial Congress of Argentina (ARGENCON)***, 1-6, IEEE.

Trochim, W.M. and Donnelly, J.P. 2001. ***Research Methods Knowledge Base***. Cincinnati, OH: Atomic Dog Publishing.

Troussas, C., Krouska, A., Sgouropoulou, C. 2020. Collaboration and Fuzzy-modeled Personalization for Mobile Game-based Learning in Higher Education. ***Comput. Educ.***, 144: 103698.

von Sloms, B. and von Sloms, R. 2018. Cybersecurity and Information Security: What Goes Where? ***Information & Computer Security***, 26 (1): 2-9.

Winder, D. 2016. ***Al Could Rescue Failing Cyber Security Sector-Raconteur***. https://www.raconteur.net/technology/ai-could-rescue-failing-cyber-security-sector

Winfield, A.F. and Jirotka, M. 2018. Ethical Governance Is Essential to Building Trust in Robotics and Artificial Intelligence Systems. ***Philosophical Transactions of the Royal Society-A: Mathematical, Physical and Engineering Sciences***, 376 (2133): 20180085.

Wu, J., Dong, M.X., Ota, K. et al. 2018. Big Data Analysis-based Secure Cluster Management for Optimized Control Plane in Software-defined Networks. ***IEEE Trans. Netw. Serv. Manag.***, 15 (1): 27-38.

Zheng, N., Paloski, A. and Wang, H. 2016. An Efficient User Verification System Using Angle-based Mouse Movement Biometrics. ***ACM Transactions on Information and System Security (TISSEC)***, 18 (3): 1-27.