جامعة نايف العربية للعلوم الأمنية
Naif Arab University for Security Sciences

أوراق السياسات الأمنية
Security Policy Papers

Volume 1, Issue (1), 2020, 1-18, https://nauss.edu.sa
http://spp.nauss.edu.sa/spp

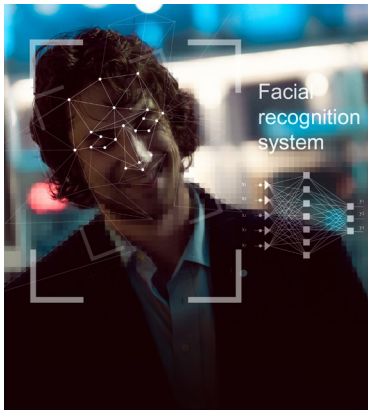
ورقة تحليل سياسات أمنية

الذكاء الاصطناعي وأبعاده الأمنية

Artificial Intelligence and its Security Dimensions

حسين يوسف أبو منصور
قسم علوم الأدلة الجنائية، كلية العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية

Hussein Yosuf Mansour
Department of Forensic Sciences, College of Criminal Justice, Naif Arab University for Security Sciences



المخرجات الرئيسية

- إنشاء وتفعيل مراكز البحث والتطوير الأمنية والعسكرية وتوطينها على غرار وكالة مشروعات البحوث المتقدمة التابعة لوزارة الدفاع، ووكالة مشروعات البحوث المتقدمة التابعة للمخابرات، وفريق متعدد الوظائف للحرب الخوارزمية.
- دعم الأبحاث المركزة على الألعاب الإستراتيجية من خلال برامج المحاكاة للبيئات الصعبة
- دعم دوريات الأمن الإلكترونية وإطلاق حزمة من البرمجيات الذكية لمراقبة جميع النشاطات المشبوهة الواردة والصادرة.
- تأهيل الكوادر الوطنية مع التركيز على المجالات والتوجهات الحديثة المتمثلة في العمل الأمني والعسكري الذكي، الذي يستند إلى تقنيات وخوارزميات الذكاء الاصطناعي.

المستخلص

مرت البشرية بكثير من الثورات الصناعية، تأتي في مقدمتها الثورة الصناعية الأولى في القرن السابع عشر الميلادي، حيث تم الانتقال من الإنتاج اليدوي في الصناعات إلى الإنتاج باستخدام طاقة البخار، وتدرج التطور إلى استخدام الطاقة الكهربائية مرورًا بثورة المعلومات والاتصالات إلى أن وصلنا الآن إلى الثورة الصناعية الرابعة، التي تعتمد على البيانات الضخمة وتقنيات الذكاء الاصطناعي وأدواته في مجالات عدة حديثة من أبرزها: الروبوتات، وإنترنت الأشياء، والمدن والمنشآت الذكية، والطباعة ثلاثية الأبعاد، والهندسة الوراثية، والمجالات الأمنية والعسكرية وغيرها من المجالات، ويعد الذكاء الاصطناعي (Artificial Intelligence) من أسرع المجالات نموًّا، وله آثار إيجابية مهمة في كثير من المجالات من أبرزها: المجالات

Abstract

Humanity has gone through many industrial revolutions, foremost among which is the first industrial revolution in the seventeenth century, where the transition from manual production in industries to production using steam energy took place. Developments in the use of electricity through the information and communication revolution have grown until we have now reached the fourth industrial revolution. This revolution is based on big data, artificial intelligence technologies and tools in several recent areas. The most prominent areas are robots, the internet of things, smart cities and facilities, 3D printing, genetic engineering, security, military, and other fields. Artificial Intelligence is one of the fastest growing fields and has important positive effects on many areas, most notably in the various areas of security in its most comprehensive sense

المختلفة للأمن بمفهومه الشامل والعمليات العسكرية. وقد اهتمت الدول بتطوير تطبيقات الذكاء الاصطناعي واستخداماتها في المجالات الأمنية والعسكرية (مثل: جمع المعلومات الاستخبارية وتحليلها، والخدمات اللوجستية، والعمليات الإلكترونية، والقيادة والسيطرة، والحرب الإلكترونية وغيرها)، وهذا التطوير تطلب بعض القرارات المتعلقة بالميزانية والقوانين والتشريعات، التي تدعم اتخاذ القرارات الأمنية، وتعزز اعتماد ودعم استخدام تطبيقات الذكاء الاصطناعي في المجالات الأمنية والعسكرية. ونستعرض في هذه الورقة ماهية الذكاء الاصطناعي، وأبرز الفرص والتحديات لاستخدام تطبيقاته في القطاعات الأمنية والعسكرية وأهم مجالات استخدامها في هذه القطاعات.

and in military operations. Countries have devoted attention to developing applications and uses of artificial intelligence in security and military areas such as intelligence gathering and analysis, logistics, electronic operations, command and control, and electronic warfare, etc. This development has required some decisions related to the budgets, laws, and legislations that support security decision-making and promote the adoption and support of the use of artificial intelligence applications in security and military areas. In this paper, we review the nature of artificial intelligence and highlight the opportunities and challenges for using its applications in the security and military sectors and their most important areas of use in these sectors.

1. المقدمة

يشهد العالم حاليًّا كثيرًا من التحولات الجذرية على المستوى السياسي والاقتصادي والاجتماعي وكذلك على المستوى الأمني والعسكري، ولقد أسست هذه التحولات بداية لعهد جديد في كثير من دول العالم، فعلى سبيل المثال في المملكة العربية السعودية، تتمثل هذه التحولات في كثير من المجالات، ويأتي في مقدمتها رؤية المملكة 2030، التي ارتكزت على ركائز عدة انبثقت عنها مجموعة من البرامج الوطنية، التي يتطلب معظمها تحقيق مطالب عدة من أبرزها: الأمن السيبراني، والسلامة المرورية (رؤية المملكة العربية السعودية 2030، 2020). وتسعى رؤية المملكة 2030 إلى إنشاء مرجعية مختصة بالأمن السيبراني مهتمة بشؤونه المختلفة من خلال زيادة عدد الكوادر الوطنية المؤهلة لتشغيله تحت مسمى "الهيئة الوطنية للأمن السيبراني" بوصفها هيئة حكومية لها شخصية مستقلة (الهيئة الوطنية للأمن السيبراني، 2020). ولدى المملكة العربية السعودية طموحات كبيرة معتمدة على إمكانات الذكاء الاصطناعي، التي جرى تحديدها في رؤية 2030، بما في ذلك بناء مدينة نيوم "NEOM" المستقبلية، التي تعتمد بشكل أساسي على تقنيات الذكاء الاصطناعي، كما أبدت المملكة العربية السعودية اهتمامًا كبيرًا باستخدام تقنيات الذكاء الاصطناعي للأغراض العسكرية، خصوصًا في الطائرات دون طيار (الدرونز)، والتحكم الذاتي، والروبوتات الذكية (Han, 2017).

ويمثل تطويع تقنيات الذكاء الاصطناعي وتطبيقاته، التي يغلب عليها الطابع التجاري، لاستخدامها في الجانب الأمني والعسكري تحديًا كبيرًا، ويتمثل هذا التحدي في القدرة على تكييفها وتخصيصها؛ لتتناسب مع الاحتياجات الأمنية

والعسكرية، وبالرغم من إمكانية التكامل بين القطاعات التجارية والتقنية من جهة، والقطاعات الأمنية والعسكرية من جهة أخرى فإنه ظهر عدد من التحديات نتيجة الشراكة بين هذين القطاعين بسبب المخاوف الأخلاقية، التي تؤدي في بعض الأحيان إلى ظهور مقاومة لدمج تقنيات الذكاء الاصطناعي في الأنظمة الأمنية والعسكرية، لما تتطلبه هذه الأنظمة من اختراق الخصوصية في بعض الأحيان (مثل: مراقبة الاتصالات وتسجيلات الدوائر التلفزيونية المغلقة وحسابات التواصل الاجتماعي ومتابعتها)، من أجل ضبط الأمن والمحافظة عليه.

وواقع الحال حاليًّا أدى إلى إيجاد منافسة شديدة بين الفاعليين الدوليين المحتملين في سوق الذكاء الاصطناعي من الدول العظمى، التي من أبرزها الولايات المتحدة الأمريكية والصين وروسيا، حيث تعد الصين من أبرز المنافسين الدوليين في هذا المجال، فقد أصدرت خطة عمل تطويرية في عام 2017م؛ لِتَتَبَوَّأ سلّم الريادة العالمية في مجال تطوير الذكاء الاصطناعي بحلول عام 2030م، وذلك من خلال توظيف تقنيات الذكاء الاصطناعي في نُظم دعم اتخاذ القرارات الإستراتيجية بفاعلية وجدوى أكبر، وكذلك في مجال تطوير المركبات العسكرية الذكية ذاتية التحكم. وبالمقابل، تنشط روسيا أيضًا في مجال تطوير الذكاء الاصطناعي في المجالات الأمنية والعسكرية بشتى المجالات مع التركيز بشكل أساسي على الروبوتات (Sayler, 2019).

وحققت تقنيات الذكاء الاصطناعي مؤخرًا تقدمًا ملحوظًا في مجال الاستشعار والتصنيف والاستنتاج وصنع القرار والتعرف على الأنماط ضمن أحجام هائلة من البيانات، وذلك من خلال الأساليب المختلفة التي من أبرزها التعلم العميق (Deep Learning) المرتكزة على العمليات العصبية للأدمغة البشرية، والتي يتم التعلم من خلالها دون إشراف (Unsupervised Learning) بالرغم من وجود بيانات محدودة للتدريب في بعض المجالات، والتعامل مع المعلومات الغامضة وغير المتماثلة أو المنتظمة، وتتركز معظم أبحاث الذكاء الاصطناعي حاليًّا على القطاعات التي لا ترتبط بشكل صريح بالمجالات الأمنية والعسكرية، مثل: الرعاية الصحية والتعليم والتجارة والصناعة، إلا أنه بالنظر إلى الإمكانات العظيمة لتقنيات الذكاء الاصطناعي وأدواته، فإنها دون شك ستكون مفيدة على الصعيدين التكتيكي والإستراتيجي في المجالات الأمنية والعسكرية في حال تطويعها لهذه المجالات.

وبالنظر إلى ما سبق، نخلص إلى أنه يمكن لتقنيات الذكاء الاصطناعي وأدواته أن تسهم في صياغة الإستراتيجيات الأمنية والعسكرية من خلال تقديم رؤى واعدة لصناع القرار بعيدًا عن العوامل النفسية الفردية والجماعية، التي لا تعد ولا تحصى في صناعة القرار، بما في ذلك التفكير الجماعي، والتحيز ومقاومة التغيير، والسياسة البيروقراطية، والتفاؤل المفرط وسوء تقدير المخاطر.

2. الذكاء الاصطناعي: الفرص والتحديات

على الرغم من أن استخدام تقنيات الذكاء الاصطناعي وأدواته المختلفة قد يفرض كثيرًا من التحديات والمعوقات الفنية والتقنية عند توظيفها في

المجالات الأمنية والعسكرية؛ فإنها تفرض في المقابل كثيرًا من الفرص في السياق نفسه، خصوصًا أن جهود مطوري هذه التقنيات مكثفة في الحرص على الحد من نقاط الضعف والآثار السلبية والاستغلال الأمثل للإمكانات التي توفرها تقنيات الذكاء الاصطناعي وأدواته المختلفة.

2. 1. الفرص

تعدّ تقنيات الذكاء الاصطناعي أدوات أساسية في التكنولوجيا الناشئة "Emerging Technology"، فهي تقدم كثيرًا من المزايا التي تعتبر إضافة إلى هذه التكنولوجيا من عدة نواحٍ سواء أكانت في الأداء أم الفاعلية. وفيما يلي نستعرض مجموعة من الفرص التي تقدمها تقنيات الذكاء الاصطناعي في سياقات عدة، نذكر من أبرزها:

2. 1. 1. التحكم الذاتي (Autonomy)

بالنظر إلى التطور التقني الحاصل في الوقت الحالي، وما نتج عنه من فرص وتحديات، فقد حرصت أغلب أنظمة التحكم الذاتي عمومًا والأمنية منها خصوصًا على تطوير أدائها من خلال دمج تقنيات الذكاء الاصطناعي بشكل أو بآخر في آليات عملها؛ سعيًا إلى أداء ما هو منوط بها من مهام على أتم وجه وأكبر فاعلية، وفي هذا السياق، حازت أنظمة التحكم الذاتي في التطبيقات الأمنية والعسكرية اهتمامًا كبيرًا من قبل الإدارة الأمريكية في عهد باراك أوباما، حيث كانت محور تركيز "إستراتيجية الإزاحة الثالثة"، التي تمثلت في إطار عمل يهدف إلى الحفاظ على التفوق التكنولوجي للجيش الأمريكي ضد المنافسين العالميين في مجال توظيف أنظمة التحكم الذاتي المعتمدة على تقنيات الذكاء الاصطناعي في المجالات الأمنية والعسكرية.

وتتمثل أهمية الأنظمة ذاتية التحكم في قدرتها على تنفيذ الأدوار التي يؤديها البشر في المهام الأمنية الخطرة التي تُعرِّض أرواحهم للخطر، من خلال استخدام الآليات والأجهزة الذكية ذاتية التحكم وتسخيرها للقيام بأعمال أكثر تعقيدًا من الناحية المعرفية، ويؤكد الخبراء أن المؤسسات الأمنية والعسكرية ستحقق فوائد جمّة من استخدام الأنظمة ذاتية التحكم من خلال استبدالها بالبشر في المهام المملّة أو الخطرة أو القذرة (Ryan, 2018)، وتشمل الأمثلة مجالات متعددة منها: جمع معلومات استخبارية طويلة الأمد وتحليلها، وتحديد وتطهير البيئات الملوثة بالأسلحة الكيميائية والنووية، ومسح الأجهزة المتفجرة، والعمليات القتالية التي يصعب قيام البشر بتنفيذها، وغيرها من المجالات في السياق نفسه، وفي هذه الأدوار، قد تقلل الأنظمة ذاتية التحكم من المخاطر التي يتعرض لها العنصر البشري وتعمل على تخفيض التكاليف على الأمد البعيد.

2. 1. 2. السرعة والتحكم (Speed and Control)

تعد تقنيات الذكاء الاصطناعي وأدواته المختلفة وسيلة فريدة للعمل في الجوانب الأمنية والعسكرية في أقصى الحدود الزمنية، حيث توفر الأنظمة التي

لديها القدرة على الاستجابة بسرعة جيجا هيرتز، والتي تمتلك بدورها القدرة على تسريع وتيرة العمليات الأمنية والعسكرية بشكل عام. ويزعم بعض المحللين الأمنيين أن الزيادة الحادة في وتيرة القتال يمكن أن تزعزع الاستقرار، خاصة إذا تجاوز القدرة البشرية على فهم الأحداث والسيطرة عليها، كما يمكن أن يزيد من إمكانات النظام المدمرة في حالة فقدان التحكم والسيطرة على النظام.

وعلى الرغم من هذه المخاطر، فقد يدعي بعضهم أن السرعة ستوفر ميزة حربية، وهو ما يُوجِد بدوره ضغوطًا من أجل تحقيقها على نطاق واسع في التطبيقات العسكرية المعتمدة على الذكاء الاصطناعي، وبالإضافة إلى ذلك، قد توفر أنظمة الذكاء الاصطناعي فوائد في المهام طويلة الأمد التي لا تتحملها قدرة البشر، مثل: جمع المعلومات الاستخبارية عبر مناطق واسعة على مدار حقب زمنية طويلة، وكذلك القدرة على اكتشاف الحالات الشاذة بشكل مستقل وتصنيف السلوك.

2. 1. 3. التدرج (Scaling)

تقوم تقنيات الذكاء الاصطناعي بتعزيز القدرات البشرية في الجوانب الأمنية والعسكرية من خلال تطوير أنظمة أمنية وعسكرية حديثة أقل تكلفة وبقدرات استثنائية، فعلى سبيل المثال، وعلى الرغم من أن طائرة فردية دون طيار منخفضة التكلفة قد تكون عاجزة ضد مقاتلة حديثة (مثل: الشبح F-35)؛ فإن سربًا من هذه الطائرات دون طيار يمكن أن يطغى على الأنظمة القتالية الفائقة، وهو ما يعني ترشيدًا كبيرًا في تكاليف الأنظمة الدفاعية.

ومن جانب آخر، يمكن لأنظمة الذكاء الاصطناعي أن تزيد من إنتاجية التقنيات الدفاعية والأمنية التي تتولى المهام الروتينية التي بدورها تتطلب الحد الأدنى من تدخل العنصر البشري.

وفي هذا السياق، يفيد بعض المحللين الأمنيين أن انتشار أنظمة الذكاء الاصطناعي قد يقلل من ارتباط القوة الأمنية والعسكرية بحجم السكان وبالقوة الاقتصادية للبلد، وهو ما يُمكّن البلدان الصغيرة والمنظمات غير الحكومية من رفع كفائة جيوشها، إذا استطاعت الاستفادة من قدرات تقنيات الذكاء الاصطناعي.

2. 1. 4. تفوق المعلومات (Information Superiority)

قد توفر تقنيات الذكاء الاصطناعي وسيلة للتعامل مع الزيادة الهائلة في كمية البيانات المتاحة للتحليل (تحليل البيانات الضخمة)، فعلى سبيل المثال، ووفقًا لأحد المصادر في وزارة الدفاع الأمريكية، "يقوم الجيش الأمريكي باستخدام أكثر من 11000 طائرة دون طيار في مهام أمنية مختلفة، حيث إن كل طائرة تقوم بالتقاط صور ومقاطع فيديو عالية الوضوح يوميًّا وهو ما يوفر بيانات ضخمة يقاس حجمها بالزيتابايت "Zettabytes"، التي بدورها تتطلب جهدًا ضخمًا وكوادر بشرية هائلة لتمشيطها وتحليلها، وهو ما قد يشكل عبئًا كبيرًا على الجهات الأمنية والعسكرية،

ناهيك عن الدقة التي يمكن أن تتأثر سلبًا نتيجة الأخطاء البشرية.

وحيث إن حجم البيانات مستمر في النمو، وبالنظر إلى اختلاف بنيتها وطبيعتها وشموليتها؛ فإنه من المحتمل أن تتفاقم مشكلة تمشيطها وتحليلها في المستقبل لانعدام الكوادر الكافية للتعامل مع هذه البيانات، فقد أفادت واحدة من الدراسات العلمية أنه من المتوقع بحلول عام 2020م أن يسهم كل إنسان على الأرض في إنتاج 1,7 ميغابايت من المعلومات كل ثانية، وبالتالي، سيزداد حجم البيانات على مستوى العالم، الذي يُنتج كل ثانية 4.4 zettabytes اليوم، إلى قرابة 44 zettabytes؛ أي بمقدار (10) عشرة أضعاف (Marr, 2015).

وتوفر الأنظمة المعتمدة على تقنيات الذكاء الاصطناعي القدرة على التكامل والتحليل لمجموعات كبيرة من البيانات الضخمة، التي يتم توليدها من خلال مصادر مختلفة من أجل تحديد الأنماط المختلفة في هذه البيانات وتسليط الضوء على المفيد منها، من خلال ما يسمى بالتحليل الاستخباري للبيانات (Threat Intelligence)، الذي يكون أحد مخرجاته التقارير المكتوبة أو الرسومات المعبرة (Written Reports and Informative Charts) (Marr, 2015).

وبناءً على ما سبق، نخلص إلى أن أدوات الذكاء الاصطناعي تمنح القدرة على تحسين نوعية ودلالة المعلومات التي تستنبطها وتوفرها لصناع القرار، وهو ما يمنحهم ميزة إيجابية في التعامل مع العمليات الأمنية والعسكرية ودعم اتخاذ القرار.

2. 1. 5. القدرة على التنبؤ (Predictability)

غالبًا ما تنتج خوارزميات الذكاء الاصطناعي نتائج غير متوقعة وغير تقليدية، ففي مارس 2016م، أنشأت شركة DeepMind المتخصصة في تقنيات الذكاء الاصطناعي "خوارزمية لعب" تسمى Alpha-Go، التي هزمت بطل العالم "لي سيدول" في لعبة Go بنتيجة أربع مباريات إلى واحدة. وبعد المباراة، علَّق "سيدول" على ذلك بأن خوارزمية Alpha-Go قامت بحركات مفاجئة ومبتكرة، وهذا ما أكده لاعبون آخرون في لعبة Go في وقت لاحق، موضحين أن AlphaGo أثبتت الحكمة في اتخاذ القرار في أثناء اللعب.

وإن قدرة الذكاء الاصطناعي على تحقيق نتائج غير تقليدية مماثلة في سياق أمني/عسكري قد توفر ميزة في القتال، خاصة إذا كانت هذه النتائج مفاجئة للطرف الآخر (الخصم). ومع ذلك، فإن تقنيات الذكاء الاصطناعي عرضة للخطأ، وغالبًا ما تكون أخطاؤها كارثية في الظروف الحرجة؛ ولذلك ينبغي اختبارها من ناحية الفاعلية والكفاية في ظروف أسوأ من الواقع.

وفي تجربة لقياس مدى فاعلية أدوات الذكاء الاصطناعي في مجال العمل الأمني، تم اختبار إحدى أدوات الذكاء الاصطناعي للتعرف على الصورة المعروضة، حيث وصف نظام الذكاء الاصطناعي الصورة بأنها "فتى صغير يحمل مضرب بيسبول" وهي ليست كذلك، وهو ما يدل على عدم قدرة الخوارزمية المستخدمة على فهم السياق، حيث تم

اقتصار التعرف على الشكل حرفيًّا؛ لذلك يحذر بعض الخبراء من أن الذكاء الاصطناعي قد يعمل بافتراضات مختلفة عن البيئة بخلاف ما يعمل به البشر وهو توظيف السياق (The context).

وبالمثل، قد تخضع أنظمة الذكاء الاصطناعي للتحيز في افتراضاتها وقراراتها، نتيجة لبيانات التدريب الخاصة بها، فعلى سبيل المثال، اكتشف الباحثون مرارًا حالات من التحيز العنصري في أنظمة الذكاء الاصطناعي الخاصة بالتعرف على الوجوه بسبب قلة التنوع/ الأنماط في الصور، التي تم تدريب الأنظمة عليها، وهذا بدوره قد يكون له آثار كبيرة على قرارات تطبيقات الذكاء الاصطناعي في السياقات الأمنية والعسكرية، خاصة إذا بقيت مثل هذه التحيزات غير مكتشفة وأُدمِجت في أنظمة ذات طابع حساس وحرج؛ ولذلك ينبغي الانتباه إلى هذه النقطة، والحرص على تنوع البيانات والأنماط والسياقات عند إنشاء أو تطوير خوارزميات الذكاء الاصطناعي، واختبارها مرات كافية؛ لضمان دقة قراراتها وقدرتها على التكيف.

ويمكننا القول إن "القدرة على التكيف في المجال"، أو قدرة أنظمة الذكاء الاصطناعي على التكيف بين بيئتين متباينتين، قد ينتج عنها تحديات عند استخدام أدوات الذكاء الاصطناعي في المجالات الأمنية والعسكرية، فعلى سبيل المثال، تم تطوير أحد أنظمة الذكاء الاصطناعي لتحليل وفهم النصوص على الإنترنت، الذي تم تدريبه على مستندات رسمية "مقالات ويكيبيديا"، حيث تم اختبار النظام لاحقًا على نصوص أحد مواقع التواصل الاجتماعي (تويتر)، التي غالبًا ما يستخدم رُوَّادُها اللغات غير الرسمية، ففي حال نجح النظام في تصنيف نصوص بيئات متعددة بالأداء نفسه ، فعندها يمكن تعميمه، وبالمقابل، قد تحدث حالات فشل في القدرة على التكيف عند نقل الأنظمة، التي يتم تطويرها في بيئة مدنية ولغايات مدنية، إلى بيئة أمنية أو عسكرية، ويعود ذلك إلى اختلاف المجال أو السياق (Scharre, 2017).

وقد يتسبب فشل نظام الذكاء الاصطناعي في أخطار كبيرة إذا تم تعميمه. وقد لاحظ أحد المحللين الأمنيين أنه على الرغم من أن البشر ليسوا محصنين من الأخطاء، إلا أن أخطاءهم عادةً ما تكون فردية، وتميل إلى الاختلاف في كل مرة يقع فيها الخطأ، على عكس ذلك، تتسم الأنظمة التي تعتمد على الذكاء الاصطناعي بتكرار أخطائها بالطريقة نفسها، وهو ما قد ينتج عنه تبعات واسعة النطاق أو مدمرة. وعليه، قد تنشأ نتائج غير متوقعة عندما تتفاعل أنظمة ذكاء اصطناعي مع أنظمة ذكاء اصطناعي أخرى مدربة على مجموعة بيانات مختلفة ذات معايير تصميم مختلفة وانحرافات ثقافية (Kania, 2017). ويحذر المحللون من أنه في حالة اندفاع الجيوش ومختلف قطاعات الأمن لإدخال التكنولوجيا، وخصوصًا تلك التي تعتمد على تقنيات الذكاء الاصطناعي في عملياتهم وأسلحتهم، دون الحصول على فهم شامل للأخطار المحتملة، فقد يتحملون تبعات ثقيلة، وهو ما يشير إلى تأثير استخدام أنظمة الذكاء الاصطناعي، التي تنطوي على حد أدنى من المخاطرة في حال عملها بشكل فردي، ولكنها تزيد من الأخطار في حال

تفاعلها مع الأنظمة الأخرى. إجمالاً، قد تتفاقم هذه الأخطار في حالة حدوث سباق تسلح تقني.

2. 2. التحديات

تقدم تقنيات الذكاء الاصطناعي كثيرًا من الفرص، التي يمكن توظيفها في المجالات الأمنية والعسكرية، إلا أن هذه التقنيات تفرض بعض التحديات التي ينبغي أن يتم الالتفات إليها وأخذها بعين الاعتبار، ومن أبرز التحديات ما يأتي:

2. 2. 1. نقاط الضعف (Vulnerabilities)

يزيد انتشار أنظمة الذكاء الاصطناعي من عدد الأشياء القابلة للاختراق (مثل: إنترنت الأشياء)، بما في ذلك أنظمة الطاقة الحركية الذكية، التي تتضمن المركبات والطائرات الذكية وأنظمة الدفاع الجوي، والتي بدورها قد تسهم في إحداث آثارٍ فتاكة يمكن أن تكون ضارة، خاصةً إذا كانت هناك منظومة متكاملة من الأنظمة، التي تعتمد على الذكاء الاصطناعي، ولديها نقاط الضعف نفسها القابلة للاستغلال، بالإضافة إلى ما سبق، فإن أنظمة الذكاء الاصطناعي معرضة بشكل خاص للسرقة؛ لأنها تعتمد على البرمجيات، فعلى سبيل المثال، لتقليد نظام دفاعي فعّال، فإن فهمه وتحليله وتأمين مواده عادةً ما يكون مكلفًا من ناحية الوقت والجهد، في حين أن هذه الأنظمة الذكية معرضة للسرقة، وهو ما يُسهِّل مهمة إعادة إنتاجها بوقت وجهد أقل.

ويجدر بالذكر أنه يوجد كثير من تطبيقات الذكاء الاصطناعي، التي تستخدم في المجالات المدنية، التي يمكن إساءة استخدامها بشكل ضار يسهم في التأثير على الأمن الوطني أو القومي لدولة ما.

وقد يتمكن المخترقون من إحداث بعض الفجوات في الأنظمة المصممة للتنبؤ، التي تعتمد في عملها على الشبكات العَصبُونِيَّة على سبيل المثال، فقد تبين بعد اختبارها إمكانية تعديل المدخلات، التي بدورها يمكن أن تُفشل عمل النظام برمته، وخصوصًا في حال التعامل مع بيانات ضخمة، مثل: الصور الواردة من كاميرات المراقبة والاستطلاع.

واستطاع بعض الباحثين في أحد الاختبارات الوصول إلى خوارزمية وبيانات التدريب في أحد أنظمة تصنيف الصور للمركبات العسكرية الذكية، وقاموا ببعض التغييرات التي تجعل من المركبة العسكرية تفسر إشارة التوقف على أنها إشارة تحديد السرعة، وبالتالي قد تتأثر فاعليتها.

ويتضح مما سبق، أن هناك نقاطَ ضعفٍ تُسهِّل اختراق النظام وتعديله، إما من خلال البيانات وإما من خلال النموذج نفسه، حيث إن أغلب الأنظمة الذكية تتعامل مع كميات ضخمة من البيانات، وهو ما يُمكِّن المخترقين من تجاوز إجراءات الأمن واختراقها، من خلال الوصول إلى بيانات التدريب أو الوصول إلى المدخلات نفسها، ولحماية الأنظمة الذكية من الاختراق من خلال البيانات المدخلة أو بيانات التدريب، فإنه يتم عادة تدريب النظام من خلال تضمين حالات اختراق أو حالات مشبوهة؛ ليتم اكتشافها مستقبلاً في حال حدوثها.

2. 2. 2. شفافية النظام (System Transparency)

تتطلب التطبيقات المعتمدة على تقنيات الذكاء الاصطناعي كثيرًا من المتطلبات؛ لكي تكون مجدية، وتتمثل أبرز هذه المتطلبات في الأداء الفعّال ومستوى أمان عالٍ وثقة المستخدم؛ إضافةً إلى الشفافية العالية، وهذه المتطلبات تعتبر أساسية في كثير من التطبيقات (مثل: أنظمة السلامة الحرجة، وأنظمة المراقبة الأمنية والعسكرية، والتشخيص الطبي، وغيرها من التطبيقات الحساسة)؛ فإنه، وعلى الرغم من التميز الذي أثبتته خوارزميات الذكاء الاصطناعي مؤخرًا، فقد ظهر هناك اهتمام بحثي متزايد بمجال الشفافية في هذه التطبيقات.

وعلى عكس الأنظمة المغلقة (Black Box Applications)، تعتمد الشفافية المطلوبة لخوارزميات الذكاء الاصطناعي على احتياجات المستخدمين النهائيين، الذين تتمثل أبرز احتياجاتهم في الثقة بتوصيات وقرارات النظام في المواقف التي يصعب فيها على المستخدمين التشكيك في توصيات النظام، ومع ذلك، قد يكون من غير الواضح ما إذا كانت ثقة المستخدم تعتمد على أداء النظام أو متانته، أو الأداء النسبي للمستخدم، أو مدى ارتياح المستخدم لتوصيات النظام، أو معرفة حدود أداء النظام بسبب تعميم النموذج مقارنة بقدرات المستخدمين، أو بعض المعلومات الإضافية حول توصيات النظام متمثلة بحيثيات اتخاذه لقرار معين دون غيره. ومن جهة أخرى، يحتاج المستخدم النهائي التأكد من العدالة في اتخاذ القرار من خلال تجنب التحيز، الذي قد يؤدي حال تحققه إلى عدم المساواة في المعاملة في الحالات المختلفة، كأن تعتمد طلبات الائتمان على الجنس أو العرق.

ومن حيث المبدأ، هناك طريقتان لجعل أنظمة الذكاء الاصطناعي شفافة، ولزيادة ثقة المستخدم بدقة ونجاعة قراراتها:

الطريقة الأولى: يُنظر إلى بعض أنواع النماذج الذكية على أنها أكثر قابلية للتفسير من غيرها، تلك التي تُصنَّف على أنها نماذج خطية، أو أنظمة مستندة إلى قواعد أو مجموعة قرارات تتيح للمستخدم فهم تكوينها وطريقة عملها وفهم خوارزمية التدريب فيها.

الطريقة الثانية: قد يفسّر النظام كيفية الوصول إلى توصياته إما نصيًّا أو رسوميًّا. فعلى سبيل المثال، يمكن أن تفسر أنظمة تصنيف الصور قراراتها أو توصياتها من خلال الإشارة إلى الجوانب التي استندت إليها خوارزمية التصنيف في تصنيف الصور، أو من خلال تمييز خصائص الإدخال للصور تحت التصنيف، التي قد تسلط الضوء على المناطق، التي تقدم أدلة لصالح أو ضد المشـــــكلة قيد البحث (Lipton, 2018).

2. 2. 3. البيانات (Data)

يُعد تطوير التطبيقات المستندة إلى تقنيات تعلم الآلة "Machine Learning" في المجالات الأمنية والعسكرية أمرًا صعبًا مليئًا بالتحديات، ويُعزى ذلك إلى أن الإجراءات الخاصة بجمع البيانات من المنشآت الأمنية والعسكرية، ومنشآت التدريب، وشبكات الاستشعار، والتسليح، وغيرها، لا تتعلق

باستخدام تلك البيانات في البحث العلمي والتطوير، بل من أجل غايات أمنية وعسكرية لا يطلع عليها إلا المصرح لهم بذلك في تلك المنشآت، ونتيجة لذلك، فإنه غالبًا ما يصعب في هذه المجالات العثور على مجموعة بيانات واقعية وعالية الجودة وكبيرة بما فيه الكفاية لاستخدامها في تعليم وتدريب النماذج الذكية؛ فإن كان مركز البحث والتطوير ملكًا لتلك المنشآت العسكرية، وهذا بدوره يُعتبر أحد أبرز التحديات، خصوصًا إذا كانت عملية التطوير بمشاركة مطور خارجي (قطاع خاص).

وتعد محدودية بيانات التدريب تحديًا رئيسًا، حيث لا تتوافر البيانات الكافية في مجال معين، وخصوصًا في المجالات الأمنية والعسكرية، أو أنها تكون متاحة ولكن ليس بالجودة والدقة والكمال المطلوب، وهو ما يتطلب الانتقال إلى البديل وهو نقل بيانات التدريب من نموذج آخر مصمم للغاية نفسها المنشودة من النموذج المزمع تطويره، وهذا ما يعرف علميًّا بـ "نقل بيانات التدريب".

ومن أجل التغلب على تحدي محدودية البيانات، فقد شرع الباحثون في إجراء التجارب المتكررة إلى أن وصلوا إلى طريقة ناجعة تعتمد على طريقة تدريب النماذج باستخدام الطريقة شبه الإشرافية "Semi-Supervised Learning"، وتكون هذه في الحالات، التي يكون فيها حجم البيانات المعنونة "la-beled" قليلًا، بحيث يتم الاعتماد على دمج الكمية المحدودة المتاحة من البيانات المعنونة مع حجم كبير نسبيًّا من البيانات غير المعنونة في الوقت نفسه، ويتم ذلك من خلال مرحلتين؛ الأولى يتم فيها تدريب المولّد "Generator" لإنتاج بيانات وهمية، والثانية يتم من خلالها تدريب المتميز discriminator على تصنيف البيانات على أنها بيانات حقيقية أو مزيفة (Good-fellow et al., 2014).

3. نقاش تحليلي

ما تقدم من تفاصيل يدور حول ماهية الذكاء الاصطناعي، وفرص استثماره في المجالات المختلفة، خاصة الأمنية والعسكرية، وما يصاحب ذلك من تحديات فنية وتقنية وأخلاقية وقانونية قد تحول دون أن تؤدي تقنيات الذكاء الاصطناعي وأدواته دورها المأمول.

وعليه، يتمحور النقاش فيما يأتي حول مجالات عدة، تتضمن الفرص والتحديات، ومجالات التطبيق، والتوصيات والرؤى المستقبلية:

3. 1. الفرص والتحديات

وفي ضوء ما سبق من ميزات استثنائية يمكن أن تقدمها تطبيقات الذكاء الاصطناعي، فإن بعض الدول قد تندفع إلى التحول التقني في المجالات شتى وخاصة المجالات الأمنية والعسكرية دون وضع إستراتيجية مثلى للتحول، معتمدين في ذلك بشكل كلي على استيراد هذه التقنيات وتشغيلها والتحكم بها من خلال الجهات المزودة لها بشكل كامل أو جزئي، وهو ما ينتج عنه بعض السلبيات، مثل: التبعية وعدم امتلاك السيطرة المطلقة على هذه التقنيات، التي قد تصل في إحدى مراحلها إلى الابتزاز، ناهيك عن

التشارك مع الجهة المزودة بالبيانات، التي غالبًا ما تعتبر حساسة بطبيعتها، وفي بعض الأحيان يمكن أن تستخدم هذه التقنيات في أغراض أخرى، مثل: التجسس؛ لذلك ينبغي وضع مجموعة من الضوابط في جميع الأحوال عند استيراد هذه التقنيات، مثل: محدودية الوصول إلى التفاصيل الحساسة، واتفاقية استخدام لما يتم الوصول إليه من بيانات من قبل الجهات المزودة تخص هذه المنشآت؛ إضافة إلى شرط نقل المعرفة قبل نهاية المشروع، وغيرها من البنود التي تضمن حق الجهة المستخدمة لهذه التقنيات.

وتعد رؤية المملكة العربية السعودية 2030 من أكثر الأمثلة على الإستراتيجيات الفعّالة في التحول، الذي فرضه الواقع السياسي والاقتصادي والعسكري في الشرق الأوسط، فهي رؤية إستراتيجية ببرامج واضحة وثابتة تسعى إلى استثمار جميع المقدرات والموارد المتاحة وإلى توطين المجالات كافة؛ ابتداءً بالحرجة والحساسة منها وانتهاءً بالتقليدية. ولعلنا نقتبس جملة من افتتاحية هذه الرؤية لصاحب السمو الملكي الأمير محمد بن سلمان: "نلتزم أمامكم أن نكون من أفضل دول العالم في الأداء الحكومي الفعّال لخدمة المواطنين، ومعًا سنكمل بناء بلادنا؛ لتكون كما نتمناها جميعًا مزدهرةً قويةً، تقوم على سواعد أبنائها وبناتها، وتستفيد من مقدراتها، دون أن نرتهن إلى قيمة سلعة أو حراك أسواق خارجية"، وهذا يعزز ما تم ذكره سابقًا باستقلال الصناعات وعلى رأسها الأمنية والعسكرية، والاعتماد على الكوادر الوطنية في صنع وتطوير التقنية بدلاً من استيرادها، وذلك وفق مجموعة من البرامج التي تمثل إستراتيجية التحول على شتى الصُّعُد.

أما فيما يتعلق بتوافر البيانات المطلوبة؛ لتبني تقنيات الذكاء الاصطناعي وأدواته المختلفة في العمل الأمني والعسكري على المستويين الوطني والقومي؛ ابتداءً من تصريف الأمور الحياتية الروتينية، مثل: تنظيم حركة المرور ورصد المخالفات، ومرورًا بآليات المراقبة والتتبع والاستشراف والأعمال الشرطية المختلفة ومراقبة الفضاء السيبراني، وانتهاءً بالنشاطات العسكرية من وقاية ومكافحة واستجابة وتصنيع عسكري ذكي، فيُعد ما سبق من أبرز التحديات على الساحة، فكما هو معروف عن طبيعة سلوك أغلب دول الشرق الأوسط، الذي يغلب عليه الطابع الاستهلاكي حتى العقد الأخير؛ فإن الجهود والرؤى الإستراتيجية في بعض بلداننا قد بدأت في النضج، وانعكس ذلك من خلال البدء في مشاريع توطين الصناعات الأمنية والحربية، وإنشاء مراكز البحث والتطوير العسكرية، ونقل الخبرة والمعرفة والتبادل الأمني المعلوماتي بين الدول العربية والأجنبية.

وللتغلب على محدودية البيانات إجمالاً، والمعنون منها على وجه الخصوص، فقد حملت الأدبيات في مجال الذكاء الاصطناعي وتعلم الآلة مجموعة من الحلول البديلة التي قد تسهم في البدء بإطلاق الدراسات التجريبية في مجال التحول الرقمي وتوظيفه في النشاطات الأمنية والعسكرية، ولعل أبرز هذه البدائل ما ورد سابقًا في هذه الورقة والمتمثل في تبني أسلوب التعلم بالطريقة شبه الإشرافية، بحيث

يتم الاعتماد على البيانات المعنونة وغير المعنونة في تعلم الآلة من الحالات السابقة، وتوظيفها في التنبؤ المستقبلي واستقلالية اتخاذ القرار، ومن ناحية أخرى، فإن أحد الحلول يتمثل في تدريب الآلة على بيانات تكون في السياق نفسه، وفي تعميم النموذج وتكييفه في المجالات العسكرية، فعلي سبيل المثال، لتصميم نموذج للتعرف على الميول الشخصية لمرتادي الإنترنت ووسائل التواصل الاجتماعي، فإنه من الممكن تدريب النموذج على بيانات نصية عامة من أي نوع ومن ثم تعميمه.

ومن جانب آخر، قد تكون التشريعات والقوانين في بعض الأحيان عائقًا أمام جمع البيانات وتحليلها، وهنا نقصد البيانات عن الأفراد والجماعات لما تتضمنه هذه القوانين من حفظ الخصوصية، فعلى سبيل المثال في الجرائم الجنائية المحلية، لو أن أحد الأدلة في شريط تسجيل إحدى كاميرات المراقبة داخل أحد المنازل، فإن الاطلاع على مضمونه وتحليله قد يتطلب إجراءات قانونية طويلة، وفي مثال آخر لجريمة عابرة للحدود، فإن كان الدليل على ارتكاب إحدى الجرائم يتمثل في معلومات حساب على أحد مواقع التواصل الاجتماعي، فإن قوانين الخصوصية في تلك المواقع تمنع مشاركة معلومات صاحب الحساب مع الجهة الأمنية، إلا في بعض الجرائم مثل: الجرائم الإرهابية وجرائم استغلال الأطفال جنسيًّا عبر الإنترنت، والجرائم المنظمة بحسب اتفاقية فيينا، التي صدرت نسختها الأخيرة في شهر أكتوبر 2015م، ويقودنا هذا كله إلى ضرورة إعادة النظر في بعض القوانين والتشريعات، التي تمنع الجهات الأمنية والعسكرية من الوصول إلى بيانات معينة بداعي حفظ الخصوصية.

وفي هذا السياق، نذكر التجربة الفرنسية بالمصادقة على "الإستراتيجية الوطنية للذكاء الاصطناعي، التي تشمل خططًا تنشر فيها الدولة مجموعات بيانات القطاعين العام والخاص على هيئة بيانات مفتوحة، تُستخدم في تطبيقات الذكاء الاصطناعي بما يخدم المصلحة العامة، وحددت الإستراتيجية أربعة قطاعات بوصفها ذات أولوية، وهي: قطاعات الصحة والنقل والبيئة والدفاع، وتقضي الإستراتيجية بإصدار تشريعات تدعم استخدام البيانات الصادرة عن القطاعين العام والخاص بما فيها البيانات الشخصية، وذلك بحسب حساسية البيانات. فعلى سبيل المثال، يمكن للأطباء الاستفادة من البيانات الشخصية الصادرة عن أجهزة إنترنت الأشياء (Internet of Things) الشخصية، مثل: الساعات في تشخيص وعلاج المرضى، وكذلك يمكن للباحثين استخدام البيانات الصادرة عن كاميرات المراقبة (CCTV) المنتشرة في الطرق لتدريب السيارات ذاتية القيادة، وتستطيع مولدات الكهرباء إدارة الطاقة بعد معرفة أوقات ذروة الاستخدام من العدادات الذكية. ويجدر بالذكر أنه في حال نجاح تطبيق الإستراتيجية الفرنسية، فستكون أول دولة تفرض استخدام البيانات الشخصية دون مخالفة" (Villani, 2018).

3. 2. مجالات التطبيق

لقد أوضحنا سابقًا أن تقنيات الذكاء الاصطناعي تعد حاليًّا أدوات أساسية في كثير من المجالات، التي

من أبرزها المجالات الأمنية والعسكرية، وتعد مجالات التطبيق في تلك المجالات كثيرة ومتشعبة، ولا يمكن حصرها بمقالة واحدة، ولكن يمكن التطرق إلى أبرزها في مجالات التطبيق المختلفة:

- قطاع المرور

إننا نلمس في هذه الأيام نشاطًا كبيرًا في توظيف تقنيات الذكاء الاصطناعي في مجالات أمنية متعددة، ولكن لا بد من تكثيف الجهود لتوظيف هذه التقنيات بشكل أفضل، وإن الجهود المبذولة في أغلب البلدان في قطاع المرور بشتى مجالاته ملحوظة، ولكن لا بد من توسيع دائرة رصد المخالفات آليًّا، حيث إنها تقتصر حاليًّا على المخالفات العامة، وأمر شمول المخالفات كافة من خلال التعرف على أنماطها ذاتيًّا، وتفعيل توظيف تسجيلات كاميرات المراقبة في الطرق العامة والفرعية من خلال تحليلها واتخاذ القرارات ذاتيًّا من أجل تسهيل حركة المرور، ناهيك عن تفعيل خاصية الإشارات الضوئية الذكية، وغير ذلك من مجالات هذا القطاع هو أمر ضمن الإمكانات المتاحة، خاصة وأن البنية التحتية تدعم ذلك.

- أمن الفضاء السيبراني

هو مجال مليء بالتحديات، فهو يعد مجالاً خصبًا بشكل خاص بسبب مواطن الضعف الناجمة عن استخدامات التقنية بشكل عام، ومن هنا لا بد من تفعيل استخدام تقنيات الذكاء الاصطناعي لحمايته، خصوصًا وأن الزمن الحالي هو عصر الحروب الإلكترونية، التي ينتج عنها تعطيل الخدمات الإلكترونية، وتعطيل أنظمة البنى التحتية، والهجوم الآلي عن بعد من خلال الطائرات المسيرة (الدرونز)، وحرب الشائعات وتضليل الرأي العام، والاستغلال والاحتيال عبر الإنترنت وغير ذلك، وهو ما يشكل مصدر تهديد للمصالح العامة والأمن الوطني والقومي. أدى ذلك إلى توجه واضح وجهود كبيرة للدول العربية في هذا المجال، حيث إن أغلب الدول تحرص على إنشاء إدارات متخصصة في الأمن السيبراني على جميع المستويات.

- مجال مراقبة الحدود

سواء أكانت البرية منها أم البحرية أم الجوية، وتعد المطارات ومحطات القطارات جميعها مجالات لتطبيقات الذكاء الاصطناعي، حيث يمكن استشعار الحركة المشبوهة، والتعرف على الوجوه، وغير ذلك من إمكانات تخدم هذه الأغراض.

- النمذجة والمحاكاة

تهدف إلى اكتشاف الواقع ومحاكاته تحت عنوان "الواقع الافتراضي" الذي تتعدد فوائده؛ إذ إنه يُساعد في إجراء التجارب مرات عدة بمساعدة الحواسيب والتقنية، وفي اكتشاف جوانب خفية من الواقع، وفي اكتشاف أنماط مُتكررة ربما كان من الصعب تبينها على أرض الواقع؛ فعلى سبيل المثال، عند تعرض ولاية فلوريدا لإعصار كان من أبرز آثاره عجز محطات الوقود عن توفير ما يكفي من الوقود عبر الطرق السريعة، التي تتجه شمالًا خارج فلوريدا، الأمر الذي يشل حركة المرور على الطرق، ويجعل عملية الإجلاء أكثر صعوبةً وفوضوية، وعندها افترض بعضهم أن نقص الوقود هو السبب وراء هذه الحالة، في حين كشفت المحاكاة أن السر يكمن في انقطاع التيار الكهربائي عن المحطات، ما أدى إلى عجزها عن

تشغيل مضخات الوقود، وقادت هذه الواقعة إلى سن قواعد جديدة تشترط على محطات الوقود الواقعة على طرق الخروج من الولاية تركيب مُوِّلدات تعمل بالوقود لتشغيل المضخات في حالات الطوارئ، ولنا أن نقيس ذلك على جميع الظروف الأمنية المختلفة.

4. الخاتمة

4. 1. الخلاصة والاستنتاجات

يسهم النضج الملحوظ في خوارزميات الذكاء الاصطناعي في الوقت الراهن في إحداث طفرة نوعية في كثير من التطبيقات التقليدية للذكاء الاصطناعي، مثل: تعلم الآلة، ورؤية الكمبيوتر، ومعالجة اللغات الطبيعية، واستنباط المعرفة، والروبوتات وغيرها من التطبيقات، وهو ما دفع الباحثين وأصحاب القرار إلى تكثيف الجهود لاستغلال هذه التطورات وتوظيفها في كثير من المجالات وخاصة في التطبيقات الأمنية والعسكرية، مثل: المراقبة والاستطلاع، وتقييم التهديدات والحروب، والدفاع، والنمذجة والمحاكاة، والأمن السيبراني، والتحليل الاستخباري، والقيادة والسيطرة، والتعليم والتدريب... إلخ. وبالرغم من ذلك؛ فإن هناك كثير من التحديات والمحددات التي ينبغي مراعاتها عند توظيف الذكاء الاصطناعي في المجالات الأمنية والعسكرية.

فعلى سبيل المثال، تعني الأخطار الكبيرة في التطبيقات العسكرية، التي تتبنى تقنيات الذكاء الاصطناعي، أن هذه الأنظمة يجب أن تكون شفافة؛ لكسب ثقة صانع القرار والمستخدمين، ولتسهيل تحليل الأخطار، ويعتبر هذا من أبرز التحديات لهذا النوع من التطبيقات، ويعزى ذلك إلى أن كثيرًا من التقنيات المستخدمة في هذه التطبيقات، هي عبارة عن صناديق سوداء مغلقة تفتقر إلى الشفافية الكافية.

ومن ناحية أخرى، ينبغي أن تتمتع هذه الأنظمة بالقوة والموثوقية؛ لأنها قد تكون عرضة للتلاعب غير المحسوس ببيانات الإدخال أو بالبرنامج المصدري.

ويعتمد كثير من تقنيات الذكاء الاصطناعي على التعلم الآلي، الذي بدوره يتطلب كميات كبيرة من بيانات التدريب، التي تعتبر شحيحة في المجالات الأمنية والعسكرية؛ وهو ما يشكل تحديًا آخر، وقد ناقشت هذه الورقة مجموعة من الموضوعات التي تضمنت تطبيقات الذكاء الاصطناعي في المجالات العسكرية والأمنية، وأبرز الفرص التي تقدمها هذه التقنيات والتحديات المقابلة لها، التي قد تحدّ من توظيفها، وبعد تحليل ما سبق من موضوعات، جرى تقديم مجموعة من التوصيات، التي كان من أبرزها ضرورة تفعيل دور مراكز البحث والتطوير في هذه القطاعات مع تركيزها البحثي على تطوير منتجات ذكية تلبي حاجات صاحب القرار.

4. 2. التوصيات

في ضوء ما سبق، ونظرًا للواقع الحالي في مجال صناعة الذكاء الاصطناعي، فلعل الآتي من التوصيات يكون له الأثر الإيجابي في تطوير العمل الأمني والعسكري:

- إنشاء وتفعيل مراكز البحث والتطوير الأمنية والعسكرية وتوطينها

على غرار التجربة الأمريكية من خلال وزارة دفاعها، فقد أطلقت الوزارة كثيرًا من المشروعات التي تهدف إلى زيادة وتطوير التصنيع العسكري وإستراتيجيات الدفاع، ومن أبرز هذه المشروعات الدفاعية التطويرية، التي جرى توظيف إمكانات الذكاء الاصطناعي في أبرز نشاطاتها: وكالة مشروعات البحوث المتقدمة التابعة لوزارة الدفاع (DARPA)، ووكالة مشروعات البحوث المتقدمة التابعة للمخابرات IARPA))، وفريق متعدد الوظائف للحرب الخوارزمية، المعروف باسم Project Maven.

- دعم الأبحاث المركزة على الألعاب الإستراتيجية "Strategic Gaming"

ترتكز إستراتيجية "التلعيب" الألعاب الإستراتيجية على دمج سمات مهمة من تصميم الألعاب الإستراتيجية ومبادئها في سياقات غير ترفيهية في المجالات المدنية والعسكرية والأمنية على حدٍّ سواء. ويتم ذلك من خلال برامج المحاكاة للبيئات الصعبة للمساعدة على تسيير الدوريات في بيئات ليسوا على علم بتفاصيلها، وبرامج أكثر تقليدية، مثل: التدريب على الطيران وعلى الأسلحة وعلى الأساليب الناجعة في الحروب؛ بالإضافة إلى الألعاب الحربية واسعة النطاق التي يتعين على صناع القرار فيها انتقاء أفضل البدائل الإستراتيجية وسط الظروف بالغة الصعوبة.

- اشتراط نقل المعرفة/ الخبرة في التقنيات والنماذج المطورة خارجيًا

يهدف نقل المعرفة إلى تنظيمها من خلال تكوينها، واكتسابها من مصدرها، وتوزيعها، إلى جانب ضمان توافرها للمستفيدين في المستقبل، وذلك عند الاستعانة بأطراف خارجية لاستحداث أو تطوير التطبيقات والأدوات المختلفة في العمل الأمني والعسكري.

- دوريات الأمن الإلكترونية

تشكل الشبكة العالمية العنكبوتية بيئةً خصبةً للخصوم والمهاجمين في استهداف الأمن الداخلي من خلال إطلاق الشائعات والتضليل والاستغلال والاحتيال والاصطياد وغيرها من أشكال الجرائم السيبرانية، التي يجري ارتكابها بعدة طرق وأساليب، وحيث إن الغالبية العظمى من مسببات هذه الجرائم ترجع إلى قصور من جانب المستخدم النهائي، فقد وجب إطلاق حزمة من البرمجيات الذكية لمراقبة جميع النشاطات المشبوهة الواردة والصادرة.

- مراجعة القوانين والتشريعات المتعلقة بحماية الخصوصية

تعد القوانين والتشريعات من التحديات الكبرى، التي تقف عائقًا، أمام العمل الأمني والعسكري وتحقيقاتهما الجنائية؛ فقد يكون مناسبًا مراجعتها بشكل يكفل التوازن بين حرية العمل الأمني والعسكري من أجل فرض الأمن وبين خصوصية الأفراد والمؤسسات، وقد كان للتجربة الفرنسية كما ذكر سابقًا عظيم الأثر في تطوير العمل الأمني في فرنسا.

- تأهيل الكوادر الوطنية

لن يكون الأمن الوطني والقومي في أفضل أحواله

إلا إذا طُوِّر وأُدير من قبل كوادر وطنية، بحيث تكون الاعتمادية على الأطراف الخارجية في حدها الأدنى، وهذا بدوره يتطلب من الجامعات والكليات والمعاهد العسكرية والأمنية التركيز على التأهيل العملي المهني للكوادر على البرامج والمجالات التي تخدم هذا الهدف، مع التركيز على المجالات والتوجهات الحديثة المتمثلة في العمل الأمني والعسكري الذكي، الذي يستند إلى تقنيات وخوارزميات الذكاء الاصطناعي، مثل: مجال الطائرات المسيرة، ومجال التحليل المكاني، ومجال النمذجة والتحقيق الرقمي وغيرها من المجالات التي يجري فيها توظيف الذكاء الاصطناعي في العمل الأمني والعسكري.

- الاستثمار في مجالات الأمن السيبراني، وتحليل البيانات الضخمة والذكاء الاصطناعي وتعلم الآلة

يعتبر الأمن السيبراني، وتحليل البيانات الضخمة، والذكاء الاصطناعي، وتعلم الآلة والنزاهة المالية...إلخ، مجالات حساسة تسهم في حماية الأمن الوطني والقومي، ويتأتى ذلك من خلال تشجيع المشروعات والمبادرات وريادة الأعمال والشراكات مع القطاع الخاص في التطبيقات الأمنية بهذه المجالات، وهو ما يؤدي إلى نتائج مهمة في مجال العمل الشرطي الذكي "Smart Policing".

المصادر والمراجع

المراجع العربية

رؤية المملكة العربية السعودية 2030. (2020). رؤيتنا، المملكة العربية السعودية، العمق العربي والإسلامي، قوة استثمارية رائدة، ومحور ربط القارات الثلاث. تم الاسترجاع بتاريخ 2020/03/01 من الموقع .https://vision2030.gov.sa/#

الهيئة الوطنية للأمن السيبراني. (2020). الصفحة الرئيسية. تم الاسترجاع بتاريخ 2020/03/01 من الموقع https://nca.gov.sa/

المراجع الأجنبية

Meghan Han. (2017, May 17). AI as the New Oil: Saudi Arabia's $500 Billion Smart City. Medium, Retrieved on April 2018. https://medium.com/syncedreview/ai-as-the-new-oil-saudi-arabias-500-billion-smart-city-f7b-63f7c9423. (الرابط لا يعمل والمحتوى غير متوفر)

Kelley M. Sayler. (2019). Congressional Research Service / R45178, Artificial Intelligence and National Security. Retrieved on 01/03/2020 from the website: https://crsreports.congress.gov/product/details?prodcode=R45178.

Kenneth Payne (2018) Artificial Intelligence: A Revolution in Strategic Affairs? Survival, 60:5, 7-32, DOI: 10.1080/00396338.2018.1518374

tion. Retrieved on 29/02/2020. https://www.defense.gov/Newsroom/Releases/Release/Article/1044811/department-of-defense-announces-successful-micro-drone-demonstration/

Ryan, M. (2018). Integrating Humans and Machines. The Strategy Bridge, January, 2.

Marr, B. (2015). mind-boggling facts every business leader must reflect on now. Forbes.

Marr, B. (2015). mind-boggling facts every business leader must reflect on now. Forbes.

Scharre, Paul. (2017). The Lethal Autonomous Weapons Governmental Meeting, Part 1: Coping with Rapid Technological Change, Just Security.

Kania, E. B. (2017). Battlefield singularity: artificial intelligence, military revolution, and China's future military power, Washington, DC: CNAS, November 2017. Costello and Elsa Kania,"Quantum Technologies, US-China Strategic Competition, and Future Dynamics of Cyber Stability," CyCon US.

Lipton, Z. C. (2018). The mythos of model interpretability. Queue, 16(3), 31-57.

Adam Stone. (2017, September 7). Army Logistics Integrating New AI. Cloud Capabilities. 2017.

Michael Rogers. (2016, September 13). Senate Armed Services Committee, hearing to Receive Testimony on Encryption and Cyber Matters. https://www.c-span.org/video/?415163-1/defense-department-officials-testify-cybersecurity-threats

Scott Rosenberg. (2017, August 27). Firewalls Don't Stop Hackers, AI Might, Wired.

DARPA. (2019). Generating Actionable Understanding of Real-World Phenomena with AI. DARPA, January 4, 2019, https://www.darpa.mil/news-events/2019-01-04

Gidget Fuentes. (2018, June 26). Navy Will Test Swarming Underwater Drones in Summer Exercise. USNI News. Retrieved on https://news.usni.org/2018/06/26/navy-will-test-swarming-underwater-drones-summer-exercise

US Department of Defense. (2017, Jan 9). Department of Defense Announces Successful Micro-Drone Demonstra-

CÉDRIC VILLANI. (2018). For a meaningful artificial intelligence towards a French and European strategy. https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf

Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., ... & Bengio, Y. (2014). Generative adversarial nets. In Advances in neural information processing systems (pp. 2672-2680).

Received 12 Mar. 2020; Accepted 14 Apr. 2020; Available Online 01 Oct. 2020

Keywords: *Security Studies, Artificial Intelligence, Electronic Warfare, the Internet of Things.*

الكلمات المفتاحية: الدراسات الأمنية، الذكاء الاصطناعي، الحرب الإلكترونية، إنترنت الأشياء.

*** Corresponding Author:** *Hussein Yosuf Mansour*

Email: *Hmansour@nauss.edu.sa*

doi: *10.26735/SKHN3682*

Production and hosting by NAUSS