

الدَّكَاةُ الاصْطِنَاعِيَّةُ وَتَحْدِيَّاتُ الْأَمْنِ الْوَطْنِيِّ: مَقَارِبَةُ تَقْنِيَّةِ

Artificial intelligence and national security challenges: Technical approach

المهندس. محمد بن نجمة*

المدرسة العليا العسكرية للإعلام والاتصال (الجزائر)، m.ben.nedjma82@gmail.com

تاريخ القبول: 2023/12/13

تاريخ الاستلام: 2023/11/13

ملخص:

يعرف العالم اليوم وجهاً جديداً من الحروب والصراعات، التي تعتمد أساساً على الحروب النفسية والتضليل الإعلامي وتزييف الأخبار، وهذا من خلال التقنيات الحديثة للدكاء الاصطناعي وتكنولوجيا الشبكات العصبية والتعلم العميق، الأمر الذي أصبح يشكل تحدياً أمنياً لمختلف شعوب ودول العالم، مما حدى بالخبراء والمختصين ومراكز البحث إلى دق ناقوس الخطر وإطلاق المشاريع والدراسات والورشات العلمية لإيجاد الآليات الكفيلة بمواجهة هذه التحديات، وكذا التقليل من المخاطر الناجمة عن هذه التقنيات.

تهدف هذه الورقة البحثية إلى تسليط الضوء على مختلف التحديات التي تفرضها تقنيات التعلم العميق على الأمن الوطني، بالإضافة إلى صياغة جملة من التوصيات حول الآليات التي يمكن من خلالها مواجهة هذه التحديات والتقليل من مخاطرها على الأمن الوطني للدولة.

الكلمات المفتاحية:

حروب الجيل الخامس، الحرب النفسية، دكاء اصطناعي، تعلم عميق، شبكات عصبية اصطناعية، الشبكات التلافيفية، تزييف الأخبار، الأمن الوطني، البيانات الضخمة.

Abstract: Today's world knows a new kind of war, that relies mainly on psychological warfare and deepfakes, and this is done through modern techniques of artificial intelligence and deep learning, which has become a security challenge for various peoples and countries of the world, which has prompted experts and specialists and research centers to sound the alarm and launch studies and scientific workshops to find mechanisms to confront these challenges and reduce the risks resulting from these technologies.

This research paper aims to shed light on various challenges posed by deep learning techniques to national security, In addition to formulating a set of recommendations about the mechanisms through which they can be confronted, and their risks to the national security of the state reduced.

Keywords:

fifth generation warfare, psychological war, AI, Deep Learning, Artificial Neural Networks, Convolutional Neural Networks, Fake news, National Security, Big Data.

* المؤلف المرسل.

مقدمة:

يشهد عالم اليوم ثورةً صناعيةً رابعةً، ميّزها التطوُّر التكنولوجي المتسارع القائم على تقنيات الدَّكَا الاصْطِنَاعِيّ، وقد عرفت هذه الأخيرة فترةً بحثيةً نوعيةً بفعل تراكم كمِّ هائلٍ من البيانات الضَّخمة في مختلف المنصَّات والشبكات وبفضل تطوُّر إمكانيَّات الحوسَّبة عالية الأداء، ممَّا أدَّى إلى تطوُّر البحوث العلميَّة المرتبطة بتقنيات تعلُّم الآلة (Machine Learning) والشبكات العصبية الاصْطِنَاعِيَّة وكذا تقنيات التعلم العميق (Deep Learning). هذه التقنيات فتحت آفاقاً جديدة في مجالاتٍ حديثةٍ على غرار المدن الذَّكيَّة والروبوتات وإنترنت الأشياء (IoT)، هذا إضافةً إلى إسهاماتها في تطوُّر العديد من المجالات المرتبطة بتحسين جودة حياة الأفراد، وكذا مختلفِ الميادين البحثية المتعلقة بالطب والاقتصاد والتسيير والأمن وحتى المرتبطة بالعلوم الإنسانيَّة والاجتماعية.

ورغم ما تنتجه تقنيات الدَّكَا الاصْطِنَاعِيّ من آثارٍ إيجابيةٍ في حياة الأفراد والمجتمعات، إلّا أنها بلا شك تنطوي على الكثير من المخاطر المتعددة الأبعاد، التي هي في تطوُّر مستمرٍّ ومثروُن بالتطوُّر المتسارع لتقنيات الدَّكَا الاصْطِنَاعِيّ، ففي المجال السياسي والإعلامي أصبح التلاعب الاجتماعي باستخدام الدَّكَا الاصْطِنَاعِيّ وسيلةً للتأثير على الرُّأي العام، وتوجيهه كما حدث مع المُقرَّعين الأمريكيين خلال الانتخابات الرئاسية الأمريكية لعام 2016، والبريطانيين خلال استفتاء خروج بريطانيا من الاتحاد الأوروبي (بريكست)، أما على المستويين الاقتصادي والاجتماعي فبحسب التقارير الصادرة من المنتدى الاقتصادي العالمي 2020، فإن وظائف المستقبل تتوجَّه نحو تقنية الروبوتات والبيانات الضَّخمة وأنظمة الدَّكَا الاصْطِنَاعِيّ، والتقنيات المطورة التي ستحل محلَّ الكثير من الوظائف الحالية، مما سيؤدِّي إلى ارتفاع معدلات البطالة وإنهاءك خصوصيات الأفراد، أمّا عسكرياً وأمنياً فلا يخفى على أحد اليوم الدور الذي يلعبه الدَّكَا الاصْطِنَاعِيّ في الاستطلاع الإلكتروني والأمن السيبراني وصناعة الأسلحة الذَّكيَّة المبرَّجة للقتل بلا رحمة ودون تمييز، والتي أدَّت إلى زيادة أعداد الضحايا المدنيين مثلما ما حدث خلال العدوان الصهيوني على غزّة خلال عملية طوفان الأقصى 07 أكتوبر 2023، بالإضافة إلى، تزييف الأخبار والتلاعب العميق أو التزييف العميق وحملات التَّضليل الإعلامي، كأدواتٍ للحرب النَّفسية والإعلامية أو "حرب المعلومات والإدراك"، ضمن ما بات يعرف بحروب الجيل الخامس¹.

وبناء على ما سبق، نطرح الإشكالية التالية:

ماهي التحديات الأمنية التي يفرضها الدَّكَا الاصْطِنَاعِيّ في ظل حروب الجيل الخامس من المنظور التقني؟

لمناقشة هذه الاشكالية نطرح التساؤلات الفرعية التالية:

- ✓ ماذا يقصد بالدَّكَا الاصْطِنَاعِيّ؟ وما هي الفرص التي يتيحها؟
- ✓ ماهي أبرز التحديات التي يفرضها تطوُّر تقنيات الدَّكَا الاصْطِنَاعِيّ على الأمن الوطني؟
- ✓ ماهي الآليات والسبل الكفيلة بمواجهة المخاطر المرتبطة بتطوُّر تقنيات الاصْطِنَاعِيّ؟

لمناقشة الاشكالية السابقة وللإجابة على هذه التساؤلات الفرعية، قسمنا هذه الورقة البحثية إلى المحاور التالية:

- المحور الأول: ماهية الدَّكَا الاصْطِنَاعِيّ.
- المحور الثاني: فرص واستخدامات الدَّكَا الاصْطِنَاعِيّ في المجالات الأمنية والعسكرية.
- المحور الثالث: فرص الدَّكَا الاصْطِنَاعِيّ في ميدان الصحافة والإعلام.
- المحور الرابع: المخاطر والتحديات المرتبطة بتطوُّر تقنيات الدَّكَا الاصْطِنَاعِيّ.
- خاتمة.

I. ماهية الذكاء الاصطناعي:

يعدّ الذكاء الاصطناعي أحد المجالات العلمية التي تعرف تطورا متسارعا في الوقت الحاضر، وهو يهدف بالأساس إلى أتمتة مجموعة واسعة من المهام التي يقوم بها الإنسان، وتحسين خوارزميات تعلم الآلة خاصة في مجال التعلم العميق، كما يستخدم لتحسين مسارات الشحن التجاري، وإدارة حركة السفن والشاحنات في الموانئ، وترجمة استعلامات بحث التجارة الإلكترونية من لغة إلى لغات أخرى والاستجابة مع المخزون المترجم². ويتضمن الحقل الدلالي للذكاء الاصطناعي مجموعة من المصطلحات والمفاهيم ذات الصلة والتي سنتطرق إليها فيما يلي.

I. 1/ تعريف الذكاء الاصطناعي:

يعرف البعض الذكاء الاصطناعي (AI) بأنه ذلك الفرع من علوم الحاسوب الذي يمكن بواسطته خلق وتصميم برامج الحاسبات التي تحاكي أسلوب الذكاء الإنساني، لكي يتمكن الحاسب من أداء بعض المهام بدلاً من الإنسان، والتي تتطلب التفكير والتفهم والسمع والتكلم والحركة بأسلوب منطقي ومنظم. في حين ينظر إليه البعض بأنه أحد تطبيقات الحاسب، أو بأنه القدرات البرمجية التي يمكن أن تقدم نوعاً من الذكاء المصطنع³، وعموماً فالذكاء الاصطناعي هو حل تقني أو نظام أو جهاز يهدف إلى محاكاة الذكاء البشري لأداء المهام مع تحسين نفسه بشكل متكرر، بناءً على المعلومات التي يجمعها والتجارب والبيانات التي تم التعرف عليها، ويدخل ضمن الذكاء الاصطناعي التعلم الآلي والتعلم العميق.

ظهرت أولى البحوث العلمية في الذكاء الاصطناعي خلال الخمسينيات من القرن الماضي تحديداً سنة 1943 م حين نشر وارن ماك كلوتش McCulloch والتر بيتس Pitts بحثاً عن الشبكات العصبية الاصطناعية، وفي الثمانينات بدأ ما يعرف بحركة التنوير أو تعلم الآلة (ML)، لنصل في بدايات القرن الواحد والعشرين إلى التعلم العميق (DL) واستخدام شبكات الألياف العصبية الاصطناعية كتقنيات لأنظمة الذكاء الاصطناعي، خاصة مع تطور إمكانيات الحوسبة وتوافر البيانات الضخمة.

I. 2/ تعلم الآلة:

التعلم الآلي (ML) أو تعلم الآلة هو مجموعة فرعية من الذكاء الاصطناعي، ويشمل العمليات التي تسمح لأجهزة الكمبيوتر باستخلاص الاستنتاجات من البيانات لأجل القيام بمجموعة واحدة من المهام دون برمجتها بشكل صريح. فهو مجموعة من الأدوات الإحصائية، الهندسية والخوارزمية التي تمكن الآلة من التعلم من خلال مجموعة من التجارب والملاحظات⁴، والتي لا تكون بالأساس في شكل بيانات ضخمة مثلما هو الحال بالنسبة للتعلم العميق، مما يمكن من حل المشكلات الأقل تعقيداً وفي فترة زمنية قصيرة.

وتنقسم خوارزميات التعلم الآلي عموماً إلى أربعة (04) أنواع هي:

- التعلم الخاضع للإشراف : Supervised learning هو أكثر أنواع التعلم الآلي شيوعاً، وفي هذا النوع تكون كل البيانات مسماة من خلال المشرف أو الخبير على عملية التعلم الآلي، ومن أنواعه التصنيف Classification والتوقع Regression.

- التعلّم غير الخاضع للإشراف : UnSupervised learning في هذا النوع تدرب الخوارزميات على بيانات غير مسمّاة، وهذا لإيجاد علاقات مخفية بين هذه البيانات، ومن أنواعه التجميع. Clustering.
- التعلّم شبه الخاضع للإشراف : Semi-Supervised Learning هو مزيج بين النوعين الأولين، أي أنه في هذه الحالة تكون بعض البيانات مسمّاة ومعينة، في حين أغلب البيانات غير مسمّاة.
- التعلّم المعزز Reinforcement Learning : وفي هذا النوع يتم التعلّم الآلي من خلال التفاعل مع البيئة والمحيط، أي أن الآلة أو الوكيل "agent" تتعلّم من من عواقب أخطائها بدلاً من تعليمها مباشرة، ويستخدم هذا النوع غالباً في الألعاب مثل لعبة Pac Man .

I. 3/ التعلّم العميق:

رغم علاج خوارزميات التعلّم الآلي للكثير من المشاكل، إلّا أنّ هناك مشاكل معقّدة لم تتمكن هذه الخوارزميات من حلها، على غرار التعرف على الأشياء والأشخاص وتعابير الوجه، ومن هنا ظهر التعلّم العميق كنوع من التعلّم الآلي الذي لا يركّز على مجموعة واحدة من المشكلات، وإنما يحقق مستوى فكرياً أوسع، وهذا من خلال بنية معقّدة من الخوارزميات في شكل شبكات عصبية اصطناعية يمكنها التعلّم في مستويات متعددة واتخاذ القرارات بصورة ذاتية، وهذا باستعمال مجموعة بيانات كبيرة (ضخمة) للتدريب.

ويشير مصطلح "عميق" هنا إلى الطبقات العميقة من الأعصاب المترابطة فيما بينها التي تكون الشبكات، والتي تستخدم لتحديد الأنماط المختلفة بصورة آلية دون تدخل الإنسان، حيث يتم إعطاء بيانات التعلّم فقط للشبكة العصبية، ويتم الباقي من خلال النموذج .

يستخدم التعلّم العميق اليوم بشكل كبير في الأنظمة المدعّمة بالدكاء الاصطناعي، وبالأخص في وسائل التواصل الاجتماعي، كتطبيقات التعرف على الأشخاص والردّشة الآلية كتطبيقات Siri و Alexa، وكذلك في مواقع الترجمة الفورية على غرار Google Translate و DeepL بالإضافة إلى منصات مشاهدة الأفلام كـ Netflix وغيرها.

I. 4/ شبكات الألياف العصبية الاصطناعية:

تعدّ الشبكات العصبية الاصطناعية أساس تقنيات التعلّم العميق، وهي عبارة عن نظام اصطناعي لمعالجة البيانات يحاكي منظومة الشبكات العصبية الطبيعية للإنسان أو للكائن الحي، التي تساعد في التحكم في العمليات الحيوية اللازمة لاستمرار الحياة كالتعلّم وتمييز الأشياء واتخاذ القرارات، وهذا من خلال التوصيلات والربط بين الخلايا العصبية، التي برهن مختصو علم الأعصاب أنّها مخزن المعلومات في العقل وأهم أجزائه⁵ .

بدأت فكرة محاكاة الشبكات العصبية لدمغ الإنسان مع أبحاث دونالد هيب Hebb في كتابه منظومة السلوك 1949م، الذي أشار فيه إلى أنّ المشابك بين الخلايا العصبية تقوى كلما تم استعمالها أكثر، مما يقوي الروابط بينها، وتصبح عملية معالجتها للعمليات أسرع مع تكرار إثارتها بنفس المعطيات، وفي سنة 1958 بدأ العالم فرانك روزنبلات بتصميم أول نموذج لعصبون عصبي بسيط Perceptron، الذي شكل نموذجاً لخوارزمية التعلّم بالإشراف لتصنيف مدخلين إلى مخرج واحد.

تتكون الشبكات العصبية الاصطناعية عموماً من ثلاث طبقات عصبونية أساسية : طبقة الادخال أو الدخل input layer، طبقة مخفية hidden layer طبقة خرج output layer طبقة، حيث تقوم طبقة الدخل بتغذية الطبقة المخفية ببيانات التدريب ومن ثم تقوم الطبقة المخفية بالمعالجة الفعلية للبيانات بالاستعانة بخوارزميات التدريب (Training) على غرار خوارزميات التغذية الأمامية (Propagation algorithm) (Back) ، والتي تعتمد انتشار الأخطاء في طبقة الخرج، من الخلف إلى الأمام لضبط أوزان الشبكة.

I. 5/ البيانات الضخمة:

تعرف البيانات على أنها مجموعة من الحروف، أو الكلمات، أو الأرقام، أو الرموز، أو الصور المتعلقة بموضوع ما. والبيانات في حد ذاتها ليس لها معنى أو قيمة، وهي الصورة الخام للمعلومة⁶ واليوم نتيجة للتحويل الرقمي والاستخدام الكثيف للانترنت ووسائل التواصل الاجتماعي، وما نتج عنه من تراكم وتدفق كم هائل من البيانات المتنوعة والمختلفة المصادر والتي هي في زيادة مستمرة، ظهر ما يعرف بالبيانات الضخمة التي ينظر إليها العديد من الخبراء والمختصين على أنها "نقط المستقبل". ويعرفها معهد ماكنزي العالمي على أنها مجموعة من البيانات التي يفوق حجمها القدرة على معالجتها باستخدام أدوات قواعد البيانات التقليدية، من التقاط ومشاركة ونقل وتخزين وإدارة وتحليل، في غضون فترة زمنية مقبولة⁷.

يتم استخدام البيانات الضخمة في مجالات عدة، خاصة منها المدعمة بتقنيات الذكاء الاصطناعي كالخدمات المالية والتسويق والتعليم، باعتبار البيانات أساس بناء واختبار نماذج التعلم العميق والشبكات العصبية الاصطناعية، حتى تحاكي سلوك الأفراد وتفكيرهم ورغباتهم وخبراتهم.

الشكل 1 : نماذج لبيانات ضخمة MNIST (على اليمين) و CIFAR10 على اليسار

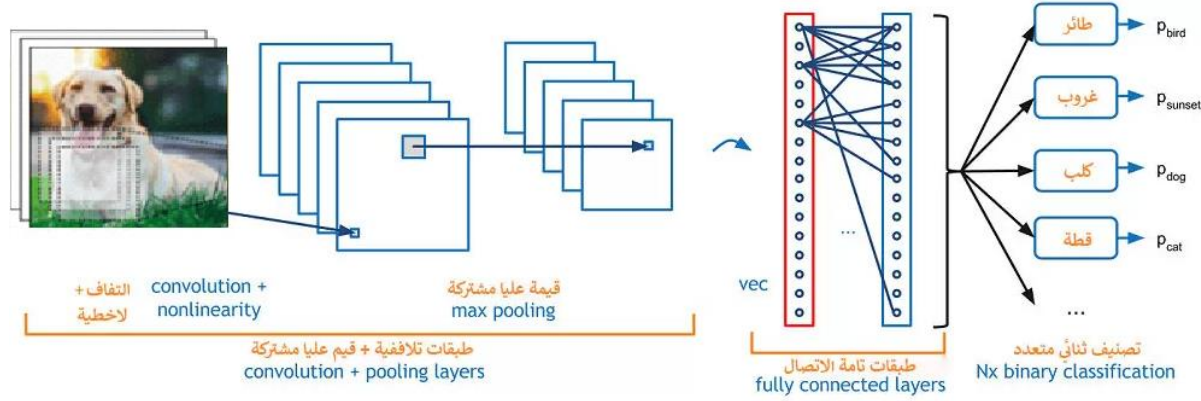


المصدر: بن نجمة محمد، تطوير وزراعة في دارة منطقية قابلة للبرمجة لشبكة عصبية التفاضلية لتطبيقات التعلم العميق

I. 6/ الشبكات العصبية الالتفافية :

تعد الشبكات العصبية التلافيفية أو الالتفافية **Convolutional Neural Network** أكثر أنواع الشبكات العصبية العميقة استخداماً، وهي تتضمن طبقات تلافيفية تمكن من تجزئة المدخلات إلى أجزاء، ثم تصنيف الأجزاء والأنماط المختلفة على حدى من أجل فهمها بشكل أوسع، وتستخدم هذه التقنية غالباً في مجال الرؤية الحاسوبية **Computer Vision** والتعرف وعلى الصور والأشكال وتصنيفها بصورة آلية وسريعة. وتعتمد عليها أساساً طائرات الدرونز في رصد وتحديد الأهداف، كما يعمل الباحثون اليوم على تطوير تطبيقات عديدة لهذه الشبكات على غرار أنظمة التعرف على الأشخاص من خلال بصماتهم.

الشكل 2: التعرف على الصور باستخدام الشبكات العصبية التلافيفية.



المصدر : من إعداد الباحث

II. فرص واستخدامات الذكاء الاصطناعي في المنظومات الأمنية والدفاعية:

تتم العديد من الدول اليوم بتطوير تطبيقات الذكاء الاصطناعي، باعتبارها أدوات أساسية في التكنولوجيا الناشئة تمكن من معالجة وجمع وتحليل كميات كبيرة من البيانات بمعدل أسرع من أي وقت مضى، وأدت في كثير من المجالات إلى طفرة حقيقية نلمسها في حياة الرفاهية للإنسان في الوقت الراهن، كما أنها تساعد على تعزيز القدرات المستقبلية للدولة وخاصة في المجالات الأمنية والعسكرية.

وقد أشار تقرير ميونخ للأمن 2019، إلى ارتفاع حجم الاستثمار في هذا المجال إلى أعلى مستوياته خلال عام 2018 ليصل إلى أكثر من 50 مليار دولار، أي حوالي ضعف حجم الاستثمارات في المجال نفسه خلال عام 2017، كما أن التقديرات سنة 2023 تشير إلى أن قيمة الاستثمارات بالقطاع الخاص في هذه التكنولوجيا مرشحة للوصول إلى 158 مليار بحلول العام 2025 ، وأن تبلغ 110 مليارات بنهاية 2023⁸ ، ما يعني أن المجتمع الدولي بات مُدرِّكاً لأهمية توظيف تقنيات الذكاء الاصطناعي والثورة الرقمية والتكنولوجيا في مختلف المجالات، لاسيما المرتبطة منها بالدفاع والأمن، بل أصبح يتنافس في تطويرها، الأمر الذي أفضى إلى سباق محموم وصراع خفي بين قوتين عظيمتين ورائدتين في الذكاء الاصطناعي، وهما الصين والولايات المتحدة الأمريكية، هذا التنافس الذي شبيه الخبراء والمختصون بالسباق نحو التسليح بين القطبين - الإتحاد السوفياتي سابقاً والولايات المتحدة الأمريكية - في فترة الحرب الباردة. في هذا المحور سوف نشير إلى أبرز الفرص والتطبيقات المعتمدة على تقنيات الذكاء الاصطناعي، وبشكل خاص تلك المتعلقة منها بمجالات الدفاع والأمن والاعلام وأدوات حروب الجيل الخامس.

II. 1/ التحكم الذاتي:

تعتبر تقنيات الذكاء الاصطناعي وبصفة أخص تقنيات التعلم العميق أدوات فعالة لأتمة الأنظمة وبناء منظومات أمنية محمولة Système Embarqué ذاتية التحكم، قادرة على تنفيذ الأدوار التي يؤديها البشر وخاصة تلك المهام الأمنية التي تعرض أرواحهم للخطر، مما يمكن من تقليل الخسائر البشرية وخفض التكاليف أثناء القيام بهذه المهام، على غرار الأسلحة ذاتية التشغيل التي أصبحت تتمتع بدرجة كبيرة من الاستقلالية والعمل دون تدخل العنصر البشري، إذ تتمكن من رصد وتتبع وتحديد ومهاجمة الأهداف بصورة آلية.

وتتجه الدول العظمى إلى زيادة الاستثمار في هذا النوع من الأسلحة، على غرار الروبوتات ذاتية التحكم التي تم اللجوء إليها في عدة مناسبات، على غرار كوريا الجنوبية في عام 2014 التي قامت باستخدامها في دوريات الحراسة على طول الحدود مع كوريا الشمالية، والمركبات القتالية الروسية URAN-9 التي تمتلك القدرة على اكتشاف الهدف والتعرف عليه وتتبعه تلقائياً. بالإضافة إلى الطائرات المسيّرة الانتحارية ذاتية التوجيه، والتي باتت تستعمل بكثافة خلال العملية العسكرية الروسية في أوكرانيا التي يجمع الخبراء على أنها أول حرب درونز وذكاء اصطناعي، على غرار المسيّرة الروسية "أفود-النير" التي تقوم بتحليل وكشف الأهداف الثابتة والمتحركة وإصابتها بصورة ذاتية وبدقة عالية من دون مشاركة الإنسان⁹، وكذا المسيّرة التركية "بيرقدارتي بي 2" التي تستعملها القوات الأوكرانية ولعبت دوراً رائداً في مهاجمة أنظمة الدفاع الجوي والوحدات المدرعة الروسية، لما تمتلكه من تقنيات ذكية تمكنها من الاقلاع والهبوط والمناورة بشكل مستقل.

II. 2/ السرعة والتحكم

تعد السرعة والمفاجأة عناصر أساسية وهامة لنجاح العمليات العسكرية والأمنية، لهذا تشكل المنظومات الأمنية والعسكرية الآلية التي تعتمد على تقنيات الذكاء الاصطناعي أسبقية تقنية مقارنة مع نظيراتها التقليدية، كون أن الأولى تمتاز بسرعة فائقة في تحليل البيانات ومعالجتها ثم اتخاذ القرار بصورة آلية وفي ظرف قياسي، خاصة إذا ما زودت بإمكانات حوسبة عالية الأداء على غرار المعالجات الدقيقة الرسومية GPU ودارات مصفوفة البوابات المنطقية القابلة للبرمجة FPGA، مما يزيد من فرص نجاحها في تنفيذ هذه العمليات مقارنة مع المنظومات الغير ذاتية، التي يكون فيها الإنسان سيد القرار .

وتستغل أنظمة الدفاع الجوي اليوم هذه الميزة من خلال دمج تقنيات الذكاء الاصطناعي والتعلم العميق، وتدريبها على رصد الأهداف المعادية والتعرف عليها باستعمال الشبكات العصبية الاصطناعية، حيث يستخدم اليوم الكيان الصهيوني هذه التكنولوجيا في منظومة القبة الحديدية، التي وعبر خوارزميات الذكاء الاصطناعي تدرس مسار الصاروخ ونوعه، وما إذا كان متوجهاً إلى منطقة مأهولة أو لا، ثم تقرّر هل يجب اعتراضه أم لا من خلال تحليل الكلفة والفائدة بحيث تكون الأولوية لمنع الخسائر البشرية، ويتم كل هذا بصورة آلية وفي وقت وجيز.

كذلك الأمر بالنسبة لأنظمة الاستخبارات ومكافحة الأنشطة الإرهابية، حيث توفر أنظمة الذكاء الاصطناعي التي تعتمد على البيانات المفتوحة المصادر فوائد في المهام طويلة الأمد التي لا تتحملها قدرة البشر، مثل جمع المعلومات الاستخباراتية عبر مناطق واسعة وعلى مدار حقب زمنية طويلة¹⁰، بالإضافة إلى القدرة على اكتشاف الحالات الشاذة وتصنيف السلوك والمشاعر وكذا التعرف على الأشخاص الذين يحتمل قيامهم بأعمال إرهابية في الأماكن الحساسة وفي وقت قصير ثم تنفيذ ضربات "استباقية"، أي اغتيال أو قتل

أشخاص مُحددين، يُنظر إليهم على أنهم قد يُشكلون تهديدا محتملا في وقت ما في المستقبل. تعمل هذه الضربات على افتراض أن الشخص المراقب لديه القدرة على تنفيذ جرم ما في المستقبل، رغم أنه ربما لم يفعل أي شيء لحظة استهدافه بالدرونز المزودة بتقنيات الذكاء الاصطناعي."

ورغم ما توفره هذه التقنيات من قدرة كبيرة على التحكم والاستجابة السريعة في العمليات الأمنية والعسكرية، يرى بعض الخبراء الأمنيين أن هذه الميزة هي سلاح ذو حدين، حيث يمكن أن تكون له تداعيات وخيمة إذا تجاوزت هذه الأنظمة قدرة البشر وخرجت عن السيطرة، أو اتخذت قرارات حاسمة بناءً على معلومات مزيفة، كإصدار خاطئ بوقوع هجوم نووي مثلاً، مما قد يؤدي إلى إنفلات الوضع، وحوادث كوارث وخيمة غير محسوبة التكاليف.

II. 3/ التدرج :

لقد برهنت حرب الدرونز خلال العملية العسكرية الروسية في أوكرانيا مدى قدرة تقنيات الذكاء الاصطناعي على ترجيح الكفة وموازين المعركة بتكلفة أقل، حيث يجمع الخبراء على أن القوات الأوكرانية اكتسبت ميزة تكنولوجية على القوات الروسية المتفوقة في العدة والعتاد باستخدام تقنيات شركة "بلانتيير" للذكاء الاصطناعي المدججة في الدرونز التي تنتجها حوالي أكثر من 30 شركة في أوكرانيا، والتي سمحت للقوات الأوكرانية بزيادة دقة وسرعة وخطورة قصفها المدفعي على الرغم من امتلاكها لقوات مدفعية أصغر نسبياً، بالإضافة إلى تنفيذ هجمات بالمسيرات الانتحارية داخل العمق الروسي، كما شهدت الأسابيع الأخيرة من الحرب دوراً متصاعداً للطائرات المسيّرة التجارية الزهيدة السعر، والتي على الرغم من أنها لا تمثل أحدث التقنيات. فقد أظهرت مقاطع فيديو انتشرت على شبكة الإنترنت ومواقع التواصل الاجتماعي لقطات مختلفة تظهر إطلاق نار على ما تقول أوكرانيا إنهم مدنيون أوكرانيون وأخرى تكشف إسقاط طائرة مسيرة تجارية يقول الأوكرانيون إن روسيا تستخدمها لتوجيه نيران المدفعية ضدهم، وهي جميعها صور لزوايا في الحرب لم يشهدها العالم من قبل. كذلك الأمر بالنسبة للقوات الروسية، والتي استخدمت المسيرات الانتحارية الإيرانية شاهد-13 لضرب أهداف داخل أوكرانيا. وعموماً يمكن تدريب الدفاعات الجوية على هذا النوع من المسيرات، إلا أن هذا الأمر يجعل من هذه الدفاعات ستلتقط أي طائر يخلق فوقها، مما يزيد من تكلفة هذه الدفاعات نتيجة الإنذارات الكاذبة، إضافة إلى صعوبة تعامل الأنظمة الدفاعية مهما كانت كفاءتها مع أسراب المسيرات التي تحلق في ارتفاع منخفض، فمثلاً في أكتوبر عام 2022، قدّرت أوكرانيا أنها أسقطت 70% أو أكثر من الطائرات الصغيرة دون طيار، لكن النسبة المتبقية كانت كافية لإضعاف واستهداف الشبكة الكهربائية في البلاد، لهذا يرى الخبراء العسكريون أن انتشار هذه التكنولوجيات القائمة على الذكاء الاصطناعي والمنخفضة التكاليف، يمكن البلدان المتأخرة عسكرياً من رفع القدرات العملياتية لجيوشها وبتكاليف أقل، مما يسمح بترشيدها نفقاتها العسكرية.

II. 4/ التعامل مع البيانات الضخمة:

من أهم الميزات التي توفرها تقنيات الذكاء الاصطناعي، هي قدرتها على التعامل مع البيانات الضخمة المختلفة المصادر وتحليلها، حيث أن هذه العملية تعد شبه مستحيلة إذا قام بها البشر، وهذا نتيجة الزيادة الهائلة في كمية البيانات خاصة في ظل الاستعمال الكثيف لوسائل التواصل الاجتماعي والمنصات الإلكترونية والانترنت بشكل عام، وبالتالي فقد وفرت هذه الأخيرة قواعد بيانات هائلة لتغذية وتدريب الأنظمة الذكية وأتمتها، لتقوم هذه الأخيرة في مرحلة ثانية بتمشيط البيانات الضخمة المفتوحة المصدر خاصة، وتحديد الأنماط المختلفة فيها ثم استنباط المعلومات منها بصورة آلية وحديثة، ودون تدخل الإنسان، مما يمكن من تسريع وتحسين آلية اتخاذ القرار، وبالتالي الرفع من مستوى وديناميكية الأداء العملياتي الأمني والعسكري للتعامل مع مختلف التهديدات المستقبلية واستشرافها .

وتبرز القيمة التي تضيفها هذه الميزة بصفة خاصة في مجال الاستخبارات الالكترونية والاستشعار عن بعد، وفي عملية التحليل الاستخباري للبيانات، أين يتم تحليل عدد ضخم من البيانات الملتقطة بالأقمار الاصطناعية والطائرات بدون طيار وعن طريق شبكات التواصل الاجتماعي وتسلط الضوء على المهمة منها فقط لاتخاذ القرارات الاستراتيجية والتكتيكية. وفي سيناريوهات أخرى، يتم بناء بنك للأهداف من خلال جمع عدد كبير من البيانات بصورة تلقائية ودورية، وذلك بالاعتماد على نموذج التوصيات القائمة على الذكاء لاختيار أهداف للغارات الجوية، ثم يتم جمع تلك المعلومات من جميع الغارات السابقة واستخدامها في الهجمات اللاحقة بسرعة باستخدام نموذج آخر للذكاء الاصطناعي يسمى "Fire Factory"، وليتم بعد ذلك استخدام النموذجين لبناء مجموعة بيانات حول الأهداف المعتمدة عسكرياً لحساب الذخيرة المحتملة وتعيين الأهداف للطائرات من دون طيار. ويستخدم الكيان الصهيوني هذه المقاربة من خلال "مركز علوم البيانات والذكاء الاصطناعي" التابع للوحدة 8200، منذ عملية سيف القدس في ماي 2021، واستعملت هذه التقنية لاغتيال قادة المقاومة الفلسطينية داخل قطاع غزة.

ومن ناحية أخرى، تجري الأبحاث في مدى إمكانية استغلال هذه الميزة للتعمية (Cryptography) وللكشف عن التهديدات السيبرانية، حيث أنه لا يمكن للأنظمة التقليدية مجابهة العدد الكبير من البرامج الضارة والفيروسات التي يتم إنشاؤها كل شهر، لذلك يلجأ خبراء الأمن السيبراني إلى تقنيات الذكاء الاصطناعي لمواجهة هذه التهديدات. كما تقوم شركات الأمن السيبراني بتدريب أنظمة الذكاء الاصطناعي للكشف عن الفيروسات والبرامج الضارة باستخدام خوارزميات التعلم العميق، حتى يتمكن الذكاء الاصطناعي من التعرف على الأنماط الضارة في البرامج بصورة آلية، ليقوم بعدها بعزلها عن النظام، مما يسمح للمحللين الأمنيين بالاستجابة للتهديدات بسرعة أكبر.

II. 5/ النماذج التنبؤية:

تشكل تقنيات الذكاء الاصطناعي أدوات محورية في التنبؤ بالأعمال التخريبية والإرهابية، وذلك من خلال تحليل البيانات الضخمة للسكان، ويتم هذا باستعمال النماذج التنبؤية التي جرى تدريبها لكشف الارهابيين المحتملين وتحييدهم قبل تنفيذ مخططاتهم. وفي مستوٍ ثانٍ تسمح هذه العملية باكتشاف الأفراد المعرضين للتطرف من خلال وإعادة توجيههم. حيث طوّرت بعض الشركات المتخصصة في الذكاء الاصطناعي أدوات لتقييم مدى قابلية التطرف العنيف؛ على غرار شركة Jigsaw التابعة لشركة Alphabet Inc. المعروفة سابقاً باسم "Google Ideas" والتي أعلنت عن مشروع باسم "إعادة التوجيه"، الذي يستهدف مستخدمي مواقع مشاركة الفيديو المعرضين للدعاية من الجماعات الإرهابية مثل تنظيم "داعش"، إذ يُعيد المشروع توجيههم إلى مقاطع الفيديو التي تتبنى رواية موثوقة ومضادة لرواية التنظيم.

III. فرص الذكاء الاصطناعي في الصحافة والإعلام:

تشهد تكنولوجيا الإعلام والاتصال اليوم ثورة تقنية قائمة على إدماج تقنيات الذكاء الاصطناعي خاصة بعد أزمة كورونا، وقد أدى هذا إلى ظهور مفهوم جديد في مجال الإعلام يعرف بـصحافة الذكاء الاصطناعي أو صحافة الروبوت، حيث من خلال محاكاة السلوك البشري، تمكن هذه التقنيات من جمع الأخبار وتلخيصها وكتابتها وتحرير التقارير الصحفية، وحتى التأثير ومخاطبة الجمهور وتشكيل الرأي العام، كل هذا بصورة آلية ودون تدخل الانسان. وتتجه اليوم المؤسسات الإعلامية إلى استخدام هذه التقنيات لأتمتة جزء كبير من العمل الصحفي والإعلامي، ولتعزيز كفاءتها وإنتاجيتها. وتعد الصين رائدة في هذا المجال، حيث قدمت وكالة الأنباء

الصينية "شينخوا" لمشاهديها أول قارئ آلي "كيو هاو" لنشرة أخبار في العالم، يعمل بالذكاء الاصطناعي ولا يختلف عن البشر، فضلاً عن تعبيرات وجهه التي لا تفرقها عن الإنسان الطبيعي في أثناء إلقاء نشرة الأخبار، الأمر الذي اعتبره البعض تهديداً للصحفيين والعاملين في قطاع الإعلام، حيث أن هذا الدور أصبح بإمكان الذكاء الاصطناعي القيام به على نحو لا يمكن فيه التمييز بين الإنسان الصحفي الحقيقي والروبوت.

وعموماً، تتمحور تطبيقات الذكاء الاصطناعي في مجال الإعلام حول خمسة (05) مهام: ¹¹

- ✓ توليد المحتوى وإنتاج الأخبار بشكل آلي وتوزيعها: وهذا بالاعتماد على البيانات الإحصائية، وتحليل الأخبار وتعليم الأخبار المهمة تلقائياً وتصنيفها إلى موضوعات، مما يسهل على المتصفح العثور على الأخبار والمحتوى الذي يبحثون عنه ويدخل في إطار اهتمامهم .
 - ✓ متابعة الأخبار العاجلة: من خلال رصد الأحداث فور وقوعها المعلومات الجديدة المتصلة بخبر معين، وتحيينها وتتبع مستجداتها، والتحقق من صحتها.
 - ✓ إجراء بحث سريع ودقيق: من خلال تحويل الصوت إلى نص، وربط المعلومات وتحويلها إلى أشكال وإحصائيات وأشكال بيانية.
 - ✓ التصحيح الإملائي والنحوي والأسلوبي: للتقارير الصحفية، واقتراح تحسينات في الصياغة، وتخصيص مقالات مختلفة حسب الجمهور المستهدف ومعالجة النصوص بصورة آلية.
 - ✓ التحقق من الأخبار بشكل سريع وموثوق وكشف الأخبار الزائفة والمضللة.
- ومن بين أبرز أدوات الذكاء الاصطناعي في الإعلام:

I. النموذج التوليدي: Bloomberg GPT

تمثل هذه الأداة النموذج التوليدي العامل بالذكاء الاصطناعي الخاص بشركة الخدمات الإخبارية والإعلامية والمعلومات المالية بلومبرج ال بي (Bloomberg LP)، حيث قامت بتطويره باستخدام نفس التكنولوجيا الأساسية لـ ChatGPT، وتم تدريب الروبوت الخاص بالأداة باستعمال بيانات نصية ضخمة مشكلة من عدد مهول من المستندات المالية والبيانات الصحفية بالإضافة إلى بيانات مواقع الويب، وبإمكانه تحرير مقالات وكتابة أخبار اقتصادية وكذا تحليل سوق الأسهم .

II. مولد الصور: DALL-E2

يعتمد هذا النموذج التوليدي على نفس بنية النموذج ChatGPT-3، ويمكنه توليد صور عالية الجودة إنطلاقاً من الإدخال النصي. هذا النموذج جرى تدريبه على مجموعة كبيرة من البيانات المكونة من صور وأوصاف نصية مقابلة لها، وهذا باستخدام خوارزميات التعلم غير الخاضعة للإشراف وباستخدام أجهزة حوسبة عالية الأداء. تستخدم هذه الأداة خاصة في إنشاء الصور الإشهارية والإعلانات والألعاب والترفيه ¹².

III. مولد المحتوى: JASPER AI

تعمل هذه الأداة أساساً بتقنيات معالجة اللغات الطبيعية (NLP) التي تعتمد أساساً على تقنيات التعلم العميق، تمكن هذه الأداة من توليد نصوص ومحتوى إعلامي، كالمقالات والمدونات والتقارير، انطلاقاً من كلمات مفتاحية، وبطريقة آلية وسريعة. تم تدريب هذا النموذج على مجموعة ضخمة من البيانات واسعة النطاق حتى يتمكن من فهم كل مايقوله البشر والاستجابة لهم بسهولة وبسرعة. أهم مايميز هذه الأداة هو القدرة على فهم السياق والتفاعلية مع البشر، بالإضافة إلى تفوقها في ترجمة اللغات مع الحفاظ على المعنى، مما يسهل على الأفراد والمؤسسات التواصل وتخطي حاجز اللغة.

IV. أداة التحقق من الأخبار الزائفة: LOGICALLY

تعد هذه الأداة أحد أهم وسائل الذكاء الاصطناعي للتحقق من الأخبار الزائفة، حيث تتم معالجة اللغة الطبيعية لفهم نص الخبر بواسطة خوارزميات التعلم العميق، التي تتحقق من مصداقية الخبر من خلال مقارنته بمحتويات كثيرة مماثلة وبالأستعانة بفريق من الخبراء. بالإضافة إلى هذا، تمكن الأداة من التأكد من خلو نص المحتوى من العبارات اللاأخلاقية ومنعه في حالة حدوث ذلك.

IV. المحور الرابع: المخاطر والتحديات الأمنية الوطنية المرتبطة بتقنيات الذكاء الاصطناعي:

في خضم التطور السريع والمزايا التي تقدمها تقنيات الذكاء الاصطناعي، نجد اليوم عددا كبيرا من الخبراء والمختصين في الشؤون الأمنية بل حتى المختصين في الذكاء الاصطناعي يبدون توجسا من التهديدات والمخاطر المحتملة التي يمكن أن تسببها هذه التكنولوجيا، التي شكلت الأداة الأساسية لحروب الجيل الخامس، خاصة فيما يتعلق باستخدامها في انتحال الشخصية وإنتاج الأخبار المضللة والتزييف العميق، بالإضافة إلى الاختراقات السيبرانية وانتهاك الخصوصية والاحتيال والخداع الإلكتروني. وظهرت اليوم عدّة نقاشات حول التحديات التي تفرضها لهذه الثورة التقنية على أمن الأفراد والمجتمعات، حيث أطلق الأمين العام للأمم المتحدة السيد "أنطونيو غوتيرش" في السادس والعشرين من أكتوبر سنة 2023 هيئة استشارية رفيعة المستوى بشأن الذكاء الاصطناعي، ودعا إلى إجراء محادثة عالمية حول إدارة هذه التكنولوجيا لضمان "تعظيم فوائدها للبشرية جمعاء، واحتواء المخاطر وتقليصها". كما بدأت الكثير من المراكز البحثية والمنظمات الغير ربحية المتخصصة في تقنيات الذكاء الاصطناعي وفي الدراسات الأمنية استشعار هذه المخاطر والتحديات، والآثار السلبية المترتبة عن استعمالها، وبدأت في تطوير وتصميم معايير وأساليب للحد من هذه الأخطار .

IV. 1/ المخاطر والتهديدات الأمنية:

ينطوي الذكاء الاصطناعي على جملة من المخاطر والتهديدات الأمنية على الأفراد والمجتمعات، وهي ما فتئت تتنامى موازاةً مع التطور المتسارع الذي تشهده هذه التقنيات، خاصة في ظل التراكم المتزايد للبيانات الضخمة المفتوحة المصدر المتاحة لتدريب الشبكات العصبية الاصطناعية، وكذا تطور الوسائل التقنية والفنية المساعدة على ذلك من إمكانيات حوسبة عالية الأداء ومنصات التطوير السحابية ومكتبات الذكاء الاصطناعي وغيرها. وإيجازاً، يمكننا الإشارة إلى جملة من هذه المخاطر وهي:

• التزييف العميق وتوليد التفاهات:

يشير هذا المفهوم إلى استخدام تقنيات الذكاء الاصطناعي من خلال الشبكات العصبية الاصطناعية لفبركة الأخبار والمحتويات السمعية والبصرية بصورة تبدو حقيقية، من أجل إنتاج الشائعات بهدف تشويه سمعة الأشخاص والسيطرة على عقول الشعوب. ويدخل هذا في إطار الحرب النفسية والإعلامية، التي تعد من أدوات ما يصطلح عليه بـ "حروب الجيل الخامس". يستهدف التلاعب العميق عموماً رواد منصات التواصل الاجتماعي، التي أصبحت بيئة جد خصبة لانتشار ولترويج الأخبار المضللة والمزيفة و"التفاهات" - على حد قول عراب الذكاء الاصطناعي "جيفري هينتون" - وهذا لكونها وسائل اتصال شديدة التأثير وواسعة النطاق، تتجاوز الحدود السياسية والطبقية وتتصل من خلالها مختلف شرائح المجتمعات.

تعتمد برامج التزييف العميق على تقنيات التعلم العميق وأشهرها "شبكة الخصومة التوليدية GAN"، يتطلب هذا قدرًا كبيرًا بشكل غير متناسب من بيانات التدريب لتدريب GAN، وغالبًا ما تستغرق شبكات GAN وقتًا أطول لتقديم صورة مقارنة بتقنيات إنشاء الصور الأخرى. تعد شبكات GAN أيضًا أفضل في إنشاء صور ثابتة من الفيديو، حيث تواجه شبكات GAN صعوبات في الحفاظ على الاتساق من إطار إلى إطار.

● الأسلحة الذكية:

تعتمد هذه الأسلحة على تقنيات التعلم العميق من أجل التعرف على الوجوه والأهداف التي تدرب عليها ورصدها ثم القضاء عليها، وهي إحدى الطرق التي يمكن أن يشكل بها الذكاء الاصطناعي خطراً على البشرية، حيث تطور منها القوى العظمى أعداداً كبيرة وتسعى إلى إدماجها في جيوشها النظامية، وهذا لتقليل الخسائر البشرية في المهمات الأمنية الخطيرة. وقد دعت الأمم المتحدة واللجنة الدولية للصليب الأحمر في أكتوبر الماضي القادة السياسيين إلى وضع قواعد دولية جديدة بشكل عاجل بشأن نظم الأسلحة ذاتية التشغيل. وقالت المنظمتان إن تلك الأسلحة، التي تختار الأهداف وتستخدم القوة بدون تدخل بشري، تثير مخاوف خطيرة، خاصة إذا خرجت عن السيطرة والتحكم البشري، ثم اتخذت قراراتها بناءً على معطيات مزيفة أو مضللة، مما يؤدي إلى عواقب وخيمة. وفي سيناريو مرعب، قد يدفع ظهور التزييف العميق الأسلحة الذكية في يوم من الأيام إلى إعلان حرب نووية مدمرة.

● انتهاك خصوصيات الأفراد التلاعب الاجتماعي:

من خلال خوارزميات الذكاء الاصطناعي المدججة في مواقع التواصل الاجتماعي، أصبح بالإمكان معرفة اهتمامات ورغبات وأسرار المستخدمين، وبالتالي إمكانية تخمين ما يفكرون فيه والتلاعب فيه، يحدث هذا غالباً تحت غطاء تحسين الخدمات. إضافة إلى أنه من خلال الروبوتات، أصبح ممكناً توجيه الرأي العام ونشر الفكر العنصري والتطرف لتفكيك النسيج الاجتماعي. ومن الأمثلة على ذلك جعل مؤسسات، مثل "كامبريدج أناليتكا"، تستخدم هذه البيانات في التأثير على المقترعين الأميركيين خلال الانتخابات الرئاسية الأميركية لعام 2016 واستفتاء خروج بريطانيا من الاتحاد الأوروبي (بريكست). تتضح هنا قوة الذكاء الاصطناعي في التلاعب الاجتماعي والتأثير السياسي وإحداث الانقسام بين الشعوب.

IV. 2/ التحديات:

وعموماً تتمحور أبرز التحديات الأمنية المرتبطة بتطور تقنيات الذكاء الاصطناعي حول ثلاثة نقاط أساسية تستوجب الاعتبار

وهي:

● نقاط الهشاشة:

إن إدماج تقنيات الذكاء الاصطناعي في المنظومات الأمنية يزيد من فرصة اختراقها، ويبدو الأمر أكثر تعقيداً إذا ما كنا أمام أنظمة متكاملة وقائمة على الذكاء الاصطناعي، وبالتالي فإن اختراق أي جزء من الأجزاء المكونة للنظام تقوضه كله وترهن أدائه، مما يؤدي إلى عواقب وخيمة. من جهة أخرى فإنه يمكن استخدام تطبيقات الذكاء الاصطناعي في مجالات أمنية على نحو سيء وغير مسؤول، مما يهدد الأمن الوطني. ومن بين السيناريوهات الخطيرة، فإن اختراق أنظمة المراقبة الذكية وتغيير إعدادات نماذجها وشبكاتها العصبية الاصطناعية يمكن أن يشل هذه الأنظمة ويعطلها ويجعلها عرضة للهجمات الإلكترونية التي تؤدي إلى تعطيل البنية التحتية للدول المتقدمة، خاصة إذا أخذنا بعين الاعتبار توفر عدة نماذج تعلم آلي مفتوحة المصدر، وانتشار منصات حوسبة سحابية ومكتبات تمكن من إنشاء وتطوير تطبيقات الذكاء الاصطناعي بكل سهولة كـ "تسرفلو" (Tensorflow) و "جوجل كولا ب" (Google Colab) وغيرها. ويحدث نفس الأمر غالباً إذا ما تم تعديل بيانات التدريب واختراقها، الأمر الذي يؤدي بنا إلى نماذج مشلولة غير فعالة ومنعدمة الكفاءة والتي يمكن أن تؤدي إلى تضليل أصحاب القرار بمعلومات مزيفة.

يتضح مما سبق، أن هناك ثغرات وهشاشات تسهل اختراق الأنظمة الأمنية المدججة لتقنيات الذكاء الاصطناعي، سواء من خلال النماذج أو من خلال بيانات التدريب، خاصة إذا أخذنا بعين الاعتبار ضخامة هذه الأخيرة التي عادة ما تكون سهلة الاختراق، وبالتالي لا بد من تدريب الأنظمة الأمنية الذكية على هكذا سيناريوهات للتعامل معها باحترافية.

● بيانات التدريب :

إن إنشاء تطبيقات ذكاء اصطناعي في المجالات الأمنية والعسكرية يستلزم توفر بيانات ضخمة لتدريب النماذج الذكية، الأمر الذي لا يعدو سهلاً في غالب الأحيان، خاصة إذا تعلق الأمر بالمعلومات الحساسة من مواقع لنقاط عصبية وتسليح ومخططات دفاعية إلى غير ذلك، وبالتالي فمن الصعب الحصول على بيانات واقعية، نزيهة وعالية الجودة اللازمة للتدريب، كما أن الأمر يكون أصعب بالنسبة للمشاريع التي تتم عن طريق الشراكة أو المناولة بين المؤسسات الأمنية والخاصة وبصفة أخص الأجنبية منها مما يرهن الأمن الوطني، الشيء الذي يعيق إنشاء مثل هذه التطبيقات. ومن أجل تجاوز مثل هذه السيناريوهات، طور الباحثون خوارزميات لتوليد بيانات ضخمة انطلاقاً من عدد محدود من البيانات كخوارزمية **ImageDataGenerator**، وهذا من خلال إضافة بعض التعديلات والملوثات عليها، ورغم أن البيانات الناتجة وهمية وليست حقيقية، إلا أنها كفيلة إلى حد ما بتدريب وبناء نماذج ذكية فعالة.

● تحيز المعلومات :

قد تكون المخرجات الناتجة عن النماذج متحيزة إلى فئة معينة أو عمر معين أو عرق معين، فتصدر أحكاماً متحيزة تجاه مجموعات معينة من الناس. يحدث هذا الأمر غالباً عندما تكون مجموعة بيانات التدريب محدودة، وتفتقر إلى عينات بيانات كافية لتمثيل جميع قيم بيانات الإدخال المحتملة بشكل مناسب. يبرز هذا كثيراً عند تبادل هذه التطبيقات من دول مختلفة حضارياً من حيث الثقافة والدين، وأحياناً في دولة واحدة، خاصة في ظل ما يسمى بالمجتمع الافتراضي الذي نجد فيه فئات اجتماعية تشكل تطبيقات الذكاء الاصطناعي أحد المصادر الرئيسية لبناء رصيدها الثقافي والمعرفي، مما ينجر عنه تصادم ثقافي بين هذه الفئات والفئات الأخرى. الأمر الذي قد يشكل في المستقبل تهديداً للأمن الثقافي والعقائدي للمجتمعات المستهلكة للتكنولوجيا، وتكون له آثار سلبية ومعاكسة على أنسجتها الاجتماعية، فالنموذج التوليدي Chat GPT مثلاً إذا سألته عن مسألة الإجهاض، ستكون إجابته إيجابية تعكس توجه الديمقراطيين

في الولايات المتحدة الأمريكية وفي نفس الوقت تناقض رأي الجمهوريين الذين لا يشجعون على الإجهاض، والسبب يعود لكون أن النموذج تم تدريبه في أول الأمر على بيانات تمثل نخبة المجتمع الأمريكي، الذين هم في الأصل غالبيتهم من الديمقراطيين. كذلك الأمر بالنسبة للتناقضات السياسية والفكرية في شاكلة : مقاومة - إرهاب، أو تطرف-تدين، إلى غير ذلك، ومنه يجب التنبيه إلى هذه النقطة الغير مألوفة والتي غالباً ما يتم إهمالها، كونها تشكل تهديداً جدياً ومباشراً على الأمن الثقافي للمجتمعات.

خاتمة :

إنَّ الدَّكَاءَ الاصْطِنَاعِيّ لم يعد قضيَّةً اقتصاديَّةً بحتةً، أو مجردَ صِرَاعٍ تكنولوجيٍّ ذو أبعادٍ اقتصاديَّةٍ كالصِّرَاعِ حَوْلَ تَكْنُوْلُوجِيَا الجِيلِ الخامسِ من الاتِّصَالَاتِ (5G) كما يروِّجُ له البعض، بل هو في الحقيقة أداةٌ سَيْطَرَةٍ وَهَيْمَنَةٍ، ووسيلةٌ من وسائل الحرب الحديثة والشاملة المتعددة المستويات والميادين، وهو ما يفسر التنافس الشديد بين عمالقة هذه التكنولوجيا في العالم، الذين ما فتئوا يستعرضون إمكانياتهم المتطورة والرَّهيبية في هذا المجال والتي يصفها البعض أنها تصل إلى حدِّ الخيال العلمي الذي كنا نشاهده في الأفلام في زمن مضي. الأمر الذي يستوجب منا قراءةً متأنَّةً للتحدياتِ الأمنيَّةِ التي يفرضها التطوُّرُ الرهيبُ لهذه التَقْنِيَّاتِ، واستشرافِ المخاطرِ التي قد تنجرُّ عنها، وأخذها على محملِ الجِدِّ للبحث في الآلياتِ الكفيلة بتحييد هذه المخاطرِ أو التقليل منها وإيجاد سُبُلِ إدارتها والتحكُّم في أبعادها، خاصة فيما يتعلق بحماية المقدَّراتِ الوطنيَّةِ وتحقيق الأمن الوطني بأبعاده المختلفة.

يقول الرئيس الروسي فلاديمير بوتين "إن الصِّرَاعَ الذي سنعيشه اليوم ومستقبلاً هو صِرَاعٌ على المعلومات"، فكمية المعلومات اليوم أصبحت بمثابة احتياطي النفط الخام في وقتٍ مضى، باعتبارها أساس بناء أنظمة الدَّكَاءِ الاصْطِنَاعِيّ التي أصبحت من أهم عواملِ الحسم في حروبِ الجيل الخامس، خاصة في بعدها النفسي الذي يعتبر التزييف العميق للأخبار أحد أهم أدواتها، بالإضافة إلى حربِ الأفكارِ والحربِ الثقافيَّةِ والاقتصاديَّةِ والمواجهة العسكرية. وبالتالي، فإن تحقيق الأمن الوطني في عالم اليوم يستند أساساً إلى السيطرة على المعلومة وتأمين مصادرها وتوظيفها واستغلال تقنيات الدَّكَاءِ الاصْطِنَاعِيّ لمواجهة الهجمات والتهديداتِ المتعددة المصادر، وهذا من خلال خططٍ وميكانيزماتٍ استراتيجيَّةٍ وفعاليَّةٍ على كافة المستويات.

فعلى المستوى الوطني، يجمع الخبراء على أن خط المواجهة الأول لكذا تحديات يتمثل في إتاحة المعلومة الصحيحة عبر مختلف منصات التواصل الاجتماعي من أجل ترسيخ بيئةٍ أقلَّ قابلية لانتشار الشائعات والتزييف العميق للأخبار، بالإضافة إلى وضع ترسانة قانونية وتنظيمية وهيئات ومراسد وطنية تعمل على التنسيق بين مختلف المصالح الأمنية للتعرف على مصادر الحروب النفسية والشائعات لمجابهتها. من جهة أخرى فإنه يتعين على الدولة تشجيع الاستثمار في البحث العلمي والمؤسسات الناشئة في الدَّكَاءِ الاصْطِنَاعِيّ وعلوم البيانات، وخاصة في المجالات المرتبطة بالدفاع والأمن، والاستفادة من الفرص التي تتيحها هذه التقنيات لرصد ومكافحة نشر الشائعات والأخبار المزيفة والهجمات السيبرانية في الفضاءات الإلكترونية، والتنبؤ بالهجمات الإرهابية كآليات تقنية لمواجهة هذه الأخطار.. هذا بالإضافة إلى ضرورة إطلاق مركز وطني للبيانات وتطبيقات الدَّكَاءِ الاصْطِنَاعِيّ، ومنصات وطنية للحوسبة السحابية، من أجل تنسيق الجهود البحثية بين مختلف القطاعات في الدَّكَاءِ الاصْطِنَاعِيّ، مع إدراج مقاييس الدَّكَاءِ الاصْطِنَاعِيّ في المنظومات التكوينية المختلفة موازاة مع ركب الرقمنة الذي تسير فيه الدولة الجزائرية، والاستلهاً من التجربتين الصَّيْنِيَّةِ والرُّوسِيَّةِ من حيث إنشاء منصاتٍ تواصلٍ اجتماعيَّةٍ وشبكات معلوماتية وطنية لحماية البيانات الوطنيَّة.

أما على المستوى الدَّولِيّ، يتطلب الأمر عقدَ إتفاقياتٍ دولية ومعاهداتٍ للحدِّ من مخاطرِ الدَّكَاءِ الاصْطِنَاعِيّ وخاصة المتعلقة منها بالأسلحة الذكيَّة وكذا التي تستهدف المنظومات القيميَّة والأخلاقيَّة للمجتمعات، وإرساء لوائح قانونيَّة دوليَّة ومعايير تنظيميَّة لتطبيقات الدَّكَاءِ الاصْطِنَاعِيّ، يخضع لها كل الفاعلين الدوليين، مع التأكيد على ضرورة التعاون الفعال بين مختلف الدُّول والمنظمات

الإقليمية والدولية في هذا المجال سواء تحت غطاء الأمم المتحدة التي بادرت في هذا الباب، أو في إطار المنظمات والتكتلات الإقليمية والدولية المتعددة.

ويبقى الوعي الفردي والمجتمعي هو الأساس الأول في مواجهة أخطار الذكاء الاصطناعي على الأمن الوطني، من خلال تنمية الحس الأمني والوعي الوطني وكذا الوازع الديني لدى الأفراد لحماية خصوصياتهم ولتخصيصهم ضد الشائعات والأخبار المزيفة، الأمر الذي يتأتى من خلال بناء إستراتيجية إنصالية فعالة، تشارك فيها مختلف مؤسسات الدولة لتعزيز ثقة المواطن بها وسد الفجوة بينه وبينها، وهذا عن طريق الحملات التحسيسية والدورات التكوينية والمتنقيات العلمية التي تستهدف مختلف فئات المجتمع حول ثقافة الأمن المعلوماتي والأمن السيبراني، التي تهدف للرفع من مستوى الوعي والثقافة لدى المواطنين ومواجهة هذه المخاطر والتقليل من آثارها.

قائمة الموامش :

¹Abbott, D. H (2010), Handbook of Fifth-generation Warfare 5gw, Nimble Books, p20.

² واثق علي الموسوي (2019)، الذكاء الاصطناعي بين النظرية والمعرفة الجزء الثاني ، دار الأيام للنشر والتوزيع، 2019 ، ص20.

³ زين عبد الهادي(2000) ، الذكاء الاصطناعي والنظم الخبيرة في المكتبات، المكتبة الأكاديمية، ص21.

⁴ بن نجمة محمد (2021) ، تطوير زراعة في دارة منطقية قابلة للبرمجة لشبكة عصبية التفاضلية لتطبيقات التعلم العميق، مذكرة لنيل شهادة الماستر في الهندسة الكهربائية مقدمة للمدرسة العسكرية المتعددة التقنيات، ص5.

⁵ نريمان مسعود بورغدة (2019) ، التجارة الإلكترونية في عصر الذكاء الاصطناعي: العقود المبرمة بواسطة العملاء الإلكترونيين الأذكياء، دار هومة للنشر والطباعة والتوزيع، ص51.

⁶ John Sanders (2016), Defining Terms : Data, Information and Knowledge , SAI Computing Conference, UK, p1.

⁷ مركز الإحصاء، (2020)، مفاهيم عامة حول البيانات الكبيرة، دليل رقم 13، أبو ظبي، ص4
⁸ كم يستثمر العالم في الذكاء الاصطناعي عام 2023، تم الاسترداد بتاريخ (15 أوت 2023)، من الموقع (https://sputnikarabic.ae).

⁹ إطلاق النسخة المحدثة من مسيرة "أوفود" الانتحارية الروسية ، تم الاسترداد بتاريخ (2023/08/14) من الموقع (<http://www.arabic.rt.com/videoclub/1485897>).

¹⁰ حسين يوسف أبو منصور (2020)، الذكاء الاصطناعي وأبعاده الأمنية، أوراق السياسات الأمنية، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، ص5.

¹¹ دور الذكاء الاصطناعي في تطوير محتوى إدارة الأزمات الإعلامية "نظرة مستقبلية" (2020)، مركز القرار للدراسات الإعلامية، تم الاسترداد بتاريخ (2023/11/15) من الموقع (<http://www.alqarar.sa/1118>)

¹² Adam Kutchak et al (2021), DAL-E, p3, Open AI, USA .

قائمة المراجع:

I- المراجع باللغة العربية: (ترتيب ألف-بائي)

1. زين عبد الهادي، الذكاء الاصطناعي والنظم الخبيرة في المكتبات، مصر، المكتبة الأكاديمية، 2000.
2. نريمان مسعود بورغدة، التجارة الإلكترونية في عصر الذكاء الاصطناعي: العقود المبرمة بواسطة العملاء الإلكترونيين الأذكاء، الجزائر، دار هومة للنشر والطباعة والتوزيع، 2019.
3. واثق علي الموسوي، الذكاء الاصطناعي بين النظرية والمعرفة الجزء الثاني، الأردن، دار الأيام للنشر والتوزيع، 2019.
4. بن نجمة محمد، تطوير زراعة في دارة منطقية قابلة للبرمجة لشبكة عصبية التفاضلية لتطبيقات التعلم العميق، مذكرة لنيل شهادة الماستر في الهندسة الكهربائية مقدمة للمدرسة العسكرية المتعددة التقنيات، الجزائر، 2021.
5. حسين يوسف أبو منصور، الذكاء الاصطناعي وأبعاده الأمنية، أوراق السياسات الأمنية، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، 2020.
6. دور الذكاء الاصطناعي في تطوير محتوى إدارة الأزمات الإعلامية "نظرة مستقبلية" ، مركز القرار للدراسات الإعلامية، تم الاسترداد بتاريخ (2023/11/15) من الموقع (<http://www.alqarar.sa/1118>).
7. كم يستثمر العالم في الذكاء الاصطناعي عام 2023، تم الاسترداد بتاريخ (15 أوت 2023)، من الموقع (<https://sputnikarabic.ae>).
8. مفاهيم عامة حول البيانات الكبيرة، مركز الإحصاء، دليل رقم 13، أبو ظبي، 2020.
9. إطلاق النسخة المحدثة من مسيرة "أوفود" الانتحارية الروسية ، تم الاسترداد بتاريخ (2023/08/14) من الموقع (<http://www.arabic.rt.com/videoclub/1485897>).

II- المراجع الأجنبية: (ترتيب ألف-بائي)

1. Abbott, D. H, **Handbook of Fifth-generation Warfare 5gw**, UK, Nimble Books, 2010.
2. Adam Kutchak et al, **DAL-E, p3, Open AI, USA, 2021.**
3. John Sanders, **Defining Terms : Data, Information and Knowledge**, SAI Computing Conference, UK, 2016.