IRAQI Academic Scientific Journals
العراقية المجلات الأكاديمية العلمية
مجلة كلية الكوت الجامعة
ISSN (E) : 2616 - 7808 II ISSN (P) : 2414 - 7419
www.kutcollegejournal.alkutcollege.edu.iq
k.u.c.j.sci@alkutcollege.edu.iq
عدد خاص لبحوث المؤتمر العلمي الدولي الخامس للإبداع والابتكار للمدة من 13 - 14 كانون الأول 2023

دور الذكاء الاصطناعي في ضبط الأمن السيبراني

ا.م.د. هبة زهير زيدان [1]

المستخلص

استقطب ميدان الذكاء الاصطناعي اهتمام العلماء لما شهده من تطورات مستمرة و سريعة ركزت على تصميم أنظمة محوسبة و منظومات مؤتمتة ذكية تحاكي القدرات العقلية للانسان و سلوكياته لكي تؤدي مهام عديدة في المجالات الاقتصادية و الطبية و الهندسية و العسكرية و التعليمية و البيئية و التنمية المستدامة و غير ذلك .بالتالي مثلت تلك الأنظمة الذكية أهم مخرجات الثورة الصناعية الرابعة لقدراتها في التحليل ، الاستنتاج ، التكيف مع ظروف الحياة ، بالإضافة إلى سرعة التعلم والاستفادة من التجارب والخبرات السابقة لحل المشاكل بالشكل السليم . لذا نرى اليوم تلك الأنظمة الذكية تخدم البشر من خلال تطبيقاتها في السيارات ذاتية القيادة والطائرات المسيرة بدون طيار و التعاملات المالية بالعملات الرقمية في التجارة الالكترونية، إضافة الى تعدين البيانات الضخمة، الروبوتات، المنظومات الصناعية المؤتمتة، و كل ذلك اثمر في تحول الحياة البشرية رقميا الى بيئة أفتراضية اندمجت فيها منصات التكنولوجيا و الاتصالات بالحوسبة السحابية و البيانات الضخمة في مايعرف بالفضاء السيبراني الذي بدوره وفرتجمعات رقمية للافراد و الحكومات و المؤسسات بهدف التواصل و الابتكار و الابداع و الانتاج و تقديم الخدمات اللامحدودة. لكنها أخضعت تلك التجمعات الى تحديات غير مسبوقة ازدادت حدتها بتداول وانتشار البيانات اللامحدود في الفضاء السيبراني بيد الخارجين عن القانون من جهات او افراد استغلت الفضاء السيبراني لنشاطها غير المشروع. فأصبح لزاما حماية الفضاء السيبراني بتقنيات و استراتيجيات أمنية ذكية تعرف بالامن السيبراني بحيث تسيطر و تضبط أمن الأنظمة المحوسبة و المؤتمتة الذكية مع الافراد و المؤسسات القائمين عليها. تبعا لذلك، تهدف ورقتنا البحثية هذه الى تسليط الضوء على دور الذكاء الاصطناعي في تحقيق الامن السيبراني الذي يحافظ على هوية الافراد و المؤسسات و خدماتهم و من ثم الثورة الصناعية الرابعة من النشاطات اللامشروعة كالاختراق، التضليل، التصيد، انتحال الشخصية، حجب الخدمات من خلال رؤية موضوعية لتطبيقاته.

الكلمات المفتاحية: الأمن السيبراني، الهجمات السيبرانية، الجريمة السيبرانية، الحرب السيبرانية، الذكاء الاصطناعي

انتساب الباحث
[1] جامعة النهرين ، كلية هندسة المعلومات ، العراق ، بغداد ، 10001

[1]hiba.zuhair.pcs2013@nahrainuniv.edu.iq

[1] **المؤلف المراسل**

معلومات البحث
تاريخ النشر: حزيران 2024

Affiliation of Author
[1] Al-Nahrain University, College of Information Engineering, Iraq, Baghdad 10001

[1]hiba.zuhair.pcs2013@nahrainuniv.edu.iq

[1] **Corresponding Author**

Paper Info.
Published: June 2024

The Role of Artificial Intelligence in Cyber-Security

Asst. Prof. Dr. Hiba Zuhair [1]

Abstract

Today, Artificial Intelligence (AI) attracts numerous scientists a continuous and a rapid development in the design of smart computerized and automated systems by simulating human mental capabilities and behaviors into smart tasks in the fields of economy, medicine, engineering, military, education, environment, and sustainable development. Thus, AI-based systems are being the topmost outcomes of the fourth industrial revolution due to their abilities in analyzing, conclusion, and adapting to alive circumstances as well as their fast compromising of the previous experiences for real-life problem solving. For example, AI-based systems and applications are serving humans in self –cars, auto-running aircraft, and financial transactions with digital crypto-currencies in e-commerce alongside data mining, robotics, and industrial internet of things. Correspondingly, human life becomes fully-digital environment in which platforms of various technologies and communications are merging together into the cyber space. That, in turn, provides digital communities and services to the individuals, governments and other enterprises for the aim of ultima innovation, creativity, and production. However, cyber-space is facing unprecedented challenges which boost up their limits by exploiting big data

exchanged in cyber space in the hands of outlaws of entities or individuals who utilize cyber-security for their illegal activities and profits. So far, it becomes necessary to protect cyberspace with sophisticated security techniques and strategies known as cyber security so that they control and control the security of computerized and smart systems with individuals and institutions in charge of them. Accordingly, our research paper aims to highlight the role of artificial intelligence in achieving liberal security that preserves both individuals' and enterprises' identities and services. Then, the fourth industrial revolution is threatening by penetration, misinformation, hijacking, hoaxing, identity theft, and denial of services.

Keywords: Cyber-security, Cyber-attacks, Cyber-crimes, Cyber-warfare, Artificial Intelligence

المقدمة

اعتادت دول العالم التنافس على اكثر التقنيات تطورا و استباقية وضع الحلول الثورية الناجحة لمعظم المشكلات و الكوارث. فأتجهت نحو تفعيل و استثمار الثورة الصناعية الرابعة و التي في مقدمة مخرجاتها تقنيات و تطبيقات الذكاء الاصطناعي لتحقيق أهدافها التنموية الطموحة. فأعتمدت قطاعات الصحة والتعليم والصناعة و النفط و الخدمات الحيوية على الذكاء الاصطناعي لما يوفره من فرص اقتصادية و استثمارية كبيرة لتحقيق أرباح طائلة بسبب مايقدمه من حلول و استنتاجات و استشارات دقيقة و قرارات حاسمة ذات تأثيرات ايجابية في تقليل الاعتماد على عمالة العنصر البشري و رفع جودة الموارد البشرية و الصناعية. و لتعزيز ذلك انتهجت دول العالم الاستراتيجيات المدروسة و الآنية لتنمية وتطوير الكفاءات العلمية المتخصصة والقدرات المحلية في مجال الذكاء الاصطناعي وعلم البيانات و تعدينها في أنظمة الكترونية ذكية و خبيرة. مما خلق ثقافة الذكاء الاصطناعي لدى فئات المجتمع كافة لتسهيل انتشار استخدام تطبيقاته ومنصاته الرقمية فأصبح المواطن العادي، الحكومة، المجتمع رقميا [1,2]. و لكن ترتب على ذلك تعرض البيانات و الهوية الرقمية للافراد ، المجتمعات، المؤسسات الى الانتهاكات و التهديدات بسبب المنصات و البيئة الرقمية الافتراضية التي تتغذى ببيانات مستخدميها وعليه اصبح لزاما التفكير في استراتيجيات و تقنيات تضمن حقوق رواد البيئة الافتراضية من أفراد، مجتمعات، و مؤسسات و الحفاظ على امنهم الافتراضي [2].

ما سبق يقودنا الى طرح التساؤلات الرئيسية التالية:

- ما مدى فعالية الذكاء الاصطناعي في مجابهة الج رائم الواقعية ؟
- كيف يوظف الذكاء الاصطناعي في تحقيق الامن السيبراني وحماية المجتمعات في الفضاء السيبراني؟

و التي ستتم الاجابة عليها من خلال ثلاثة مباحث في هذه الورقة البحثية ، و هي:

- أنظمة الذكاء الاصطناعي و تقنياته.
- دور أنظمة الذكاء الاصطناعي في ضبط الجرائم الواقعية حاليا.
- توظيف أنظمة الذكاء الاصطناعي في ضبط الجرائم الالكترونية و توفير الأمن السيبراني مستقبلا.

المبحث الأول: أنظمة الذكاء الاصطناعي وتقنياته

الذكاء الاصطناعي هو قدرة الآلة على محاكاة العقل البشري و قدرت ه على التفكير، والاكتشاف والاستفادة من التجارب السابقة، ومنذ التطوّر الذي شهدته أجهزة و تقنيات الحاسوب و الانترنيت في منتصف القرن العشرين، تمَّ اكتشاف أنَّ أنظمة الحاسوب باستطاعتها القيام بمهمات أكثر تعق يداً مما يعتقد البشر، حيث يمكنها اكتشاف الإثباتات للنظريات الرياضية المعقدة بالإضافة لقدرتها لحل المسائل الفكرية المعقدة كممارسة لعبة الشطرنج بمهارة كبيرة، و بالرغم من إيجابياتها الكثيرة من حيث سرعة معالجة البيانات باعداد هائلة و توفير السعة العالية لتخزين هذه البيانات إلا أنها لازالت غير فعالة بمجاراة مرونة العقل البشري خصوصاً بمايتعلق بالوعي و الادراك و التحليل و الاستنتاج التلقائي لاعطاء القرارات الحاسمة للمهمات المطلوبة منها [1,3]. ولجعل هذه الانظمة تضاهي مستوى أداء العقل البشري تم دعم قدراتها المحدودة بخصائص و تقنيات الذكاء الاصطناعي للقيام بمهامها كأنظمة كفوءة في التشخيص الطبي. على سبيل المثال، أنظمة التعرف هوية الفرد من خلال موجات الصوت او الاستدلال عن هويته بالكتابة اليدوية. كما أصبح الذكاء الاصطناعي الاتجاه البديل عن العقل البشري و مهاراته في كثير من المجالات. فمثلا، قد يحتاج قائد طائرة مقاتلة إلى عون أنظمة ذكية للمساعدة في قيادة

الطائرة بمسارات وظروف ملاحية شديدة التعقيد[4]. لذا سنتطرق الى مميزات الذكاء الاصطناعي التي تشمل:

أولا: خصائص الذكاء الاصطناعي [3]:

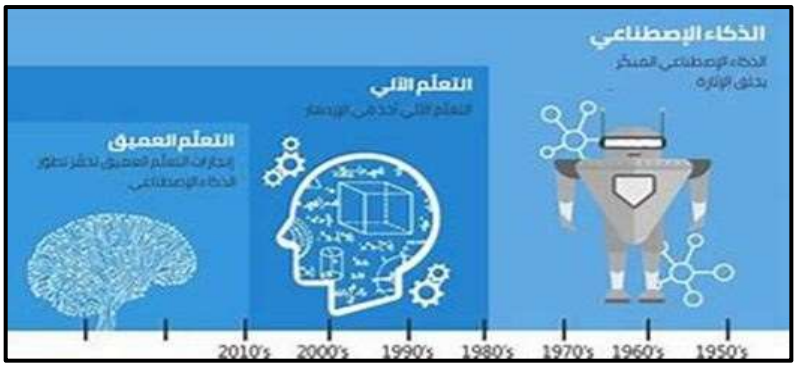
- التمثيل الرمزي: وهو عن طريق استخدام الرموز ف ي تمثيل المعلومات المختلفة.
- استخدام الأسلوب التجريبي المتفائل: من الصفات المهمة في مجال الذكاء الاصطناعي ان برامجها تقتحم المسائل التي ليس لها طريقة حل عامة معروفة، وهذا يعني ان البرامج لا تستخدم خطوات متسلسلة تؤدي الى الحل الصحيح ولكنها تختار طريقة معينة للحل تبدو جيدة مع الاحتفاظ باحتمالية تغيير الطريقة إذا اتضح ان الخيار الأول لا يؤدي الى الحل سريعاً، أي التركيز على الحلول الوافية.
- البيانات غير المؤكدة أو غير الكاملة: وذلك عن طريق ايجاد الحلول المناسبة في الوقت المناسب، وليس معنى ذلك أن نقوم بإعطاء حلول مهما كانت الحلول غير صحيحة أو صحيحة، وإنما أن تكون قادرة على تقديم الحلول المقبولة، وإلا تصبح غير وافية.
- القدرة على التعلم: وهي قدرة مهمة تهدف إلى إكساب الإنسان المزيد من المعلومات والمهارات الإضافية التي تساعده في تنمية قدراته.

ثانيا: أنظمة الذكاء الاصطناعي [4]:

- النظم الخبيرة: هي برامج معلوماتية خاصة تهدف الى محاكاة منطق الانسان الخاص بالخبراء في ميدان معرفي خاص.
- الشبكات العصبيةNeural Networks : هي شبكات تستند الى نظم قواعد المعرف ة الموزعة على حزم ة من النظم والبرام ج التي تعمل من خلا ل عدد كبير من المعالجات بأسلوب المعالجة الموازية وتستند الشبكات العصبية على قواعد المعرفة وتستخدم المنطق المهم غيرالقاطع. وبالتالي يمكن القول ان الشبكات العصبية هي نظم معلومات ديناميكية تتشكل وتبرمج طيلة مدة التطوير المخصصة للتدريب والتعليم، أي انها نظم تتعلم من التجربة وتكتسب خبراتها ومعارفها من خلال التدريب والتعلم بالممارسة العلمية.
- نظم الخوارزميات الجينية: هي برامج الكمبيوتر التي تحاكي عمليات بيولوجية من اجل تحليل مشاكل النظم التطورية.
- نظم المنطق الغامض أو المبهم Fuzzy Logic : و هو طريقة تعتمد على الادراك وتحاكي طريقة إدراك العنصر البشري من حيث تقدير القيم عن طريق بيانات غير ضبابية، ويقوم المنطق الجديد على استكشاف الظواهر والحالات الأخرى الوسطى أو غيرها، بمعنى البحث عن المنطقة الرمادية بى ن اللونين المتناقضين الأسود والأبيض.
- نظم الوكيل الذكي Agent Systems: يعرف الوكيل الذكي بأنه عبارة عن كائن يستطيع إدراك بيئته التي يكون موجود فيها وذلك عبر المستشعرات التي يمتلكها هذا الكائن ومن ثم التجاوب معها بواسطة آليات التنفيذ أو الجوارح.

ثالثا: تقنيات الذكاء الاصطناعي [4]:

- التعلم الآلي MACHINE LEARNING : قد أخذ التعلم الآلي الذكاء الاصطناعي إلى مستوى أعلى من تنفيذ القواعد المحددة مسبقًا. بواسطة الخوارزميات التي تمكن أنظمة الكمبيوتر من التعلم من بياناتها عن طريق إنشاء روابط بينها.
- التعلم العميق DEEP LEARNING: ذو مستوى أعلى من التعلم ا لآلي حيث يعتمد على خوارزميات التعلم التي لا تتطلب الإدارة اليدوية. كما يسمح باستخدام مجموعات البيانات الكبيرة المتاحة Big Data وقوة الحوسبة لأجهزة الكمبيوتر و مستودعات البيانات data Warehousesو الخوادمServers ، وقوة المعالجProcessors ، والحوسبة في السحابةCloud Computing.
- التعلم الطبيعي NATURAL LEARNING PROCESSING: تعد معالج ة اللغة الطبيعية أحد تطبيقات التعلم الآلي و العميق والتي تهدف إلى التعر ف على الكلام. لقد مكنتنا سنوات عديدة من البحث في هذ ا المجال من العمل مع مجموعات كبيرة من البيانات كعينات نصية توفر السياق والمعجم اللغوي والنحوي والمعاني الدلالية. الشكل (1) يوضح تقنيات الذكاء الاصطناعي الحالية و مستوى تقدمها و تطورها عن مثيلاتها.



الشكل (1): أشهر تقنيات الذكاء الاصطناعي.

المبحث الثاني: دور أنظمة الذكاء الاصطناعي في ضبط الجرائم الواقعية

لجعل أنظمة الحاسوب والمعلومات تضاهي مستوى أداء العقل البشري تم دعم قدراتها المحدودة بتقنيات الذكاء الاصطناعي للقيام بمهامها كأنظمة كفوءة في التشخيص الطبي على سبيل المثال، أنظمة التعرف هوية الفرد من خلال موجات الصوت او الاستدلال عن هويته بالكتابة اليدوية. كما أصبح الذكاء الاصطناعي الاتجاه البديل عن العقل البشري و مهاراته في كثير من المجالات. فمثلا، قد يحتاج قائد طائرة مقاتلة إلى عون أنظمة ذكية للمساعدة في قيادة الطائرة بمسارات ملاحية محددة وظروف ملاحية شديدة التعقيد. في مجال الطب مثلا، تستخدم انظمة الذكاء الاصطناعي لدعم العاملين بالقطاع الصحي أثناء تأديتهم لواجباتهم و خصوصا المهام التي تعتمد على مداولة البيانات التشخيصية للامراض المستعصية فقد يعمل النظام الحاسوبي الطبي القائم على الذكاء الاصطناعي داعما للطبيب في أجراء الفحص السريري مثل أنظمة التصوير بالرنين المغناطيسي(MRI) لاكتشاف مؤشرات تساهم في وضع الخ طة العلاجية التي تتطلبها حالة المريض كما تمكن الطبيب المعالج من أكتشاف أنماط في البيانات تشير الى حدوث تغييرات فسلجية مهمة في تحسن حالة المريض [5,6].

كما دعمت أنظمة الذكاء الإصطناعي عملية البحث العلمي في مجالات العلوم والهندسة كما في مجالات الطب. تحديدا، تمتلك أنظمة الذكاء الاصطناع ي قابلى ة التعلم والتدريب على انماط واردة ومتكررة في الوقت الحالي لاكتشاف ظواهر جديدة وخلق مجال معرفي متخصص. فعلى سبيل المثال، يمكن استخدام نظام حاسوب قائم على تقنيات الذكاء الاصطناعية و آليات التعلم التلقائي لتحليل كميات كبيرة من البيانات تعدينها بالبحث عن أنماط مركبة بها توحي بإرتباطات او أنماط جديدة من البيانات لم تكن متوقعة و غير مكتشفة من قبل [6].

و في الجانب الأمني، كان للتكنولوجيا الحديثة لاسيما الانظمة المعتمدة على الذكاء الاصطناعي دورا هاما في الحد من الجريمة كأنظمة كاميرات المراقبة حيث لم تعد أنظمة كاميرات المراقبة مجرد مشروع تكميلي او رفاهية في المنازل، وتقاطعات الشوارع، المحال التجارية ، و مداخل أبنية المؤسسات و الشركات. بل نجحت في رصد لاسيما في رصد وإزالة غموض الكثير من الجرائم كما أسهمت كأداة مساعدة للجهات الأمنية في القبض على المجرمين، والمطلوبين أمنياً. خصوصا عندما اعتمدت على خوارزميات ذكية و أجهزة استشعار حرارية لتعقب الكيانات الحية و رصد ملامح الوجوه و تحليلها و استخلاص بيانات هامة في مطابقة الأنماط المتوفرة في ارشيف المطلوبين أمنيا [6]. حيث تتكون أنظمة المراقبة بالكاميرات من مجموعة كاميرات متصلة عن طريق وسط تراسلي مع جهاز تسجيل مركزي أو عدة أجهزة تسجيل منفصلة تقوم بتسجيل الأحداث لمدة زمنية تتحدد طبقا للسعة التخزينية المتاحة لنظامها الالكتروني وفي كثير من الأحيان يتم تحليل المادة المصورة بالكاميرا ذاتها أو بجهاز التسجيل لإستخراج إحصائيات وبيانات تفيد في إكتشاف بوادر الجريمة قبل لحظة وقوعها و تؤمن مستويات مختلفة لدخول المنظومة والتعامل معها من خلال كاميرات داخلية ثابتة أومتحركة، كاميرات خارجية ثابتة ومتحركة، كاميرات بعيدة المدى ، كاميرات رؤية ليلية، كاميرات حرارية. لذلك أسهمت هذه الانظمة الذكية في حماية الأصول والممتلكات وتوفير الشعور بالأمان في مجتمعاتنا على ارض الواقع مؤخرا [7، 8] .

و بشكل مماثل، كان للبوابات الإلكترونية دور كبير في تنظيم عمل المنشآت بما يتلائم مع طبيعة عمل كل منشآة، مثل توزيع صلاحيات الدخول للافراد العاملين و الرؤساء و المدراء اضافة الى أليات السماح للأفراد من الجمهور بدخول المنشآة. فمثلا في المستشفيات، تحدد ساعات معينة في اليوم لزيارة المرضى، وإذا لم يكن هناك حراس للبوابات ستحدث فوضى في دخول الجمهور في

أوقات غير مسموح لهم بالزيارة، وإذا لم يتم أستخدام بوابات إلكترونية للكشف عن الداخلين و الخارجين من المستشفى فقد يتيح ذلك الفرصة لدخول أشخاص بدوافع اجرامية او أدوات ومواد غير مصرح بها، وبالتالي تعرض المستشفى والمرضى لخطر جسيم [7، 8].

المطارات ايضا كمنشآت لها استراتيجيات أمنية خاصة تتوافق مع طبيعتها، والتي تشمل ادارة مسارات الطائرات ، ادارة اوقات الاقلاع و الهبوط، تأهيل و فتح مدارج الطائرات باوقات محددة، ادارة بيانات المسافرين ، تحديد أوقات و شروط الدخول والخروج للمسافرين، إلي جانب تفتيش المركبات، سواء قبل دخولها أو عند خروجها، فمن الممكن أن يتعرض المسافرين و المطار لهجمات ارهابية، و بذلك فان أنظمة البوابات الالكترونية الذكية تمكن طاقم حراس مداخل و مخارج حيز المطار من مراقبة و متابعة و تدقيق المركبات و الافراد تلافيا لأي خطر جسيم. فعلى سبيل المثال تقوم البوابات الإلكترونية بإكتشاف المواد المعدنية و يتم الابلاغ عنها ان وجدت باضاءة لمبات تشير الى اتجاه المعدن مع صدور صوت انذار لتحذير طواقم الحماية و أمن المطار و ادارة حركة المسافرين بأنسياب ية وكفاءة العالية [7].

من الامثلة الاخرى، أنظمة الذكاء الاصطناعي لكشف بصمة العين و التعرف على هوية الافراد المطلوبين من خلالها باستخدام سمات بشرية و فسلجية دقيقة مع تقنيات أحيائية تعمل من خلال التقاط صورة لقزحية العين او الشبكية ومن ثم تخزينها، وإنشاء رموز مشفرة تستخدم لمطابقة البصمات المستخلصة مع بصمات العين المؤرشفة للمطلوبين أمنيا بسرعة وفاعلية و قد لا تستغرق العملية سوى ثوان معدودة [8].

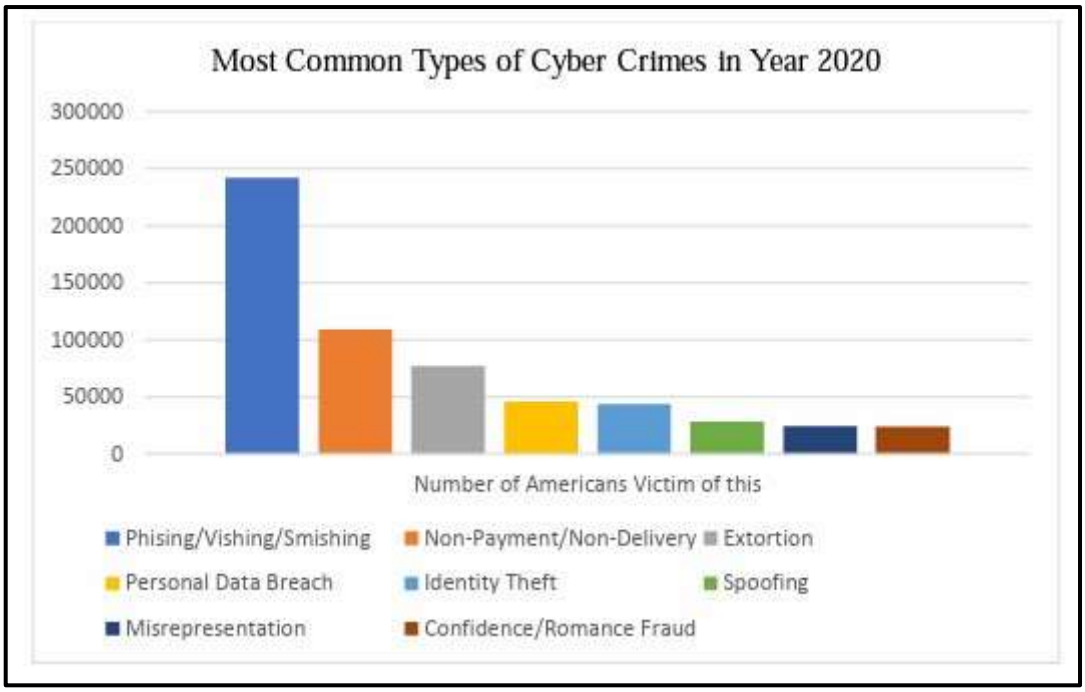
كل ماسبق ذكره من أمثلة واقعية يبرر ضرورة الذكاء الاصطناعي في حياة البشر و تنمية المجتمعات و تطوير البنى التحتية الأمنية المعقدة. حيث تتيح الانظمة الذكية التنبؤ بالجرائم المتوقعة باستخدام خاصية التعلم الآلي Machine Learningالمعتمدة على البيانات المرصودة او المؤرشفة التي تتعامل مع الجريمة أو الحدث على أنهما من أنماط السلوك الإنساني التي تترجم بصيغة نماذج حسابية لخوارزميات الذكاء الاصطناعي لكي تتنبأ بما هو آت من فعل قد يكون غير متوقعا. وبذلك تفوقت أنظمة الذكاء الاصطناعي على الاساليب والأدوات التقليدية المستخدمة في المجالات الأمنية من حيث [8,9]:

- الكشف عن التفاصيل الدقيقة التي يعجز العنصر البشري عن إكتشافها .
- العمل في مختلف الظروف و البيئات الواقعية.
- الاستمرارية بالعمل دون ملل أو كلل وعد م التقيد بأوقات عمل محددة.
- وسيلة مهمة للردع النفسي لافراد والمجموعات بمختلف دوافعهم الاجرامية.
- المساهمة في كشف الجريمة قبل وقوعها.
- المساهمة في التوصل للجناة وتعقب المطلوبين بعد ارتكابهم الجرائم.

المبحث الثالث: دور أنظمة الذكاء الاصطناعي في ضبط الأمن السيبراني

يعرف الأمن السيبراني Cyber security بأنه تأمين الأنظمة والشبكات والبرامج من الهجمات الرقمية ومن أي مشكلة أو عائق إلكتروني أثناء تبادل البيانات المتاحة في الفضاء السيبراني والمخزنة في خوادم مترابطة عبر شبكات الحاسوب اللاسلكية وشبكات التواصل الاجتماعية والمواقع الالكترونية. وتهدف الهجمات الرقمية عادة إلى الوصول إلى المعلومات السرية بهدف تغييرها أو إتلافها أو استخدامها كوسيلة لابتزاز الأموال من أصحابها و مستخدميها. كما أفرز التحول الرقمي من البيئة الواقعية الى البيئة الرقمية الافتراضية حاجة ملحة لدى المجتمع لما يعرف بشبكات ومنصات التواصل الاجتماعية Social Networks و لكن الاستخدام المتنامي لتلك المنصات تم على مستوى العالم بدون وجود لوائح متسقة ومُقننة لتنظيم استخداماته، مع عدم وجود بروتوكولات عالمية تضمن إمكانية استخدام أوجه مختلفة من الذكاء الاصطناعي بطرق لا تشكل تجاوزات للخصوصية والحرية الشخصية واستخدام البيانات، إلى جانب عدم وجود الإرادة السياسية لوضع المعايير والقواعد المنظمة لهذا المجال فاصبحت عواقب استخدامها كارثية مما سبب زيادة كبيرة في الهجمات و التهديدات السيبرانية بمختلف أنواعها كما هو موضح في الشكل (2) [10].

وعليه سيتناول هذا المبحث الجهد العالمي لدمج الذكاء الاصطناعي مع اساليب وتقنيات الدفاع والردع السيبراني لضبط الامن السيبراني تليه بعض الملاحظات و التوصيات.



الشكل (2): الزيادة الملحوظة لأشهر هجمات الامن السيبراني التي تستخدم تقنيات الذكاء الاصطناعي لسنة 2020 [10].

أولا: الهجمات السيبرانية Cyber-Attacks

باتت الهجمات السيبرانية أكثر تعقيداً من أي وقت مضى على مدار السنوات الأخيرة، إذ عانت أنواع التكوينات الإلكترونية المختلفة والعديد من القطاعات الصناعية من مجموعة كبيرة من الهجمات السيبرانية التي أسفرت عن بعض النتائج المُدمرة. وقد تجلت تلك السبل في هيئة برمج يات فدية وبرمجيات ضارة خبيثة (Malware) وطرائق تلاعب وتصيد إلكتروني وتصيد احتيالي استهدافي Phishing. وقد تحملت البنية التحتية الوطنية الحرجة Cyber National Infrastructure - CNI العبء الأكبر. لهذه الهجمات، وذلك لأسباب عدة، بدايةً من البيانات الحسّاسة التي يمكن أن تتراكم تدريجياً في هذه البنية، وصولاً إلى معرفة حجم التأثير في نطاقها. فإما أن يكون لتلك الهجمات آثار مدمرة لكن محتملة، وإما أنها ستخلِّف حالة من عدم الاستقرار أو الريبة والشك لتشكِّل مصدراً للخطر الجسيم [10].

ورغم أن حالات خرق البيانات تعد حوادث بالغة الخطورة، فإن هناك قلقاً متزايداً بين السواد الأعظم من المؤسسات من الهجمات المُصمَّمَة لإحداث أثر أكثر تدميراً، كهجوم أوكرانيا السيبراني في عام 2015 الذي أدى إلى تعطل شبكة الكهرباء بالكامل كالهجوم المتطور الذي وقع بعامٍ واحد في مدينة كييف، ورغم أنه أدى إلى انقطاع التيار الكهربائي لفترة وجيزة، فقد أثار المزيد من القلق بشأن الكيفية التي صُمِّمَ بها الهجوم ووُضِّع موضع التنفيذ، أو كهجوم برمجيات الفدية Ransomwaresالمشهور بـ WannaCry عام 2017 الذي أدى إلى شيوع حالة من الفوضى واسعة النطاق في مؤسسات الرعاية الصحية في العديد من دول العالم، حيث عجزت تلك المؤسسات عن تنفيذ أي مهام بعد أن أمسى الوصول إلى بياناتها و نظمها غير متاح وتؤدي مثل هذه الهجمات التي تنال من البنية الأساسية الوطنية الحرجة في قطاعات كالرعاية الصحية والطاقة وما إلى ذلك، إلى حالات خرق/انقطاع للبيانات، كما أن لديها القدرة أيضاً على تعزيز نقاط الضعف في العمليات الصناعية، خاصة أن البنية الأساسية القديمة تشتمل على نظم تحكم آلي ونظُم للتحكم الإشرافي وتحصيل البيانات [11].

ولعل الهجمات السيبرانية المدعومة من الدول هي التي تثير القلق أكثر من غيرها، إذ تميل إلى تبنّي مستوى أكثر تعقيداً وتزيد من حجم الأضرار المحتملة التي تلحق بأهدافها إلى أقصى حد ممكن. ولذلك، ينبغي أن تتمتع منظومة القيادة والتحكم والاتصالات والحوسبة والأمن السيبراني والاستخبارات والمراقبة والاستطلاع بمستويات أعلى من قابلية التشغيل البيني، وأن تدُمج في المناخ الحالي والمتسارع للحرب الرقمية وأن تستجيب له استجابة سريعة لا إبطاء فيها. ومن الواضح أن القيادة السيبرانية باتت أولوية بالغة الأهمية، حيث تصب المبادرات الجاري بحثها براً وبحراً وجواً والاستثمارات الكبيرة في ضمان تطورها وتقدمها [12].

ثانيا: الحرب السيبرانية الباردة Cyber Warfare

بالتزامن مع تطور تقنية الأتمتة والذكاء الاصطناعي التي انتشرت في القطاعات العامة والخاصة والحياة الصناعية جميعها، أمسى الترابط البيني للنظم التي كانت في فترة من الفترات بعيدة ومستقلة وتفصل بينها فجوات هوائية، يزداد بشكل مُطرد. ورغم أن هذا الترابط يكفل طرائق مثمرة وسلسة وفعّالة لتشغيل تلك النظم ومراقبتها وتعظيم فعاليتها إلى أقصى حد ممكن، فإن هذا الترابط بحد ذاته هو الذي يمكن أن يخلق نقطة ضعف جسيمة. وهذا الضعف هو مصدر الإجراءات الانتهازية التي نشير إليها في سياق الحرب السيبرانية [13].

وتستطيع الأطراف مصدر التهديد المرتبطة بالدولة أو المعادية، باستغلال آلياتٍ على شبكة الإنترنت، التسلل إلى هذه النظم والتلاعب بها وشن هجمات عليها، فتصيبها بأثر مدمر جسيم. ومن الأهمية بمكان أن تتُخذ إجراءات لائقة للحد من خطورة هذه التهديدات ونقاط الضعف عبر مراجعة النظم الداخلية وتأمينها، وكذلك عن طريق فهم المَوَاطن التي يمكن أن تستتر فيها نقاط الضعف تلك داخل النظُم، وأثر الضرر الذي يمكن أن يلحق بها إذا ما استغُلتَّ. ومن المهم ألا نفهم قدرات كيفية الاستجابة حال وقوع أي هجوم فقط، وإنما أن ندرك مدى مواءمة ردود الأفعال تلك وموقفها القانوني أيضا [13].

تتمثل التهديدات المستمرة المتقدمة في هجمات سيبرانية مدمرة وخبيثة تستهدف أهدافاً رفيعة المستوى وعظيمة القيمة. وفي غالبية الحالات، وُجِّدَ أن مجموعات التهديد هذه مدعومة من الدولة، ما يجعلها ممولة تمويلاً كبيراً ومنظمة وواسعة الحيلة. وتتراوح أهداف الهجمات بين سرقة البيانات وتقويض البنية التحتية الوطنية الحرجة. وتختلف هذه الهجمات السيبرانية المدمرة والخبيثة عن الهجمات السيبرانية التقليدية من أوجه عدة، غير أن الفارق الأساسي الذي يميزها هو نهجها "المستتر والوئيد" الذي يحول دون رصدها. وقد حقق هذا النهج نجاحاً كبيراً في حالات عدة، إذ رُصدت الهجمات من هذا النوع بعد سنوات من عدوانها. وكثير من الهجمات التي ترُصد حالياً ظل قيد الإعداد والتجهيز لأكثر من عقد كامل. وما يثير القلق أكثر من غيره حقيقة أن آليات الدفاع التقليدية فشلت في رصد تلك الهجمات [14].

ثالثا: تقنية التزييف العميق الذكية Deep Fake

من الممكن أن يستخدم الذكاء الاصطناعي كأداة من أدوات الحرب النفسية في الواقع المعاصر، من خلال ما يعرف بـ "التزييف العميق" الذي يمكن أن يتم من خلاله تخليق صورة إنسان استناداً إلى خوارزميات الذكاء الاصطناعي. وقد ظهرت تقنية التزييف العميق أول مرة لأغراض الترفيه والتسلية. وتتيح برمجيات خاصة تستند إلى الذكاء الاصطناعي فرصة خلق مُستنسخات تظهر وتتحدث وتتصرف بالضبط كأصولها المعتمدة عليها. وهناك تزايد في احتمالات استغلال التزييف العميق لأغراض خبيثة، إذ يمكن أن يخلق المرء مُستنسخاً من شخصية معروفة ويتلاعب بكلماتها. وهناك مجموعة كبيرة من الأمثلة على التزييف العميق في العالم الحديث، وكذلك خدمات الإنترنت التي تساعد على صنع تلك النماذج. لكن بالمنطق نفسه، يمكن استغلال الذكاء الاصطناعي وتقنياته بغية الحيلولة دون انتشار الاستخدام الخبيث لتقنية التزييف العميق أيضاً، التي يمكن أن تشُكِّل خطراً داهماً على الأمن النفسي [16,15].

رابعا: الذكاء الاصطناعي وإنترنت الأشياء IoT

يتبنّى المستهلكون بحماسٍ شديد تقنية إنترنت الأشياء وفي عام 2020، بلغ عدد أجهزة إنترنت الأشياء إجمالاً 31 مليار جهاز مُنتشرة حول العالم. لكن بينما تشهد هذه الأجهزة انتشاراً كبيراً وسريعاً، يتفاقم في الوقت نفسه مشهد المخاطر ومكامن الضعف المترتبة على هذا الانتشار. وما يزيد من خطورة الأمر هو أن هذه الأجهزة دخلت البيوت والشركات والصناعات وتسللت إليها ، وباتت الآن موجودة في مختلف القطاعات الحساسة بما فيها قطاع الرعاية الصحية. وإحدى هذه المخاطر هي أن تلك الأجهزة عُرضةً بسهولة للهجمات، كما أنها عُرضة كذلك كي تسُتخدم لشن هجمات على نطاق اقتصادي ومجتمعي واسع. وفي ظل قصور إجراءات التقييم وتنامي حدة المنافسة المُتسارعة، يعُمم مزودو خدمات إنترنت الأشياء أجهزةً يَنْصَب تركيزها على الابتكار دون مراعاة التوازن السليم بين عناصر الأمن والأداء وسهولة الاستخدام. ويؤدي ذلك إلى وجود طرق هجوم جديدة تسُهِّل على المهاجمين اختراع النظُُم بثقةٍ شديدة دون الحاجة إلى أن يكونوا خبراء، والفضل في ذلك يرجع إلى مجموعة متنوعة من الأدوات مفتوحة المصدر المتاحة على شبكة الإنترنت [18، 17].

خامسا: الذكاء الاصطناعي وأجيال الشبكة اللاسلكية (Wireless Network Generations)

صُمم الجيل الخامس من الاتصالات اللاسلكية للسماح بالتغطية بعيدة المدى والاتصالات المستقرة، وكذلك التحميل والتنزيل فائق السرعة للبيانات. ونتيجة للتقنية اللاسلكية المعتمدة على هذا الجيل، يساعد تكامل البيانات على وصول السرعات إلى 20 جيجابايت

في الثانية عبر وصلات البيانات النقالة اللاسلكية. وتجعل قدرة بروتوكولات الإنترنت على نقل كميات مهولة من البيانات بسرعات فائقة ودون تأخير ملحوظة، مقارنةً بالأجيال السابقة من تقنية نقل البيانات المحمولة، وهذا الجيل الجديد مثالياً لنظم إنترنت الأشياء والنظم المؤتمتة الحالية، وتساعد كذلك على استحداث نظم جديدة ونشرها [19]. وبينما يبدو أنّ الجيل الخامس من الاتصالات سيبدد مثل هذه القيود التي خلقتها الأجيال السابقة، فإن هناك جوانب سلبية لهذا الجيل أيضاً. فترددات هذا الجيل وموجاته القصيرة، التي تعُرف باسم "الموجة المليمترية"، لهما نطاق تأثير محدود جداً، رغم إتاحتهما لسرعات نقل بيانات فائقة وتقليصهما لبطء انتقال البيانات. على سبيل المثال، لا تستطيع إشارات الجيل الخامس من الاتصالات اختراق البنايات وغيرها من الحواجز أو الانعكاس عنها. وهذا يعني أنه لتحسين شبكات الجيل الخامس بأقصى قدرممكن، لا بد من الحفاظ على مسار رؤية مستقيمة بين الأجهزة المتصلة والمُرَحِّلات) نقاط الاتصال (أو على أقل تقدير إبقاء أدنى عدد ممكن من المعوقات. وثمة طريقة للتحايل على هذا القيد تتمثل في تكثيف الإشارة واستغلال عدد كبير من نقاط اتصال خلايا الراديو الصغيرة في شتى أنحاء منطقة التغطية. غير أن ذلك سيتطلب استثماراً أكبر وإعادة تطوير للبنية التحتية للهواتف المحمولة كي يتسنى تنفيذ هذه الاستراتيجية [21].

سادسا: الذكاء الاصطناعي و تقنية "بلوك تشين" Block-Chain

يُنظر إلى تقنية "بلوك تشين" وتقنيات السجلات المُوزَّعَة[8] اللامركزية، بوصفها آلية لتقديم مستوى أعلى من الحماية والارتقاء بأمن البيانات، وذلك من خلال استخدام خصائص الحصانة وقابلية التدقيق والتشفير التي تتمتع بها، مع ضمان الشفافية بين الأشخاص الذين لا يعرفون بعضهم بعضاً. وصحيح أن تقنية "بلوك تشين" تضرب بجذورها في تطبيقات العملات المُشفرة، وما زالت تتطور لخدمة هذا الغرض تحديداً في القطاع المالي، إلا أن العديد من المؤسسات بدأت تلمس حالات الاستخدام غير التشفيري لتسجيل البيانات التي يستحيل تغييرها أو عكسها أو العمل بها كتعاقدات ذكية)كوسيلة لدمغ المعاملات بتوقيت محدد بين الأطراف(. وقد اضطلع العديد من قطاعات الصناعة، بخلاف القطاع المالي، باستخدام هذه التقنيات الموزعة والخصائص المفيدة لسلسلة الكتل) بلوك تشين(، بدايةً من الرعاية الصحية وقطاع المستحضرات الدوائية وقطاع العقارات وتجارة التجزئة وسلسلة الإمداد والقطاع القانوني وقطاع النشر[22]. ولدى المؤسسات خيارات مرنة لتشغيل تقنية "بلوك تشين" بلا تصريح)أي شخص يستطيع الانضمام(أو بموجب إذن)حيث ينضم الذين تقتضي الحاجة دعوته فقط(أو الخيار الهجين)نوع يختص باتحادات الشركات(، والاختيار ما بين إذا ما كان ينبغي الحفاظ على البيانات داخل تقنية "بلوك تشين" أم خارجها. وفي ظل اقتحام ا لصناعات الثورة الصناعية الرابعة، تحتل "بلوك تشين" بوصفها تقنية تكميلية مكانتها، وهناك صناعات مناسبة جداً للفائدة الكبيرة التي يمكن أن تحققها تلك التقنية [23].

سابعا: الذكاء الاصطناعي وحماية الخصوصية User Privacy Protection

أدت الزيادة المهولة في استخدام البيانات والتطور السريع للتقنيات الجديدة، كالسحابة الإلكترونية وإنترنت الأشياء، إلى حدوث زيادة مطردة في الهجمات السيبرانية على شبكة الإنترنت. وقد شهدت خدمات إخفاء الهوية وخدمات الخصوصية معدل نمو

استثنائي منذ استحداث تقنية "بلوك تشين" وشبكة "تور" حيث طالب عدد أكبر من الأشخاص بخدمات إخفاء الهوية مبتعدين

عن العروض المركزية التقليدية، حيث تساعد تقنية "بلوك تشين" في الحفاظ على البيانات المخزنة والحيلولة دون التلاعب فيها، وتتيح تبادلاً آمناً للمواد القيمّة كالأموال أو الأسهم أو حقوق الوصول إلى البيانات. وخلافاً لأنظمة التجارة التقليدية، لا حاجة لوسيط أو نظام تسجيل مركزي لمتابعة حركة التبادل، بل تقوم كل الجهات بالتعامل مباشرة بعضها مع بعض [25,24].

ثامنا: الذكاء الاصطناعي وتهديدات تضليل المعلومات Misinformation and Disinformation

أن ترويج المعلومات الخاطئة أو المضللة عبر الفضاء السيبراني ه ي نش ر لمحتويات قد تكون خاطئة عن غير قصد أو بقصد والتي يتم تقاسمها مقابل المعلومات التي تعتمد على التضليل والتي تكون أساسا كاذبة أو ملفقة لذا فأن التمييز بين المعلومات الخاطئة والمضللة مهم جد ا الرغم من صعوبة الفصل ما بين كلا المصطلحى ن .ويلع ب الذكاء الاصطناعي لعب دورا محوريا في تسهيل نشر المعلومات المضللة والأخبا ر الزائف ة عبر وسائط الاعلام وشبكا ت التواصل الاجتماعي بتقنيا ت التزييف العميق التي تستخدم لمونتاج محتوى صوتي او صوري بشكل كامل ليستعرض شيئاً لم يكن موجوًدًا فيه بالأصل. كما تستخدم في الع بث بوجوه النجوم والمشاهير ورجال الاعمال والسياس ة وإدخال وجوههم في فيديوهات لا علاقة لهم فيه ا وتعتبر هذه التقنية من

الأساليب السهلة والمتاح ة للعديد من الجهات والافرا د للتعديل على الفيديوهات أو تركيبها بالكامل، مما يجعلها خطيرة وتفتح باب لإساءة سمعة الأخرين أو الترويج لأجندة معينة

الاستنتاجات

تزداد شهرة عملية جمع البيانات المُخزَّنَة واستغلالها حتى أصبحت مكوناً أساسياً من مكونات البنية التحتية للبنايات الذكية. ويمكن تخزين البيانات المرصودة مثلاً داخل بنية أساسية لخدمة سحابية خاصة أو عامة أو هجينة أو خدمة مُوزّعَة باستغلال منصات البيانات. ويمكن استخدام البيانات المُخزّنَة عند تنفيذ الخدمات، كأتمتة المباني. ومن الممكن أن تواجه الخدمات السحابية ومستشعرات إنترنت الأشياء ومنصات البيانات الخاصة بالمباني الذكية العديد من أنواع الهجوم السيبراني كهجمات الخصوم والهجمات المعتمدة على الذكاء الاصطناعي وهجمات الحرمان من الخدمات والهجمات الداخلية.

التوصيات والمقترحات:

ختاماً توصلنا الى أن الاعتماد على أنظمة الذكاء الاصطناعي المتكاملة مع الحاسب الآلي وامكاناته يتيح الكثير من الفرص الناجحة والفعالة للقائمين والعاملين بمختلف قطاعات الدولة بما فيها وأهمها المؤسسات الأمنية للتوصل الى حلول ذكية تلقائية وقرارات حاسمة صائبة التي تواجه وتحد من مخاطر وتهديدات الامن السيبراني وتوفر الحماية الرقمية للأفراد والمؤسسات كما تساعد أجهزة فرض القانون ف ي السيطرة على البيئة الرقمية الافتراضية بالتحليل السريع لكل موقف مخالف لأمن وسلامة هذه البيئة. وذلك بدعم جملة من التوجهات في التوصيات أدناه:

أولا: تسخير الذكاء الاصطناعي لتعزيز القدرات البشرية في مواجهة الازمات

وهي احدى أهم الجوانب الانسانية في استخدام الذكاء الاصطناعي حيث سيتم الاعتماد عليها بشكل متزايد مستقبلا لتمكين الموارد البشرية من دمج إمكاناتهم البشرية بتقنيات الذكاء الاصطناعي لإ يجاد حلول مناسبة للتحديات و الازمات الاجتماعية، و ذلك سيساهم في تحقيق عوائد ايجابية كبيرة فيما يتعلق بالقضايا المجتمعية والتي تتضمن من بينها تمكين و حماية المراءة في المجتمع ،مساعدة المجتمعات على التعافي من الكوارث الطبيعية، وتلبية احتياجات الأطفال في العالم من أدوات و برامج تعليمية و العاب فكرية و منصات تواصل تعليمية، فضلا عن تطبيق قوانين حقوق الإنسان. مثل مشروع شركة مايكروسوفت التي أطلقته لمدة خمس سنوات بقيمة 40 مليون دولار، ويسمى بالذكاء الاصطناعي لخدمة العمل الإنساني AI for Humanity .

ثانيا: بناء بنية تحتية سيبرانية مؤمنة

ضرورة التغيير الجذري في الاستراتيجيات الحكومية المتبعة لكشف ومتابعة ومنع الهجمات و التهديدات السيبرانية الى جانب الجرائم الالكترونية والتعامل معها بأنظمة ذكية خبيرة التي تستبدل الاعتماد على مجموعات جامدة من البيانات بنماذج و أنماط ذكاء اصطناعي مرنة. لتكون قادرة على فهم السلوك غير الطبيعي للمجرمين التي تزايدت مع استخدام الأجهزة المحمولة في مواقع العمل وتحويل عمل الشركات الى البيئة الرقمية الافتراضية وتوفير البيانات الضخمة Big data في الحوسبة السحابية Cloud computing مع دعم وتعزيز وسائل الحماية من الاختراق الرقمي. إعادة تصميم الأنظمة الأمنية بحيث لا تعتمد الطرق التقليدية للمصادقة وتوزيع صلاحيات الوصول والاستخدام مثل كلماتالمرور وانما تلجا الى تقنيات الذكاء الاصطناعي كتقنيات التشفير Encryption و الكابشتا Captcha أو تقنيات بصمة العين ،مسحات الوجه ،بصمات الأصابع و الابهام للتحقق من الهويات والسلوكيات الرقمية مشيرة .

ثالثا: الرقابة الرقمية

ضرورة البدء في استخدام تقنيات الذكاء الاصطناعي لتحسين كفاءة الخدمات والبرامج الحكومية مع الاسراع في خلق برامج تدريبية لبناء أنظمة ذكية تعنى بإدارة المؤسسات الصناعية واستثمار اليات التعاون الدولي المشترك في مجال الذكاء الاصطناعي لتطوير هذه الأنظمة مع الإبقاء على أمكانية ايقافها بمجرد ظهور بوادر خطورتها على تلك الخدمات. وبذلك تفرض رقابة رقمية حكومية لوجستية مشددة على المختبرات والمصانع التي تعنى بتطوير أنظمة الذكاء الصناعي وعدم اهمال الدور البشري في اتخاذ القرارات وإدراج التعليمات.

المصادر:

[1] Kolata ،G. ,"How can computers get common sense?", Science (217), 1982, pp. 1237–1238.

[2] Kris-bondi, "The House That Learns: How AI Makes Smart Homes Smarter"

security", Defense & Security Analysis, 35(2), 2019, pp. 147-169.

[11] Yamin, M. M., Ullah, M., Ullah, H., & Katt, B., "Weaponized AI for Cyber-attacks", Journal of Information Security and Applications, 57, 2021, pp. 102-722.

[12] Johnson, J., "The AI-cyber nexus: implications for military escalation, deterrence and strategic stability", Journal of Cyber Policy, 4(3), 2021, pp. 442-460.

[13] Sayler, K. M., & Harris, L. A. "Deep fakes and national security", Congressional Research SVC Washington United States, 2020.

[14] Pantserev, K. A. "The malicious use of AI-based deepfake technology as the new threat to psychological security and political stability", Cyber defense in the age of AI, smart societies and augmented humanity, 2020, pp. 37-55.

[15] Lu, Z. X., Qian, P., Bi, D., Ye, Z. W., He, X., Zhao, Y. H., ... & Zhu, Z. L. "Application of AI and IoT in clinical medicine: summary and challenges", *Current Medical Science*, *41*, 2021, pp.1134-1150.

[16] Merenda, M., Porcaro, C., & Iero, D., "Edge Machine Learning for AI-enabled IoT devices: A review", Sensors, 20(9), 2020, pp. 2533.

[17] Alsharif, M. H., Kelechi, A. H., Albreem, M. A., Chaudhry, S. A., Zia, M. S., & Kim, S., " Sixth generation (6G) wireless networks: Vision, research activities, challenges and potential solutions", Symmetry, 12(4), 2020, pp. 676.

[18] Kibria, M. G., Nguyen, K., Villardi, G. P., Zhao, O., Ishizu, K., & Kojima, F. , "Big data analytics, machine learning, and artificial intelligence in next-generation wireless ،www.huffingtonpost.co.uk, Retrieved in 27-4-2018.

[3] David H., "Why Are There Still So Many Jobs? The History and Future of Workplace Automation," The Journal of Economic Perspectives, Vol. 29, No. 3, 2015, pp. 3–30.

[4] Chang, Jae Hee, Gary Rynhart, and Phu Huynh, "ASEAN in Transformation: How Technology is Changing Jobs and Enterprises", Working Paper No. 10, Switzerland: Bureau for Employers' Activities, International Labour Office, 2016.

[5] Li, J. H., "Cyber security meets artificial intelligence: a survey", Frontiers of Information Technology & Electronic Engineering, 19(12), 2018, pp. 1462-1474.

[6] Dash, B., Ansari, M. F., Sharma, P., & Ali, A. "Threats and Opportunities with AI-based Cyber Security Intrusion Detection: A Review", International Journal of Software Engineering & Applications (IJSEA), 2022, 13(5).

[7] Sedjelmaci, H., Guenab, F., Senouci, S. M., Moustafa, H., Liu, J., & Han, S. "Cyber security based on artificial intelligence for cyber-physical systems,"IEEE Network, 34(3), 2020, pp. 6-7.

[8] Das, R., & Sandhane, R., "Artificial intelligence in cyber security", In Journal of Physics: Conference Series", 1964 (4), 2021, pp. 42-72, IOP Publishing.

[9] Zarina I, K., Ildar R, B., & Elina L, S., "Artificial Intelligence and Problems of Ensuring Cyber Security", International Journal of Cyber Criminology, 13(2), 2019.

[10] Johnson, J. "Artificial intelligence & future warfare: implications for international

networks", IEEE access, 6, 2018, pp. 32328-32338.

[19] Shen, X., Gao, J., Wu, W., Lyu, K., Li, M., Zhuang, W., ... & Rao, J. , " AI-assisted networkslicing based next-generation wireless networks", IEEE Open Journal of Vehicular Technology, 1, 2020, pp. 45-66.

[20] Phansalkar, S., Kamat, P., Ahirrao, S., & Pawar, A., "Decentralizing AI applications with block chain", International Journal of Scientific & Technology Research, 8(9), 2019, pp. 9.

[21] Shetty, A., Shetty, A. D., Pai, R. Y., Rao, R. R., Bhandary, R., Shetty, J., ... & Dsouza, K. J., "Block chain application in insurance services: A systematic review of the evidence", SAGE Open, 12(1), 2022, pp. 2158-2440.

[22] Gulmezoglu, B., Zankl, A., Tol, M. C., Islam, S., Eisenbarth, T., & Sunar, B., "Undermining user privacy on mobile devices using AI", In Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security, (2019, July), pp. 214-227.

[23] Gupta, R., Tanwar, S., Al-Turjman, F., Italiya, P., Nauman, A., & Kim, S. W., "Smart contract privacy protection using AI in cyber-physical systems: tools, techniques and challenges", IEEE access, 8, 2020, pp. 24746-24772.

[24] Agarwal, V., Sultana, H. P., Malhotra, S., & Sarkar, A., "Analysis of classifiers for fake news detection", Procedia Computer Science, 165, 2020, pp. 377-383.

[25] Demartini, G., Mizzaro, S., & Spina, D., "Human-in-the-loop Artificial Intelligence for Fighting Online Misinformation: Challenges and Opportunities", IEEE Data Eng. Bull., 43(3), 2020, pp. 65-74.