مجلة التربية للعلوم الانسانية

مجلة علمية فصلية محكّمة، تصدر عن كلية التربية للعلوم الإنسانية / جامعة الموصل

الذكاء الاصطناعي والفضاء السيبراني: بين تعزيز الأمن وتهديده

غصون احمد عراك [1] عامر هاشم عواد [2]

كلية العلوم السياسية / جامعة النهرين [1، 2]

معلومات الارشفة

تاريخ القبول : 2025/11/27

تاريخ النشر : 2026/6/19

الكلمات المفتاحية :

الذكاء الاصطناعي، الفضاء السيبراني، الإرهاب السيبراني، الامن السيبراني

معلومات الاتصال

غصون احمد

الملخص

أصبحت تقنيات الذكاء الاصطناعي أحد الركائز الأساسية في الفضاء السيبراني، بما تحمله من قدرات تكون سلاح ذا حدين، يمكن ان تُستغل من قبل الفاعلين وعلى رأسهم الجماعات الإرهابية لنشر التطرف، وتنفيذ هجمات حجب الخدمة، والتلاعب بالمحتوى الإعلامي، اذ يكون من الصعب اكتشافها، كما يمكن ان يكون الذكاء الاصطناعي أداة فعالة في مكافحة الإرهاب السيبراني، من خلال تقنيات مثل التعرف على الوجه، والبلوك تشين، وإنترنت الأشياء، الأمر الذي يشكل تحدياً كبيراً للأمن السيبراني يتطلب تطوير آليات الرقابة والضوابط القانونية والأخلاقية، لضمان تعزيز الأمن السيبراني، إضافة الى التعاون الدولي لتطوير سياسات قادرة على مواجهة التهديدات المدعومة بالذكاء الاصطناعي

DOI: **********,,

Journal of Education for Humanities

A peer-reviewed quarterly scientific journal issued by College of Education for Humanities / University of Mosul

Artificial Intelligence and Cyberspace: Between Enhancing Security and Threatening It

Ghosoon Ahmed Arrak [1] Amer Hashim Awwad [2]
College of Political Science / Al-Nahrain University[1,2]

Article information

Accepted : 27/11/2025
Published 19/6/2026

Keywords:
Artificial Intelligence, Cyberspace, Cyber Terrorism, Cybersecurity

Correspondence:
Ghosoon Ahmed Arrak

Abstract

Artificial intelligence technologies have become a fundamental pillar in cyberspace, acting as a double-edged sword. They can be exploited by actors-particularly terrorist groups-to spread extremism, carry out denial-of-service attacks, and manipulate media content in ways that are difficult to detect, conversely, artificial intelligence can serve as an effective tool in combating cyber terrorism through technologies such as facial recognition, blockchain, and the Internet of things. This duality presents a significant challenge to cybersecurity, necessitating, as well as legal and ethical frameworks, to ensure the enhancement of cybersecurity, Furthermore, international cooperation is essential to develop policies capable of addressing Al-enabled threats

DOI: **********,,

المقدمة

في عالم يتسم بالتغير السريع، دخلت البشرية عصراً جديداً من التكنولوجيا جمعت بين تسريع الأتمتة، واختصار الوقت في الابتكارات الحديثة، والتقارب في الوجودين الفعلي والرقمي فنتج عنها ما يعرف بالذكاء الاصطناعي ويمثل احد فروع علم الحاسوب وأحد أعمدة التطور التكنولوجي، الذي سيكون محرك التقدم والنمو والازدهار وهو يشكل طفرة تطورية غير مسبوقة تمكن الآلات من محاكاة طريقة التفكير البشري الا انها تكون أكثر تركيزاً ولا تتعرض للإجهاد الذي يصيب الانسان، وهي تقوم بأداء مهام كان الانسان هو الوحيد القادر على أدائها، ويتم استخدام هذه التقنيات الذكية في العديد من المجالات ، ولاسيما مجال الأمن السيبراني، مما خلق فضاءً سيبرانياً معقداً، اذ ان هذه التقنيات الذكية تشكل أثاراً مزدوجة في الفضاء السيبراني بين فرص هائلة لتعزيز الأمن السيبراني وبين مخاطر تهدد البنى التحتية وأنظمة الشبكات للدول والمؤسسات.

اولا: اهمية البحث والهدف منه

تتأتى اهمية البحث والهدف منه من ان الذكاء الاصطناعي يوفر تقنيات متقدمة لرصد التهديدات السيبرانية وتحليل الأنماط الخبيثة، وتعزيز الدفاع السيبراني للدول فيمكن تحسين البحث عن نقاط الضعف وأنظمة المراقبة باستخدام الأتمتة الذكية. كما انه سيُمكن من إضافة نماذج جديدة للدفاع السيبراني تقوم بمراقبة السلوك الشاذ لاكتشاف التهديدات غير المعروفة والاستجابة لها، ومن ناحية أخرى أصبحت هذه التقنيات أداة خطرة بيد الفاعلين الخطرين مثل الجماعات الإرهابية في تطوير هجمات سيبرانية يكون من الصعب اكتشافها باستخدام الطرق التقليدية، الامر الذي شكل تحدياً كبيراً للأمن السيبراني يتطلب من الدول تحديد آليات الرقابة والضوابط القانونية والأخلاقية لضمان استخدام هذه التقنيات من أجل تعزيز الأمن السيبراني بدلاً من تقويضه، كما يتطلب التعاون الدولي لتطوير سياسات إقليمية ودولية قادرة على مواجهة التهديدات السيبرانية الجديدة المدعومة بتقنيات الذكاء الاصطناعي.

ثانيا: اشكالية البحث

يذهب البحث لمعالجة اشكالية نابعة من الجملة التساؤلية الاتية: تجاوز تأثير الذكاء الاصطناعي في الفضاء السيبراني موضوع تعزيز الامن والحفاظ عليه، بل أصبح الفضاء السيبراني بيئة للصراع التكنولوجي بين الفاعلين من الدول وغير الدول، واخذ الذكاء الاصطناعي يحجز مساحة كبيرة فيه ايجاباً وسلباً.

ثالثا: فرضية البحث

يعمد البحث لأثبات فرضية قوامها (كلما توسع دور الذكاء الاصطناعي في الفضاء السيبراني كلما أثر ذلك في موضوع الامن العالمي تعزيزاً او تهديداً).

رابعا: منهج البحث

يعتمد البحث على تبني المنهج الوصفي التحليلي.

خامساً: هيكلية البحث:

ستوزع فقرات البحث على مبحثين، يتناول الاول اطارا نظرياً ومفاهيمياً للموضوعي الذكاء الاصطناعي والفضاء السيبراني وسينقسم على مطلبين. والثاني يتناول تأثير الذكاء الاصطناعي في الامن السيبراني عبر مطلبين ايضا.

المبحث الأول: إطار نظري ومفاهيمي

أصبح الذكاء الاصطناعي واحداً من المصطلحات التي تتردد على مسامعنا كثيراً خلال العقد الأخير من القرن الحالي، فمع التطور التكنولوجي الكبير الذي نشهده ودخول الحاسوب في كافة المجالات اصبح الذكاء الاصطناعي جزءاً مهماً منها، مع توقعات بتسارع هذا التطور في مفاصل الحياة المختلفة، وتعد دراسة الذكاء الاصطناعي اطاراً له أهمية كبيرة في البيئة الدولية في القرن الحادي والعشرين وذلك نتيجة التطورات العالمية والإقليمية، ويمثل الذكاء الاصطناعي محاكاة للذكاء البشري من خلال الآلات لاسيما أنظمة الحواسيب، ويشمل معالجة اللغة والتعرف على الكلام والصور، ويهدف الى جعل الحواسيب والآلات تكتسب صفة الذكاء، بمعنى ان تكون قادرة على القيام بأشياء كانت حكراً على الأنسان مثل التعلم والابداع والتفكير.

اما الفضاء السيبراني فهو يمثل نتاج التطور التكنولوجي اذ شكل حجر الأساس لعصر المعلومات الذي وجد فضاء واسعاً لتدفق المعلومات، من خلال مجموعة من العناصر ساهمت في تشكيله، وهي الحواسيب، والأنظمة، والبرمجيات، ونقل وتخزين البيانات، والمعلومات، بالإضافة الى اهم عنصر وهو المستخدم للعناصر السابقة والمتمثل بالعنصر البشري، ان هذا الفضاء قد أعاد تشكيل مفاهيم الزمان والمكان وطبيعة الأشياء التي يتم تداولها من خلاله، لذا يتطلب من الدول التكيف مع التغيير السريع الذي يفرضه هذا الفضاء في مختلف المجالات وبضمنها المجال الأمني. وفي هذا الإطار سوف نتناول مفهوم الذكاء الاصطناعي وأنواعه والفضاء السيبراني وخصائصه.

المطلب الأول: مفهوم الذكاء الاصطناعي

اختلف الباحثون في إيجاد تعريف دقيق لمصطلح الذكاء الاصطناعي، اذ ان فهم الذكاء الاصطناعي يعود الى فهم طبيعة الذكاء الإنساني من خلال عمل برامج للحاسب الآلي قادرة على محاكاة السلوك الإنساني،

بمعنى انه يعمل بنفس طريقة عمل الدماغ البشري، ويقوم باتخاذ القرار في موقف معين بناء على الوصف لهذا الموقف[1].

ونظراً لاختلاف وجهات نظر الباحثين في تعريف مفهوم الذكاء الاصطناعي سوف نقوم بتعريفه لغة واصطلاحاً.

اولا: الذكاء الاصطناعي في اللغة:

يتكون مصطلح الذكاء الاصطناعي من كلمتين (الذكاء والاصطناعي) ولكي نتمكن من التعرف على معناه اللغوي يتطلب ان نعرف كل مصطلح على حدة وكالتالي:

أ- الذكاء Intelligence: هو اسم يعود أصله الى جذور مادة (ذكو) فيقال "ذكا يذكو ذكاء، وذكو ذكت النار تذكو ذكواً وذكاً واستذكت أي تصاعد لهبها واشتعلت، والذكاء هو سرعة الفطنة[2]".

ب- اصطناعي Artificial: ترتبط الكلمة بالفعل "يصنع" او "يصطنع" وتطلق على جميع الأشياء التي تنشأ نتيجة النشاط او الفعل الذي يتم عن طريق اصطناع وتشكيل الأشياء تمييزاً عن الأشياء الموجودة بصورة طبيعية دون تدخل الانسان[3].

ثانيا: الذكاء الاصطناعي اصطلاحاً:

يعرف الذكاء الاصطناعي على انه " المسار العلمي والتقني الذي يشمل الطرق والتقنيات والنظريات التي تهدف الى تطوير آلات لها القدرة على محاكاة الذكاء البشري[4]".

كان جون مكارثي (John McCarthy) وهو أحد رواد منظمة العفو الدولية، اول من حدد مصطلح الذكاء الاصطناعي، وعرفه بانه "تطوير آلات تتصرف وكأنها ذكية[5]".

---

[1] -الان بونيه، الذكاء الاصطناعي واقعه ومستقبله، ترجمة علي صبري فرغلي، سلسلة علم المعرفة، المجلس الوطني للثقافة والفنون والآداب، الكويت، 1993، العدد172، ص11.

[2] -ابي الفضل جمال الدين محمد بن مكرم ابن منظور الافريقي المصري، ط4، لسان العرب، دار صادر للطباعة والنشر، بيروت، المجلد6، 2005، ص37.

[3] -احمد عبد المجيد عبد العزيز منصور، الذكاء الاصطناعي والامن القومي، دار التعليم الجامعي، الإسكندرية، 2024، ص15.

[4] -Chun-wei yang and others, application of intelligence in intelligent manufacturing, the second academy of China aerospace science and technology Corporation, Beijing, China, 2017, p87.

[5] -عبد الله موسى، احمد حبيب بلال، الذكاء الاصطناعي ثورة في تقنيات العصر، ط1، المجموعة العربية للتدريب والنشر، القاهرة، 2019، ص20.

اما مارفن منسكي (Marvin Minsky) فقد عرف الذكاء الاصطناعي انه "عملية بناء برامج حاسوب آلي تقوم بإنجاز المهام التي يتم إنجازها من قبل البشر، أي هو علم يجعل الآلات تكون قادرة على انجاز أشياء تتطلب الذكاء أذا قام بها البشر[1]".

وفقاً لتعريف أكسفورد فان الذكاء هو " القدرة على التعلم والفهم والتفكير وهناك مجموعة من القدرات يمكن ان نعتبرها مؤشرات للذكاء وهي الفهم او التعلم من التجارب واستخلاص المعنى من الأمور التي تحتمل معنيين[2]".

ثالثا: أنواع الذكاء الاصطناعي:

هناك عدة أنواع او تصنيفات للذكاء الاصطناعي والتي تنوعت مع كل مرحلة من مراحل تطوره، وتقسم هذه الأنواع الى ما يلي:

1-الذكاء الاصطناعي الضيق Narrow AI

هذا النوع من الذكاء الاصطناعي يتمثل في العمليات الحسابية التي تؤديها الآلات الحاسبة، ونوعية الذكاء المحدود الذي تعتمد عليه هذه الحواسيب الآلية والذي يعتمد بالأساس على عمليات البرمجة، وتكون لها القدرة على تكرار مهام محددة تفوق قدرات العقل البشري، الا انها لم تصل بعد لمستوى العقل البشري من حيث التعقيد في التفكير، وليس لديها وعي وادراك مماثل للعقل البشري، ومن امثلة هذه النظم برامج المساعدة الآلية مثل سيريSiri واليكساAlexa وكورتاناCortana تتمكن هذه البرامج من خلال الخوارزميات من جمع المدخلات للخروج بمخرجات جديدة مبنية على تفضيلات المستخدمين، ويمكنها التفاعل مع البشر لكن بشكل محدود كونها لا تماثل العقل البشري ولا تمتلك الوعي والخبرات والبشرية[3].

2-الذكاء الاصطناعي العام General AI

في هذا النوع من الذكاء الاصطناعي يكون بمقدور هذه الأنظمة ان تتعلم كل شيء بدون برمجة، ويمكنها محاكاة العقل البشري بشكل كامل مع ما يعنيه ذلك من مراحل للإدراك والاحساس، ولا تتوفر هذه الأنظمة في الوقت الحالي نظراً لكونها تحتاج الى المزيد من تطوير الذكاء الاصطناعي وتجريبها على نطاق واسع، وهو يتعلق بمحاولة تطوير عقول رقمية تتسم بالقدرة على الإدراك والإحساس بناءً على الخبرات البشرية المتراكمة،

---

[1] - Wayne E. Baker and others, Artificial Intelligence, United States Army Sergeants Major Academy, 2007, p4.

[2]- السعيد عبد الحميد إبراهيم، مخاطر تطورات تقنيات الذكاء الاصطناعي، ط1، دار العلم والايمان للنشر والتوزيع، مصر 2024، ص17.

[3]- احمد عبد المجيد عبد العزيز منصور، مصدر سبق ذكره، ص44.

دون ان يحتاج المرور بكم التجارب التي يعيشها الانسان خلال عمره كاملاً، اذ يمكن لهذه التطبيقات المرور بهذه الخبرات من خلال عدد محدود من الأيام فقط، وهو بذلك يضاهي ويتفوق على البشر في جميع القدرات الفكرية والذهنية ويفهم جميع الاختصاصات البشرية العلمية والأدبية والفنية والابداعية...الخ[1].

1- الذكاء الاصطناعي الخارق Super AI

في هذا المستوى من الذكاء الاصطناعي يكون بمقدور الحواسيب الآلية ان تفكر مثل البشر، حتى انها ستتفوق على البشر نتيجة تفوق قدرات الكفاءة للحواسيب الآلية، ومع تطور علم الروبوتات سوف يتفوق على القدرات المحدودة للأجسام البشرية، ويكون ممكناً الوصول الى الذكاء الاصطناعي الخارق فقط عندما يستطيع العالم ان يطور أنظمة الذكاء الاصطناعي، وهذه المرحلة من الذكاء الاصطناعي تثير العديد من المخاوف حول مخاطر تلك الأنظمة على البشر، وهنا يمكن التمييز بين نمطين أساسيين، الأول: يسعى الى فهم الأفكار البشرية، والانفعالات التي تؤثر على سلوك البشر، وتكون قدرته على التفاعل الاجتماعي محدودة، اما الثاني فهو يمثل نموذج لنظرية العقل اذ تستطيع ان تعبر عن حالتها الداخلية وتتنبأ بمشاعر الاخرين وتتفاعل معها فهي تمثل الجيل القادم من الآلات فائقة الذكاء[2].

المطلب الثاني: مفهوم الفضاء السيبراني

يعد الفضاء السيبراني من نتاج التطور التكنولوجي الذي شهده عصر المعلومات، وهو يتكون من البنى التحتية لتكنولوجيا المعلومات بما في ذلك الانترنت وشبكات الاتصال، وأنظمة الحاسوب، والمعالجات، ووحدات التحكم المدمجة[3].

ولقد تعرض مفهوم الفضاء السيبراني لجدل واسع كشف عن تقاطع في الرؤى والخلفيات الايديلوجية والمعرفية، نتيجة التطورات التي مر بها هذا المفهوم حتى اتسع ليتداخل في نطاقه، مع مفاهيم مقاربة ولهذا توجب الوقوف على تعريف مفهوم الفضاء السيبراني لغوياً واصطلاحاً.

اولا: مفهوم الفضاء السيبراني في اللغة

ان مصدر كلمة سايبر يعود أصلها الى الكلمة الاغريقيةCybernetics، وتعني الموجه او الحاكم، بينما في قاموس المعاني نجد ان كلمة Cybernetics بالإنكليزية تعني: انها علم التحكم الاوتوماتيكي او التحكم

[1]- المصدر السابق نفسه، ص45-46.

[2]- إيهاب خليفة، الذكاء الاصطناعي: تأثيرات تزايد دور التقنيات الذكية في الحياة اليومية للبشر، مجلة اتجاهات الاحداث، الامارات، العدد20، 2017، ص63.

[3]- اسراء شريف جيجان، صفا عباس فاضل، تأثير الفضاء السيبراني على الحروب الحديثة، مجلة دراسات تربوية، مركز البحوث والدراسات التربوية، العراق، العدد65، 2024، ص11-12.

الآلي، الا انها تمثل البنية الافتراضية التي يتم فيها الاتصال عبر شبكات الحاسوب[1]. وتعد كلمة سايبر (Cyber) كلمة إنكليزية بمعنى (إلكتروني) وتخيلي أي من الخيال، او افتراضي ويتم تعريفه بإنه التحكم او ضبط الأشياء عن بعد[2].

ثانيا: مفهوم الفضاء السيبراني اصطلاحاً

يعرف الفضاء السيبراني (Cyber Space): انه الحيز او المجال الرقمي الممتد من خلال خطوط الاتصالات المعدنية والضوئية والهوائية وقنواتها في شبكة الانترنت، وهو بهذا يعني طريق المعلومات الفائقة السرعة بتعبيره التكنولوجي[3]".

ان اول من استعمل مصطلح الفضاء السيبراني هو كاتب الخيال العلمي ويليام جيبسون (Wiliam Gibson) عام 1984، وقصد به شبكات الكمبيوتر والاتصالات الالكترونية، وهي عبارة عن شبكات خيالية تحتوي على كميات هائلة من المعلومات التي يتم الحصول عليها لتحقيق السلطة والثروة[4].

لقد عرفه جوزيف ناي (Joseph Nye) انه "مجال تشغيلي يعتمد على استعمال المعلومات عبر الأنظمة المترابطة والبنية التحتية المتصلة بها، ويصوره على انه نظام يتكون من طبقة مادية وأخرى افتراضية، الطبقة المادية تشمل الأنظمة والبنية التحتية المادية (الحواسيب، الأجهزة، كابيلات، وغيرها)، اما الطبقة الافتراضية فتشمل ساحة الانترنت والبرمجيات والمعلومات والأرقام، يستعمل هذه المجال في شن الهجمات والتجسس والاختراق ضد البنية المادية، التي تشمل الأجهزة المتصلة بشبكة الانترنت والشبكات الخلوية الداخلية[5]".

[1]– مثنى مشعان المزروعي، ضياء مدلول فرج، "الفضاء الالكتروني ودوره في رسم خريطة جديدة للشرق الأوسط"، مجلة ديالى للبحوث الإنسانية، جامعة ديالى، العدد 76، 2018، ص400–401.

[2]– سيف نصرت توفيق الهرمزي، "فواعل النظام الدولي الجديد في القرن الحادي والعشرين"، مجلة تكريت للعلوم السياسية، تكريت، العدد11، 2017، ص130.

[3]– عمار ياسر زهير البابلي، التحديات الأمنية المعاصرة للهجمات السيبرانية، مجلة الفكر الشرطي، القيادة العامة لشرطة الشارقة، مركز بحوث الشرطة، الامارات، المجلد30، العدد3، 2012، ص27.

[4]– صباح عبد الصبور عبد الحي، "استخدام القوة الالكترونية في التفاعلات الدولية: تنظيم القاعدة نموذجاً"، مجلة المعهد المصري، إسطنبول، العدد2، 2015، 183.

[5]– إيهاب خليفة، القوة الالكترونية: كيف يمكن ان تدير الدول شؤونها في عصر الانترنت "الولايات المتحدة الامريكية نموذجا"، ط1، العربي للنشر والتوزيع، القاهرة، 2017، ص56.

عرف المعهد الوطني للمعايير والتقنية (NIST) الفضاء السيبراني بانه "مجال علمي داخل البيئة المعلوماتية يتكون من شبكة مستقلة من البنى التحتية لأنظمة المعلومات ويتضمن ذلك شبكات الانترنت وشبكات الاتصالات وأنظمة الحاسب الآلي والمعالجات وأجهزة التحكم المدمجة[1]"

ثالثا: خصائص الفضاء السيبراني

هناك العديد من الخصائص والمميزات التي يتمتع بها الفضاء السيبراني، والتي تحسن من عملية التواصل وتبادل المعلومات داخل شبكة الانترنت، ويمكن التعرف على هذه الخصائص كالاتي[2]:

1. سهولة التعرف على هوية المستخدم: للفضاء السيبراني العديد من الخيارات فيما يتعلق بالتعريف عن المستخدم، اذ بالإمكان التعرف على هوية المستخدم بأفضل الطرق، كما يمكن إخفاء الهوية، بالإضافة الى إمكانية انشاء هوية وهمية مزيفة.
2. التواصل للجميع: الفضاء السيبراني يتيح فرص التواصل بجميع الخدمات لجميع المستخدمين، دون تمييز مستخدم عن غيره.
3. التواصل في كل مكان وزمان: الفضاء السيبراني يسمح لجميع المستخدمين التواصل في أي مكان واي وقت، وبالرغم من المسافات البعيدة بين المستخدمين الا انه يمكن التواصل مع بعضهم في مختلف البلدان وعلى مساحات جغرافية واسعة.
4. تسهيل التفاعل: بإمكان الفضاء السيبراني ان يوفر استمرارية التواصل طوال الوقت، سواء مع شخص او مجموعة اشخاص عبر أجهزة الحاسوب دون انقطاع، كما يوفر للمستخدم اخذ الوقت الكافي للإجابة، اذ ليس هناك وقت محدد للرد على أي استفسار او سؤال.
5. خاصية مركزية: يمكن للمؤسسات العامة والخاصة، والمؤسسات العسكرية والأمنية التواصل مع مجموعة واسعة من الأطراف التابعة لها، من خلال مساحات جغرافية واسعة للوصول للمعلومات الصحيحة والضرورية لاتخاذ القرارات الصائبة، مما يوفر الكثير من الوقت والجهد وتقليل هامش الخطأ.

المبحث الثاني: تأثير الذكاء الاصطناعي في الأمن السيبراني

اعتمدت الدول على العنصر البشري في تحقيق الأمن السيبراني، من خلال جمع المعلومات وتشديد الرقابة، وملاحقة التهديدات، والاستجابة لأي حوادث سيبرانية، الا انه مع التطور التكنولوجي السريع ظهر ما يسمى الذكاء الاصطناعي كتقنية جديدة غزت كافة المجالات، اذ ازدادت أهمية الفضاء السيبراني مع ظهور هذه التقنية باعتبارها الأساس الذي يقوم عليه هذا البعد، وبالرغم من الفوائد الكبيرة لهذه التقنية في الفضاء

[1]– خالد ممدوح إبراهيم، التهديدات السيبرانية وحماية البيانات، ط1، دار الفكر الجامعي، الإسكندرية، 2024، ص33.

[2]– شريفة الكلاع، الامن السيبراني واشكال التهديدات: تحديات عالمية، الفا للوثائق للنشر والتوزيع، عمان، 2023، ص30–31.

السيبراني فإنه يلعب دوراً مزدوجاً، فهو من جهة يتم استخدامه لحماية الأمن السيبراني، ومن جهة أخرى يشكل تهديداً للأمن السيبراني عند استخدامه من قبل المهاجمين، وسوف نتناول في هذا المبحث التأثير المزدوج للذكاء الاصطناعي في الأمن السيبراني، من خلال دراسة استخدامه من قبل المنظمات الإرهابية، بالإضافة الى الدور الذي تؤديه تقنيات الذكاء الاصطناعي في مكافحة الإرهاب السيبراني.

المطلب الأول: استخدام الذكاء الاصطناعي من قبل المنظمات الإرهابية

لقد أصبحت تحديات الأمن السيبراني أكثر تعقيداً بسبب النمو السريع للتقدم التكنولوجي وزيادة الرقمنة في مختلف المجالات مما يجعل الأمن السيبراني اكثر صعوبة[1]، واحد هذه التطورات التكنولوجية هو الذكاء الاصطناعي والتعلم الآلي، وتعد الهجمات السيبرانية المعتمدة على الذكاء الاصطناعي أكثر تعقيداً وصعوبة، مما يجعلها تشكل تحدياً للأمن السيبراني، وتعتمد الهجمات التي تستخدم الذكاء الاصطناعي على أتمتة عملية الهجمات التي تتزايد بسرعات عالية، مما يعيق القدرة على التصدي لها والدفاع عن الموارد المستهدفة وبالتالي أتلافها[2].

من الاستخدامات السلبية للتقنيات الذكية هو استغلالها من قبل المنظمات الإرهابية في نشاطاتها وذلك لصعوبة رصدها وانخفاض كلفتها، إضافة الى أثرها الضار على اقتصاديات الدول، وإمكانية نشر الخوف في المجتمعات في ظل الاعتماد على الأنظمة الحاسوبية سواء في القوات المسلحة كالأجهزة العسكرية ذاتية التشغيل او في المدن الذكية التي يرتبط كل شيء فيها بالأنترنت[3].

اذ تعتمد التنظيمات الإرهابية على الاتمتة (دمج الآلات) لإنشاء محتوى دعائي مخصص لجذب وتجنيد الافراد، كما يتيح الذكاء الاصطناعي تطوير برمجيات خبيثة يمكنها التكيف مع محاولات الكشف، بالإضافة الى تطوير أنظمة ذاتية التحكم لتنفيذ مهام إرهابية دون تدخل بشري مباشر، وتستخدم الجماعات الإرهابية التقنيات الذكية للحصول على معلومات من المصادر المفتوحة، مما يساعدها في تتبع الافراد المستهدفين ورصد تحركاتهم بدقة[4].

ان هناك عدة دوافع تدفع المنظمات الإرهابية لاستخدام تقنيات الذكاء الاصطناعي وهي:

---

[1]– خالد ممدوح إبراهيم، التنظيم القانوني للذكاء الاصطناعي، دار الفكر الجامعي، الاسكندرية، 2022، ص31–32.

[2] –خالد ممدوح إبراهيم، التهديدات السيبرانية وحماية البيانات، مصدر سبق ذكره، ص71.

[3]– إيهاب خليفة، الحرب السيبرانية الاستعداد لقيادة المعارك في الميدان الخامس، العربي للنشر والتوزيع، القاهرة، 2021، ص81.

[4]– الذكاء الاصطناعي وتوظيفه من قبل الجماعات الإرهابية.. خبير يكشف مخاطر جديدة، تاريخ النشر 16\مارس\2025، متاح على الرابط التالي: https://search.app/YsFHjW1amcXYrZ6SA تاريخ الدخول: 22\4\2025.

1. تستخدم المنظمات الإرهابية الذكاء الاصطناعي في التلاعب بالمحتوى الإعلامي من خلال تقنية التزييف العميق لأنشاء محتوى مزيف يبدو حقيقياً من خلال الجمع بين الصور ومقاطع الفيديو الموجودة على الصور والمقاطع الاصلية[1].
2. هجمات حجب الخدمة: تعتمد هذه الهجمات على ارسال الجماعات الإرهابية كميات كبيرة من البيانات او طلبات الاتصال، للمواقع المراد الهجوم عليها، مما يجعل هذه المواقع غير قابلة للدخول عليها من قبل المستخدمين العاديين، وهذا النوع من الهجمات هو الأشهر والأكثر استعمالاً بسبب أنه الأكثر سهولة، ولا يحتاج الى مجهود كبير[2]، اذ يستخدم المهاجمون أكثر من جهاز واحد، وفي الكثير من الأحيان الاف الأجهزة لتوجيه الطلبات الى النظام المستهدف، ومن الأمثلة على استخدام هذه التقنية انه بين آواخر عام 2016 وبداية عام2017 أطلق تنظيم داعش أول سلسلة ناجحة من هجمات حجب الخدمة، واستهدفت عبر الذكاء الاصطناعي قطاعات اقتصادية وعسكرية[3].
3. يمكن من خلال تطبيقات الذكاء الاصطناعي ان تتمكن الجماعات الإرهابية من تحديد الافراد الأكثر استعداداً للانخراط في التنظيمات الإرهابية عن طريق توجهاتهم وميولهم وتفضيلاتهم على مواقع التواصل الاجتماعي[4].
4. تطوير تكتيكات الإرهاب: اختلفت تكتيكات الجماعات الإرهابية وأصبح الإرهاب أكثر تعقيداً، وأصبحت التكنولوجيا تشكل اهم أدوات الإرهابيين، اذ أصبح الانترنت ووسائل التواصل الاجتماعي ومنصات التجارة الإلكترونية من أدوات التنظيمات الإرهابية لنشر التطرف، والتحريض على العنف، ولقد توسعت الترسانات الإرهابية بشكل كبير، وأدت التطورات التكنولوجية الى زيادة سرعة عملياتها ومدى وصولها وحجمها، وجعلها تقدم على تهديدات عالمية ليست فقط محلية[5].

---

[1]– إيهاب خليفة، فرص وتهديدات الذكاء الاصطناعي في السنوات العشر القادمة، تقرير المستقبل: مجلة اتجاهات الاحداث، أبو ظبي، الامارات، العدد27، 2018، ص14.

[2]– حمد الحوسني، الذكاء الاصطناعي والإرهاب.. الآليات وسبل المواجهة، تاريخ النشر 11\مارس\2024، متاح على الرابط التالي: https://search.app/eUcgqFZnZnRuQo3x9 تاريخ الدخول:23\4\2025.

[3] –ماهر فرغلي، ضرورة مجابهة الاستخدام الإرهابي للذكاء الاصطناعي، تاريخ النشر 22\يناير\2024، متاح على الرابط التالي: https://search.app/HZ5r7NUqPoB6H4FF9 تاريخ الدخول: 23\4\2025.

[4]–حسام رشيد هادي الربيعي، الذكاء الاصطناعي وأثره في النظام الدولي، رسالة ماجستير، (غير منشورة)، الجامعة المستنصرية، كلية العلوم السياسية، 2022، ص116.

[5]– اماني عصام محمد عبد الحميد، الحرب والإرهاب الالكتروني في ظل الذكاء الاصطناعي: التهديدات وآليات المواجهة، مجلة وادي النيل للدراسات والبحوث الإنسانية والاجتماعية والتربوية، جامعة القاهرة، كلية الآداب، القاهرة، المجلد 43، العدد43، 2024، ص449.

5. تستخدم الجماعات الإرهابية مواقع التواصل الاجتماعي بهدف التدريب، مثل موقع (اليوتيوب) اذ تستخدمه الجماعات المسلحة لتحميل فيديوهات لكيفية القيام بهجمات او استخدام الأسلحة مثل الكلاشينكوف، ولا يمكن حذف الفيديو الا بعد القيام بالإبلاغ من قبل المشاهدين، كما تستخدم (الفيسبوك) لنشر رسائلها، و(تويتر) لنشر الاخبار الترويجية للأفكار المتطرفة لسهولة استخدامه عبر الهواتف[1].
6. يمكن للجماعات الإرهابية مهاجمة نظم مراقبة الحركة الجوية، والتسبب في تصادم الطائرات المدنية، لان الإرهاب سيدخل ويخترق أجهزة استشعار قمرة القيادة، ويمكن عمل نفس الشيء لخطوط السكك الحديدية ويتسبب ايضاً في تصادم الطائرات[2].

ان استغلال الذكاء الاصطناعي في خدمة الإرهاب يعد عاملاً رئيسياً في تدمير المجتمعات وزعزعة الاستقرار داخل الدول، وهذه التهديدات لا تقتصر على الدول المتقدمة فحسب، بل تمتد الى الدول الأقل تقدماً التي تسعى الى التحول الرقمي، وبدأت العديد من المؤسسات في تطبيق أنظمة الحكومة الالكترونية، مما يجعلها عرضة للهجمات الإرهابية، من ناحية أخرى فإن أجهزة المخابرات التي تتبع دولاً تدعم الإرهاب تستغل هذه التقنيات لزعزعة الاستقرار السياسي، وتعريض أمن المواطنين للخطر، ولكل هذه الأسباب يجب الاستعداد الأمني لكل هذه المخاطر[3].

المطلب الثاني: دور الذكاء الاصطناعي في مكافحة الإرهاب السيبراني

يعد الإرهاب السيبراني من أخطر اشكال الإرهاب في العالم، نظراً لدور الفضاء السيبراني في مختلف المجالات، ويكمن خطر المنظمات الإرهابية في استخدام التقنيات الذكية للدعم والتجنيد ونشر الأفكار، بالإضافة الى التلاعب بأنظمة الأمان، والتهديد، الا ان هذه التقنيات الذكية ليست مقتصرة على استخدامها من قبل الجماعات الإرهابية فقط، ولكن تستخدمها الدول للحد من خطر الإرهاب والتعرف على الجماعات الإرهابية. ومن أبرز الاستخدامات لتقنيات الذكاء الاصطناعي في مكافحة الإرهاب السيبراني هي كالاتي:

1. المساعدة في تقويض الأفكار المتطرفة

ان الجماعات الإرهابية تستخدم التقنيات الذكية لعمل فيديوهات وصور تروج لأفكارها الإرهابية، وذلك لجذب المواطنين العاديين، لذا تقوم الدول باستخدام الذكاء الاصطناعي في التعرف على ذلك المحتوى

[1] – المصدر السابق نفسه، ص455.

[2] –علي احمد أبراهيم، تطبيقات الذكاء الاصطناعي في مواجهة الجرائم الالكترونية، المجلة القانونية، جامعة القاهرة، كلية الحقوق، القاهرة، المجلد9، العدد8، 2021، ص2822.

[3] –طارق السيد محمود تقنيات الذكاء الاصطناعي ودورها في تسهيل الإرهاب الالكتروني ومكافحته، مجلة جامعة الزيتونة الأردنية للدراسات القانونية، جامعة الزيتونة الأردنية، الأردن، اصدار خاص، 2024، ص298–299.

الذي يحمل افكاراً إرهابية وتعمل على حجبه وتصدير محتوى مضاد يحمل حقائق مخالفة للأفكار الإرهابية[1].

2. تقنية التعرف على الوجه

تقوم هذه التقنية على استخدام الكاميرات الاعتيادية التي يستخدمها المرور لحصد البيانات من كل مكان وتحليلها انياً لتشخيص المشتبه بهم وتتبع المجرمين، كما تتمكن خوارزميات الذكاء الاصطناعي من القيام بتشخيص ومطابقة صور الإرهابيين التي تم رسمها من قبل مختصي الأدلة الجنائية، وتنبيه المراقبين في حالة مرور الشخص من أمام أي كاميرا[2]، وتمتلك الصين الريادة في هذا الموضوع كونها تنشر أنظمة المراقبة والتعرف على الوجوه بعدة طرق مثل كاميرات الشوارع والمرور والنظارات الحاسوبية التي زودت بها رجال الشرطة منذ عام2018 اذ اعتمدت على النظارات المجهزة بكاميرات ذكية تسمح بالتعرف على هوية الأشخاص المفهرسين في قاعدة البيانات وتمييزهم بألوان حمراء او خضراء حسب سجلاتهم الجنائية، وتقوم الأنظمة الذكية بالتقاط صور للوجوه الجديدة غير الموجودة في قاعدة البيانات من خلال لقطات فديو حية والبحث عن هويتها في مواقع التواصل الاجتماعي او مصادر أخرى مفتوحة وعمل ملف تعريفي عن الشخص بشكل آني[3].

3. تقنية البلوك تشين blockchain

هي التقنية التي تضمن صلاحية العملات الرقمية، ويمكن ان تساعد في التصدي للهجمات السيبرانية، لأنه لا يمكن تعديل او حذف البيانات المخزنة بمرور الوقت، وتعتبر هذه التقنية احد الاحتمالات القابلة للتطبيق للحفاظ على المعلومات الحساسة في مأمن من الإرهابيين، اذ يتم التحقق من المعلومات وأضافتها بشكل دائم في دفتر الأستاذ الرقمي، ولهذا من الصعب التلاعب بالمحتوى، لاسيما انها تعزز الشفافية بين جميع الأطراف المعنية، يُمكن البلوك تشين المؤسسات من التعامل الآمن مع المعلومات، مما دفع العديد من الشركات الكبرى مثل UPS وIbm وWalmart وMicrosoft تستخدمه لحماية بياناتها واكتشاف أي شكل من اشكال التخريب السيبراني[4].

---

[1] –محمد خليفة محمد سليمان، نزار محمد احمد، دور الذكاء الاصطناعي في مكافحة جريمة تمويل الإرهاب الإلكتروني، بيردانا المجلة الدولية للبحوث الاكاديمية، المجلد19، العدد1، 2024، ص73.

[2] –عبد الله موسى، احمد حبيب بلال، مصدر سبق ذكره، ص180.

[3] –جلين جيه. فويلز، صعود الحرب الالكترونية والهوية والمعلومات وخصائص الحرب الحديثة، ترجمة مركز حازم لترجمة الدراسات الاستراتيجية، 2015، ص109، متاح على الرابط التالي: https://share.google/asIRpOPDOAJTzLHWn تاريخ الدخول: 24\4\2025.

[4] – أماني عصام محمد عبد الحميد، مصدر سبق ذكره، ص466.

4. استخدام انترنت الأشياء لمكافحة الإرهاب

ان عملية تشخيص المشتبه بهم او من لديهم سلوك عنيف ستكون اسهل اذا ما عدنا الى قواعد البيانات الأمنية المتعلقة بالدولة والتي تم دمجها مع البيانات التي يجمعها أنترنت الأشياء آنياً، اذ من السهل تشخيص الإرهابيين بالاعتماد على مقارنة السجلات السابقة مع لقطة كاميرا او بصمة صوتية اثناء مكالمة او من خلال السيارات ذاتية القيادة، وأجهزة الكمبيوتر والمصاعد وغيرها من المستشعرات المرتبطة بالإنترنت والتي تجمع البيانات، كما يمكن تتبع الأماكن التي يرتادها الشخص ومكان عيشه بالاعتماد على الجوال الذي بحوزته، بالإضافة الى مراقبة الأماكن التي يرتادها الشخص والتجمعات الدينية والاوقات التي يقضيها ويحدد نوع الرفقة لهذه الأماكن[1].

5. رصد الحدود ومنع التسلل

يمكن للإرهابيين الانتقال الى دول أخرى لممارسة انشطتهم الإرهابية من خلال التسلل عبر الحدود، مما دفع الدول الى التأكد من ان الحركة عبر الحدود تجري أمام انظارها، ولقد استخدمت تقنيات الذكاء الاصطناعي لمنع عمليات التسلل مع دقة عالية وكلفة منخفضة بالمقارنة مع المشاريع الانشائية، على سبيل المثال قامت شركة (Anduril) وهي شركة تقنيات دفاعية أمريكية، بتقديم جهاز ذكاء اصطناعي يقوم برصد وتحديد الأشياء من مسافات بعيدة مع عدد أقل من الأجهزة، كما تلعب الطائرات المسيرة دوراً كبيراً في مراقبة الحدود ومكافحة التسلل من مسافات بعيدة[2].

6. الكشف عن مواد المتفجرات والمواد السامة

أدى التطور التكنولوجي في أجهزة الاستشعار والحساسات الإلكترونية الى تمكين الحواسيب من امتلاك قدرات شبيهة بحواس الانسان، بالإضافة الى المستشعرات بالغة الحساسية التي تنقل الصوت والصورة واللمس، ويمكن من خلال هذه التقنية كشف المتفجرات والسموم والمخدرات ومنع نقلها او تصنيعها لأغراض إرهابية، اذ تضيف هذه التقنية بُعداً جديداً في مجال الإجراءات الأمنية للحماية من الإرهاب وتعرقل أنشطة الإرهابيين، مما يجعل هذه التقنية تشكل المشكلة الاعقد بالنسبة للإرهابيين كون مستشعرات الروائح لا يمكن رصدها بسهولة مثل كاميرات المراقبة[3].

هذه الإمكانات جميعها تمثل سبل للحد من انتشار الإرهاب وسرعة احباط النشاطات الإرهابية، وللتخفيف من تأثير هذه الهجمات السيبرانية في حالة وقوع هجوم سيبراني، يعد اتخاذ اجراء سريع امراً بالغ الأهمية للتخفيف من تأثير الهجوم ومنع المزيد من الاضرار، بالإضافة الى تعزيز ثقافة الاستخدام المسؤول للتكنولوجيا

[1]– غسان مراد، دهاء شبكات التواصل الاجتماعي وخبايا الذكاء الاصطناعي، ط2، شركة المطبوعات للتوزيع والنشر، بيروت، لبنان، 2019، ص140.

[2]– حسام رشيد هادي الربيعي، مصدر سبق ذكره، ص124–125.

[3]– محمد علي عباس علي، الذكاء الاصطناعي ومستقبل النظام الدولي، المجلة السياسية والدولية، الجامعة المستنصرية، كلية العلوم السياسية، بغداد، العدد62، 2025، ص418.

وتنفيذ تدابير قوية للأمن السيبراني، وبهذا يمكننا الاستفادة من فوائد الذكاء الاصطناعي مع الحماية من إساءة استخدامه[1].

يتضح مما تقدم ان تقنيات الذكاء الاصطناعي على الرغم من استخدامها من قبل المنظمات الإرهابية، الا ان هناك جانب إيجابي في هذه التقنيات وهو ان الحكومات تستخدمها لمكافحة هذه المنظمات الإرهابية من القيام بأعمالها الاجرامية، وحماية الأمن السيبراني للدول والمؤسسات من خطر هذه المنظمات.

الخاتمة

يشهد العالم تسارعا ملحوظا نحو توظيف الذكاء الاصطناعي لاسيما ما يتعلق بموضوع الفضاء السيبراني والأمن تحديداً، الأمر الذي تحاول الجماعات الارهابية استغلاله، لتحقيق اهدافها ومراميها وهو ما أثر في الأمن الدولي بشكل عام.

وبسبب التطور التكنولوجي ظهرت أنواع جديدة من التهديدات السيبرانية، شكلت تحدياً جديداً للأمن السيبراني نتيجة استخدام تقنيات الذكاء الاصطناعي، وازداد اعتماد الجماعات الإرهابية على هذه التقنيات الذكية في نشاطاتها، اذ أصبح هناك نوع اخر من الحروب هو الحروب غير التقليدية بين الجماعات الإرهابية والأجهزة الأمنية للدول، وأصبح الجانب الأمني أكثر تغلغلاً في المجالات التكنولوجية والمعلوماتية من اجل التعامل مع التطورات التكنولوجية التي قد تهدد الأمن القومي للدول.

المقترحات

تذهب الدراسة باتجاه طرح المقترحات الاتية:

1- تعزيز اجراءات الدفاع السيبراني في العراق لا سيما في الوزارات ذات العلاقة بالأمن عبر الاستفادة من الطاقات المتاحة.
2- دعم كلية الذكاء الاصطناعي التي ستفتتح في جامعة بغداد.
3- دعم دراسات الامن السيبراني واستحداث مسابقة لأفضل دراسة نظرية وتطبيقية في هذا المجال.
4- دعم المؤتمرات العلمية التخصصية حول الذكاء الاصطناعي.
5- استحداث جمعية علمية مخصصة للذكاء الاصطناعي ومركز متخصص في هذا المجال.

[1]- نسيم رمضان، كيف يمكن للذكاء الاصطناعي أن يؤجج الجرائم الإلكترونية؟، تاريخ النشر 12\مارس\2024، متاح على الرابط التالي: https://search.app/wHbAkisPpM2XURuEA تاريخ الدخول: 26\4\2025.

قائمة المصادر والمراجع :

- -الان بونيه، الذكاء الاصطناعي واقعه ومستقبله، ترجمة علي صبري فرغلي، سلسلة علم المعرفة، المجلس الوطني للثقافة والفنون والآداب، الكويت، 1993، العدد172، ص11 .
- -ابي الفضل جمال الدين محمد بن مكرم ابن منظور الافريقي المصري، ط4، لسان العرب، دار صادر للطباعة والنشر، بيروت، المجلد6، 2005، ص37 .
- -احمد عبد المجيد عبد العزيز منصور، الذكاء الاصطناعي والامن القومي، دار التعليم الجامعي، الإسكندرية، 2024، ص15 .
- -عبد الله موسى، احمد حبيب بلال، الذكاء الاصطناعي ثورة في تقنيات العصر، ط1، المجموعة العربية للتدريب والنشر، القاهرة، 2019، ص20 .
- السعيد عبد الحميد إبراهيم، مخاطر تطورات تقنيات الذكاء الاصطناعي، ط1، دار العلم والايمان للنشر والتوزيع، مصر 2024، ص17 .
- احمد عبد المجيد عبد العزيز منصور، مصدر سبق ذكره، ص44.
- المصدر السابق نفسه، ص45-46.
- إيهاب خليفة، الذكاء الاصطناعي: تأثيرات تزايد دور التقنيات الذكية في الحياة اليومية للبشر، مجلة اتجاهات الاحداث، الامارات، العدد20، 2017، ص63.
- اسراء شريف جيجان، صفا عباس فاضل، تأثير الفضاء السيبراني على الحروب الحديثة، مجلة دراسات تربوية، مركز البحوث والدراسات التربوية، العراق، العدد65، 2024، ص1 12 .
- مثنى مشعان المزروعي، ضياء مدلول فرج، "الفضاء الالكتروني ودوره في رسم خريطة جديدة للشرق الأوسط"، مجلة ديالى للبحوث الإنسانية، جامعة ديالى، العدد 76، 2018، ص400-401.
- سيف نصرت توفيق الهرمزي، "فواعل النظام الدولي الجديد في القرن الحادي والعشرين"، مجلة تكريت للعلوم السياسية، تكريت، العدد11، 2017، ص130 .
- عمار ياسر زهير البابلي، التحديات الأمنية المعاصرة للهجمات السيبرانية، مجلة الفكر الشرطي، القيادة العامة لشرطة الشارقة، مركز بحوث الشرطة، الامارات، المجلد30، العدد3، 2012، ص27 .
- صباح عبد الصبور عبد الحي، "استخدام القوة الالكترونية في التفاعلات الدولية: تنظيم القاعدة نموذجاً"، مجلة المعهد المصري، إسطنبول، العدد2، 2015، 183 .
- إيهاب خليفة، القوة الالكترونية: كيف يمكن ان تدير الدول شؤونها في عصر الانترنت "الولايات المتحدة الامريكية نموذجا"، ط1، العربي للنشر والتوزيع، القاهرة، 2017، ص56.
- خالد ممدوح إبراهيم، التهديدات السيبرانية وحماية البيانات، ط1، دار الفكر الجامعي، الإسكندرية، 2024، ص33.
- شريفة الكلاع، الامن السيبراني واشكال التهديدات: تحديات عالمية، الفا للوثائق للنشر والتوزيع، عمان، 2023، ص30-31.
- خالد ممدوح إبراهيم، التنظيم القانوني للذكاء الاصطناعي، دار الفكر الجامعي، الاسكندرية، 2022، ص3 32.
- -خالد ممدوح إبراهيم، التهديدات السيبرانية وحماية البيانات، مصدر سبق ذكره، ص71 .
- إيهاب خليفة، الحرب السيبرانية الاستعداد لقيادة المعارك في الميدان الخامس، العربي للنشر والتوزيع، القاهرة، 2021، ص81 .

- الذكاء الاصطناعي وتوظيفه من قبل الجماعات الإرهابية.. خبير يكشف مخاطر جديدة، تاريخ النشر 16\مارس\2025، متاح على الرابط التالي : https://search.app/YsFHjW1amcXYrZ6SA تاريخ الدخول: 22\4\2025.
- إيهاب خليفة، فرص وتهديدات الذكاء الاصطناعي في السنوات العشر القادمة، تقرير المستقبل: مجلة اتجاهات الاحداث، أبو ظبي، الامارات، العدد27، 2018، ص14 .
- حمد الحوسني، الذكاء الاصطناعي والإرهاب.. الآليات وسبل المواجهة، تاريخ النشر 11\مارس\2024، متاح على الرابط التالي https://search.app/eUcgqFZnZnRuQo3x9 : تاريخ الدخول:23\4\2025.
- -ماهر فرغلي، ضرورة مجابهة الاستخدام الإرهابي للذكاء الاصطناعي، تاريخ النشر 22\يناير\2024، متاح على الرابط التالي https://search.app/HZ5r7NUqPoB6H4FF9 : تاريخ الدخول: 23\4\2025.
- -حسام رشيد هادي الربيعي، الذكاء الاصطناعي وأثره في النظام الدولي، رسالة ماجستير، (غير منشورة)، الجامعة المستنصرية، كلية العلوم السياسية، 2022، ص116 .
- اماني عصام محمد عبد الحميد، الحرب والإرهاب الالكتروني في ظل الذكاء الاصطناعي: التهديدات وآليات المواجهة، مجلة وادي النيل للدراسات والبحوث الإنسانية والاجتماعية والتربوية، جامعة القاهرة، كلية الآداب، القاهرة، المجلد 43، العدد43، 2024، ص449.
- المصدر السابق نفسه، ص455 .
- -علي احمد أبراهيم، تطبيقات الذكاء الاصطناعي في مواجهة الجرائم الالكترونية، المجلة القانونية، جامعة القاهرة، كلية الحقوق، القاهرة، المجلد9، العدد8، 2021، ص2822.
- -طارق السيد محمود تقنيات الذكاء الاصطناعي ودورها في تسهيل الإرهاب الالكتروني ومكافحته، مجلة جامعة الزيتونة الأردنية للدراسات القانونية، جامعة الزيتونة الأردنية، الأردن، اصدار خاص، 2024، ص298-299 .
- -محمد خليفة محمد سليمان، نزار محمد احمد، دور الذكاء الاصطناعي في مكافحة جريمة تمويل الإرهاب الإلكتروني، بيردانا المجلة الدولية للبحوث الاكاديمية، المجلد19، العدد1، 2024، ص73.
- -عبد الله موسى، احمد حبيب بلال، مصدر سبق ذكره، ص180 .
- -جلين جيه. فويلز، صعود الحرب الالكترونية والهوية والمعلومات وخصائص الحرب الحديثة، ترجمة مركز حازم لترجمة الدراسات الاستراتيجية، 2015، ص109، متاح على الرابط التالي : https://share.google/asIRpOPDOAJTzLHWn تاريخ الدخول: 24\4\2025 .
- أماني عصام محمد عبد الحميد، مصدر سبق ذكره، ص466 .
- غسان مراد، دهاء شبكات التواصل الاجتماعي وخبايا الذكاء الاصطناعي، ط2، شركة المطبوعات للتوزيع والنشر، بيروت، لبنان، 2019، ص140 .
- حسام رشيد هادي الربيعي، مصدر سبق ذكره، ص124-125 .
- محمد علي عباس علي، الذكاء الاصطناعي ومستقبل النظام الدولي، المجلة السياسية والدولية، الجامعة المستنصرية، كلية العلوم السياسية، بغداد، العدد62، 2025، ص418 .
- نسيم رمضان، كيف يمكن للذكاء الاصطناعي أن يؤجج الجرائم الإلكترونية؟، تاريخ النشر 12\مارس\2024، متاح على الرابط التالي : https://search.app/wHbAkisPpM2XURuEA تاريخ الدخول: 26\4\2025.

- Wayne E. Baker and others, Artificial Intelligence, United States Army Sergeants Major Academy, 2007, p4.
- Chun-wei yang and others, application of intelligence in intelligent manufacturing, the second academy of China aerospace science and technology Corporation, Beijing, China, 2017, p87.

Bibliography of Arabic References (Translated toEnglish)

- Alain Bonnet, Artificial Intelligence: Its Reality and Future, translated by Ali Sabri Farghali, World of Knowledge Series, National Council for Culture, Arts and Letters, Kuwait, 1993, Issue 172, p. 11.
- Abu al-Fadl Jamal al-Din Muhammad ibn Makram Ibn Manzur al-Afriqi al-Misri, 4th ed., Lisan al-Arab, Dar Sader for Printing and Publishing, Beirut, Vol. 6, 2005, p. 37.
- Ahmed Abdel Majeed Abdel Aziz Mansour, Artificial Intelligence and National Security, University Education House, Alexandria, 2024, p. 15.
- Chun-wei Yang and others, Application of Intelligence in Intelligent Manufacturing, The Second Academy of China Aerospace Science and Technology Corporation, Beijing, China, 2017, p. 87.
- Abdullah Musa, Ahmed Habib Bilal, Artificial Intelligence: A Revolution in Modern Technologies, 1st ed., Arab Group for Training and Publishing, Cairo, 2019, p. 20.
- Wayne E. Baker and others, Artificial Intelligence, United States Army Sergeants Major Academy, 2007, p. 4.
- Al-Saeed Abdel Hamid Ibrahim, Risks of Developments in Artificial Intelligence Technologies, 1st ed., Dar Al-Ilm wa Al-Iman for Publishing and Distribution, Egypt, 2024, p. 17.
- Ahmed Abdel Majeed Abdel Aziz Mansour, previously cited source, p. 44.
- The same previous source, pp. 45–46.
- Ihab Khalifa, Artificial Intelligence: The Effects of the Increasing Role of Smart Technologies in the Daily Life of Humans, Trends of Events Journal, UAE, Issue 20, 2017, p. 63.
- Isra Sharif Jaijan, Safa Abbas Fadel, The Impact of Cyberspace on Modern Wars, Educational Studies Journal, Center for Educational Research and Studies, Iraq, Issue 65, 2024, p. 1 12.
- Khaled Mamdouh Ibrahim, Cyber Threats and Data Protection, 1st ed., Dar Al-Fikr Al-Jami‘i, Alexandria, 2024, p. 33.

- Muthanna Mishaan Al-Mazrouei, Diaa Madlool Faraj, "Cyberspace and Its Role in Drawing a New Map for the Middle East," Diyala Journal for Human Research, University of Diyala, Issue 76, 2018, pp. 400–401.
- Saif Nasrat Tawfiq Al-Harmzi, "Actors of the New International System in the Twenty-First Century," Tikrit Journal of Political Science, Tikrit, Issue 11, 2017, p. 130.
- Ammar Yasser Zuhair Al-Babli, Contemporary Security Challenges of Cyberattacks, Police Thought Journal, Sharjah Police General Headquarters, Police Research Center, UAE, Vol. 30, Issue 3, 2012, p. 27.
- Sabah Abdel Sabour Abdel Hay, "The Use of Cyber Power in International Interactions: Al-Qaeda as a Model," Journal of the Egyptian Institute, Istanbul, Issue 2, 2015, p. 183.
- Ihab Khalifa, Cyber Power: How States Can Manage Their Affairs in the Internet Age, "The United States of America as a Model," 1st ed., Al-Arabi for Publishing and Distribution, Cairo, 2017, p. 56.
- Sharifa Al-Kalla', Cybersecurity and Forms of Threats: Global Challenges, Alpha for Documentation Publishing and Distribution, Amman, 2023, pp. 30–31.
- Khaled Mamdouh Ibrahim, The Legal Regulation of Artificial Intelligence, Dar Al-Fikr Al-Jami'i, Alexandria, 2022, p. 3 32.
- Khaled Mamdouh Ibrahim, Cyber Threats and Data Protection, previously cited source, p. 71.
- Ihab Khalifa, Cyber Warfare: Preparing to Lead Battles in the Fifth Domain, Al-Arabi for Publishing and Distribution, Cairo, 2021, p. 81.
- Artificial Intelligence and Its Use by Terrorist Groups: An Expert Reveals New Risks, publication date: 16 March 2025, available at the following link: https://search.app/YsFHjW1amcXYrZ6SA access date: 22/4/2025.
- Ihab Khalifa, Opportunities and Threats of Artificial Intelligence in the Next Ten Years, Future Report: Trends of Events Journal, Abu Dhabi, UAE, Issue 27, 2018, p. 14.
- Hamad Al-Hosani, Artificial Intelligence and Terrorism: Mechanisms and Ways of Confrontation, publication date: 11 March 2024, available at the following link: https://search.app/eUcgqFZnZnRuQo3x9 access date: 23/4/2025.
- Maher Farghali, The Necessity of Confronting the Terrorist Use of Artificial Intelligence, publication date: 22 January 2024, available at the following link: https://search.app/HZ5r7NUqPoB6H4FF9 access date: 23/4/2025.

- Hussam Rashid Hadi Al-Rubaie, Artificial Intelligence and Its Impact on the International System, Master's Thesis, unpublished, Al-Mustansiriya University, College of Political Science, 2022, p. 116.
- Amani Essam Mohammed Abdel Hamid, Cyber Warfare and Cyber Terrorism under Artificial Intelligence: Threats and Mechanisms of Confrontation, Nile Valley Journal for Human, Social and Educational Studies and Research, Cairo University, Faculty of Arts, Cairo, Vol. 43, Issue 43, 2024, p. 449.
- The same previous source, p. 455.
- Ali Ahmed Ibrahim, Applications of Artificial Intelligence in Combating Cybercrimes, Legal Journal, Cairo University, Faculty of Law, Cairo, Vol. 9, Issue 8, 2021, p. 2822.
- Tariq Al-Sayed Mahmoud, Artificial Intelligence Technologies and Their Role in Facilitating and Combating Cyber Terrorism, Al-Zaytoonah University of Jordan Journal for Legal Studies, Al-Zaytoonah University of Jordan, Jordan, Special Issue, 2024, pp. 298–299.
- Mohammed Khalifa Mohammed Suleiman, Nizar Mohammed Ahmed, The Role of Artificial Intelligence in Combating the Crime of Financing Cyber Terrorism, Berdana International Journal of Academic Research, Vol. 19, Issue 1, 2024, p. 73.
- Abdullah Musa, Ahmed Habib Bilal, previously cited source, p. 180.
- Glenn J. Voelz, The Rise of Cyber Warfare: Identity, Information, and the Characteristics of Modern Warfare, translated by Hazem Center for Translation of Strategic Studies, 2015, p. 109, available at the following link: https://share.google/asIRpOPDOAJTzLHWn access date: 24/4/2025.
- Amani Essam Mohammed Abdel Hamid, previously cited source, p. 466.
- Ghassan Murad, The Cunning of Social Networks and the Secrets of Artificial Intelligence, 2nd ed., Publications Company for Distribution and Publishing, Beirut, Lebanon, 2019, p. 140.
- Hussam Rashid Hadi Al-Rubaie, previously cited source, pp. 124–125.
- Mohammed Ali Abbas Ali, Artificial Intelligence and the Future of the International System, Political and International Journal, Al-Mustansiriya University, College of Political Science, Baghdad, Issue 62, 2025, p. 418.
- Naseem Ramadan, How Can Artificial Intelligence Fuel Cybercrimes?, publication date: 12 March 2024, available at the following link: https://search.app/wHbAkisPpM2XURuEA access date: 26/4/2025.