تقنيات الذكاء الاصطناعي ودورها فى تسهيل الإرهاب الإلكتروني ومكافحته

طارق السيد محمود يوسف *

DOI:10.15849/ZJJLS.240330.14

* **القانون الجنائي، كلية الحقوق.**
* للمراسلة: Tarek.okeal2023@gmail.com

الملخص

يأتي هذا البحث ليلقى الضوء على أحد المخاطر التى يشكلها التطور الرهيب لتقنيات الذكاء الاصطناعي، حيث قد يؤدي هذا التطور إلى تهديد للأمن القومى من خلال قيام الجماعات الإرهابية فى استغلال هذه التقنية فى مشاريعها الإجرامية. وقد تم التعرض خلال البحث التعريف بتقنيات الذكاء الاصطناعي وخصائصها، مع إلقاء الضوء على الفجوة الواسعة بين عالمنا العربي والدول الغربية فى هذا المجال، وتم التركيز على علاقة الذكاء الاصطناعي بالإرهاب الإلكتروني، مع بيان الوسائل التي من خلالها يتم استخدام هذه التقنية من قبل الجماعات الإرهابية ومدى خطورتها، وهو ما يتطلب وضع حلول لهذه الإشكالية.

الكلمات الدالة: الذكاء الاصطناعي؛ الإرهاب الإلكتروني؛ الخوارزميات؛ الهجمات السيبرانية؛ طائرات بدون طيار؛ التزييف العميق.

Artificial Intelligence Techniques and Their Role in Facilitating and Combating Electronic Terrorism

Tarek Elsayed Mahmoud Yousef *

* **Criminal Law, Faculty of Law.**

*** Crossponding author: Tarek.okeal2023@gmail.com**

Abstract

This research sheds light on one of the dangers posed by the terrible development of artificial intelligence technologies, as this development may lead to a threat to national security through terrorist groups exploiting this technology in their criminal projects. During the research, the definition of artificial intelligence techniques and their characteristics was presented, while highlighting the wide gap between our Arab world and Western countries in this field. The focus was on the relationship of artificial intelligence to electronic terrorism, with an explanation of the means through which this technology is used by terrorist groups and to what extent. Its seriousness, which requires developing solutions to this problem.

Keywords: artificial intelligence; cyber terrorism; algorithms; cyber-attacks; Drones; Deep fakes.

مقدمة

التفكير وهو الأمر الذي كان محل استغراب، باعتباره ضربًا من الخيال، ثم بدأت الفكرة تأخذ بعدًا آخر حينما تمكن أحد الباحثين فى جامعة برنستن الأمريكية من تنفيذ أول جهاز كمبيوتر يستعمل الشبكات العصبية فى عام 1951م وبعد مرور أربع سنوات دعا العالم الأمريكى جون ماكارثى مجموعة من الباحثين المهتمين بعلوم الكمبيوتر إلى مؤتمر بشأن التشاور حول تأسيس ميدان جديد للبحث العلمي،[1] وخلال المؤتمر وضعت اللبنات الأولى لعلم الذكاء الاصطناعي.

ومنذ ذلك الوقت بدأ الاهتمام بعلم الذكاء الاصطناعي، والعمل على تطويره على فترات، حيث مرّت عملية تطوير الذكاء الاصطناعي بخمس مراحل رئيسية تُمثّل دورة حياة الذكاء الاصطناعي، تبدأ من مرحلة فهم الأشياء، ثم خلق علاقات بينها، ثم إدراك كامل البيئة المحيطة بها، ثم الاستقلال الكامل واتخاذ القرار بصورة منفردة، وصولًا إلى موجة خامسة يتفوق فيها الذكاء الاصطناعي على قدرات البشر.[2]

وما كان حلمًا بالأمس بات اليوم واقعًا ملموسًا، من خلال الثورة التكنولوجية التى يشهدها عالمنا المعاصر فقد أصبح الذكاء الاصطناعي حاضرًا فى شتى المجالات، فظهرت تقنيات التعلم العميق، وتكنولوجيا الروبوتات، والسيارات ذاتية القيادة، والطائرات دون طيار، فضلًا عن استخدام تقنيات الذكاء الصناعي فى التعليم كالتدريس الآلي،[3] وكذلك فى المجالات الطبية، كربوت الرعاية الصحية.[4]

وامتد تطور الذكاء الاصطناعي إلى مجال التسلح، فظهرت الأسلحة المستقلة الفتاكة، وما يعرف بالروبوت القاتل وهو الأمر الذي أصبح يشكل تحديًا خطيرًا على الصعيدين القانونى والأخلاقى،[5] وأصبح الذكاء الاصطناعي مجالًا رحبًا لسباق التسلح بين الدول الكبرى، وتتجه كل من الولايات المتحدة والصين وروسيا إلى تطوير أجيال جديدة ومتقدمة من أنواع الأسلحة التي تعتمد على الذكاء الاصطناعي.[6]

أمام هذا التطور الهائل فى تقنيات الذكاء الصناعي أصبح هناك هاجس لدى الكثيرين من حجم المخاطر الكارثية التى قد يسببها استخدام هذه التقنيات دون ضوابط، وفى سبيل ذلك يتم عقد المناقشات على المستوى الدولى

---

(1) عبد النور عبد النور، عادل، مدخل إلى عالم الذكاء الاصطناعي، مدينة الملك عبد العزيز للعلوم والتقنية، المملكة العربية السعودية، 1426هـ، 2005م، ص22: 23.

(2) خليفة، إيهاب، هيمنة الآلات:دورة حياة الذكاء الاصطناعي من الإدراك إلى تهديد البشر، 8 يناير، 2019، مركز المستقبل للدراسات والأبحاث المتقدمة، متاح على الرابط التالى، بشبكة المعلومات الدولية، تاريخ الدخول، 2023/10/8م.
https://futureuae.com/ar-AE/Mainpage/Item/4451

(3) أندرو بيرغ وإدوارد بايف ولويس–فليبي زانا، الروبوت والنمو وعدم المساواة، مجلة التمويل والتنمية، عدد سبتمر 2016م، صندوق النقد الدولى، ص10، متاح على الرابط التالى، تمت الزيارة 2023/10/8م
https://www.imf.org/external/arabic/pubs/ft/fandd/2016/09/pdf/berg.pdf

2 Moritz Goldener, Cornelius Herstatt, Frank TIietze, "The emergence of care robotics – A patent and publication analysis", Technological Forecasting and Social Change, Vol. 92, March 2015, pp.115 et seq

(5) الشادى، سما سلطان، بعض التحديات التي تثيرها أنظمة الأسلحة الفتاكة ذاتية التشغيل على الصعيدين القانون والأخلاقي، المجلة القانونية والقضائية، السنة 14، العدد2، وزارة العدل القطرية، 2020م، ص342، وما بعدها.

(6) أحمد، رانية محمد طاهر، أثر الذكاء الاصطناعي على الأمن الدولى، مجلة البحوث المالية والتجارية، العدد 3،كلية التجارة، جامعة بور سعيد يوليو 2020م، ص248.

فى محاولة وضع قواعد للتحكم البشري فى هذا المجال، وإصدار التشريعات التى تنظم استخدام تقنيات الذكاء الاصطناعي.[1]

ويحتل الذكاء الاصطناعي فى الوقت الحاضر مكان الصدارة بين موضوعات البحث العلمي على مستوى العالم فى محاولة جادة للبحث عن وسائل الاستفادة منه فى مختلف النواحي الحياتية، والوقوف كذلك على مدى الخطر الذي يشكله التطور السريع فى هذا المجال، ومحاولة البحث عن سبل للوقاية من تلك المخاطر، وقبل التركيز على موضوع البحث سنحاول من خلال الأبحاث التى نشرت فى هذا الموضوع أن نتعرف على تعريف الذكاء الاصطناعي وخصائصه، مع بيان أنواع الذكاء الاصطناعي، وأخيرًا عرض الفجوة بين عالمنا العربي والغرب فى هذا المجال، وذلك على النحو التالى:

تعريف الذكاء الاصطناعي وخصائصه:

الذكاء الاصطناعي مصطلح عام وشامل يتضمن العديد من المجالات الفرعية، وقد تعددت وجهات النظر فى تحديد مدلول الذكاء الاصطناعي،[2] ومعظم هذه التعريفات قد تأثرت . إلى حد بعيد . بأول تعريف وضعه جون ماكارثى، إذ عرفه بأنه: " علم هندسة إنشاء آلات ذكية، وبصورة خاصة برامج الكمبيوتر"، فهو علم إنشاء أجهزة وبرامج كمبيوتر قادرة على التفكير بنفس الطريقة التي يعمل بها الدماغ البشري، تتعلم مثلما نتعلم، وتقرر كما نقرر، وتتصرف كما نتصرف".[3]

وبهذا المعنى، فإن الذكاء الاصطناعي هو عملية محاكاة الذكاء البشري عبر أنظمة الكمبيوتر، فهي محاولة لتقليد سلوك البشر ونمط تفكيرهم وطريقة اتخاذ قراراتهم،[4] وتتم من خلال دراسة سلوك البشر عبر إجراء تجارب على تصرفاتهم، ووضعهم في مواقف معينة، ومراقبة رد فعلهم ونمط تفكيرهم وتعاملهم مع هذه المواقف، ومن ثم محاولة محاكاة طريقة التفكير البشرية عبر أنظمة كمبيوتر، تنتهي بإنشاء آلة بقدرات عقلية بشرية قادرة على الفهم والتمييز والتصرف واتخاذ القرارات.

ومن وجهة نظر البعض إن هذا التعدد فى وجهات النظر حول تعريف الذكاء الاصطناعي يدور حول نقطة واحدة تتمثل فى كيفية منح الآلة صفة الذكاء،أو بمعنى بناء أنظمة ذكية تساير أو تحاكي الذكاء البشري.[5]

---

[1] عباس، علا غازى فرحان، أسلحة الذكاء الاصطناعي فى ظل مبادئ القانون الدولى الإنسانى، مجلة الميزان للدراسات الإسلامية والقانونية، المجلد 9، عدد3،عمادة البحث العلمى، جامعة العلوم الإسلامية العالمية، عمان، الأردن، أيلول، 2022م، ص413.

[2] عبد الله كريم، سلام، التنظيم القانونى للذكاء الاصطناعي، رسالة دكتوراه، كلية القانون، جامعة كربلاء، العراق، 2022م، ص16: 20.

[3] العميريين، وجيه محمد سليمان، الذكاء الاصطناعي في التحري والتحقيق عن الجريمة: دراسة مقارنة، مجلة الميزان للدراسات الإسلامية والقانونية، المجلد9، العدد3، جامعة العلوم الإسلامية العالمية – عمادة البحث العلمي، عمان، الأردن، أيلول،2022م، ص454

Christian Montag, Harald Baumeister, Digital Phenotyping and Mobile Sensing New Developments in Psychoinformatics,2 Edition, SpringerNature Switzerland AG 2023,p.451:452

(1) Luger G F. Artificial intelligence : structures and strategies for complex problem solving, 6th Ed, Pearson Education, Harlow, England , 2009 , p5.

[5] سعد الدين محمد سعيد، وليد، المسؤلية الجنائية الناشئة عن تطبيقات الذكاء الاصطناعي، مجلة العلوم القانونية والاقتصادية، المجلد 64، العدد2، كلية الحقوق، جامعة عين شمس، يوليو2022م، ص492

وفى تعريف آخر يشير مصطلح الذكاء الاصطناعي إلى أنه: " فرع من علوم الحاسب يُعنَى بتصميم آلات قادرة على فهم بيئتها وتنفيذ مهام تتطلب في مجملها مستوى محدد من الذكاء. ويمكن لآلات الذكاء الاصطناعي أن تكون بطبيعتها قائمة على البرامج مثل المساعدين الافتراضيين الموجودين في الهواتف المحمولة، أو يمكن أن تكون مزيجًا من الأجهزة والبرامج، مثل أنظمة القيادة المستقلة الموجودة في بعض السيارات".[1]

وهناك من نادى باستبدال مصطلح الذكاء الاصطناعي بالتعلم الآلي باعتبار أن الأخير أكثر دقة؛ نظرًا لوجود ما هو اصطناعى ولكنه يتخطى الذكاء البشري.[2]

وفى رأينا أن التعريفات التى تقوم على اعتبار الذكاء الاصطناعي مجرد محاكاة للذكاء البشري تفتقر إلى الدقة؛ وذلك لعدة أسباب، أهمها أن ذكاء الآلة يجب النظر إليه بمفهوم يختلف تمامًا عن الذكاء البشري، كما أن هذا التعريف وإن صدق على تطبيقات الذكاء الاصطناعي البسيطة، فهى لا تصدق على الذكاء الاصطناعي التوليدي وهو الذي يتخطى حدود ذكاء العقل البشري، وفى ضوء ذلك يمكننا تعريف الذكاء الاصطناعي بأنه: " علم قائم على توظيف التكنولوجيا فى منح الآلة قدرات تمكنها من التصرف واتخاذ القرار بطريقة محدودة وفقًا لتوجيه العنصر البشري، أو بطريقة غير محدودة وتلقائية دون أي سيطرة بشرية".

ويتميز الذكاء الاصطناعي عن علم البيانات، وهو العلم الذي يعتني بجمع وتحليل البيانات ومعالجتها كما يختلف فى ذات الوقت عن التعلم الآلي والتعلم العميق، فالتعلم الآلي يعني قدرة الأجهزة على التعلم التلقائى دون تلقين، بينما التعلم العميق يقوم على استخدام عدة طبقات من الخوارزميات والشبكات العصبية، فمفهوم الذكاء الاصطناعي أعم وأشمل، حيث إن التعلم الآلي والتعلم العميق، كليهما يعد فرعًا من فروع الذكاء الاصطناعي.[3]

من هنا يؤكد البعض على أنه يشترط لكي نطلق هذا المصطلح على آلة فلا بد أن تكون قادرة على التعلم، وجمع البيانات، وتحليلها، واتخاذ قراراتٍ بناءً على عملية التحليل هذه بصورة مستقلة[4].

ومن هنا يؤكد البعض على أن الخصائص التى تميز الذكاء الاصطناعي تتثمل فى: القدرة على التواصل القدرة على معرفة الذات، القدرة على المعرفة الخارجية، السلوك الموجه نحو الهدف، والإبداع الذي يتمثل فى استطاعة اتخاذ قرارات بديلة عند اللزوم[5].

---

(1) https://www.mcit.gov.sa/node/15

(2) جلسة استماع في الكونجرس الأمريكي، اللجنة الفرعية للاستخبارات ومكافحة الإرهاب، لجنة الأمن القومى متاح على الرابط التالى بشبكة المعلومات الدولية، الزيارة 2023/10/9م.
https://www.congress.gov/116/chrg/CHRG-116hhrg38781/CHRG-116hhrg38781.pdf

(3) محمد أبو المعاطى صقر، وفاء، المسؤلية الجنائية عن جرائم الذكاء الاصطناعي، دراسة تحليلية، مجلة روح القوانين، العدد 96، كلية الحقوق، جامعة طنطا، أكتوبر 2021م،ص33 وما بعدها.

(4) العميرين، وجيه محمد سليمان، الذكاء الاصطناعي فى التحرى والتحقيق، مرجع سابق، ص456.

2 Hallevy, Gabriel (2010) "The Criminal Liability of Artificial Intelligence Entities - from Science Fiction to Legal Social Control," Akron Intellectual Property Journal: Vol. 4 : Iss. 2 , Article 1,p.175:176.

أنواع الذكاء الاصطناعي:

يميز الخبراء بين ثلاثة أنواع للذكاء الاصطناعي، أو كما يفضل البعض تسميتها بمستويات الذكاء الاصطناعي وهى:[1]

- الذكاء الاصطناعي الضيق: وهو أبسط مستويات الذكاء الاصطناعي، حيث يقتصر دوره على التعامل مع التجارب الحالية، وأبرز مثال له جهاز الكمبيوتر العادي، ومحرك البحث جوجل، حيث لا يمكنه التفكير ذاتيًا، فكلاهما لا يتجاوز المهمة المخصصة له.
- الذكاء الاصطناعي العام: وفى هذا المستوى يقوم الذكاء الاصطناعي بتنفيذ كافة ما يسند إليه من مهام.
- الذكاء الاصطناعي الخارق: وهو الذي يتخطى حدود الذكاء البشري ومزود بامكانية العمل بشكل مستقل.

ويسعى المتخصصون فى الوقت الحاضر على تطوير قدرات الذكاء الاصطناعي العام، بهدف الوصول إلى النوع الثالث من الذكاء الذي يستطيع تطوير نفسه، فيما يعرف بالذكاء التوليدي، الذي يتسم بالاستقلال كما أنه يتخطى الذكاء البشري، وهذا النوع من الذكاء هو الذي يثير القلق، ويعتبره البعض تهديدًا وجوديًا للبشرية.

اتساع الفجوة فى استخدامات الذكاء الاصطناعي بين الغرب وعالمنا العربي:

تشير القراءة المتأنية للتطورات المتلاحقة فى مجال تقنية الذكاء الاصطناعي إلى مدى الفجوة الواسعة بين دول عالمنا العربي والدول الأوروبية فى هذا المجال، ففيما يخص البحث والتطوير، تعتبر الولايات المتحدة الأمريكية الأولى عالميًا، حيث أنشأت أكبر القوى الأكاديمية المتخصصة فى الذكاء الاصطناعي، كما أنها سمحت بسيطرة القطاع الخاص على هذا المجال بالتعاون مع الأجهزة العسكرية وأجهزة الاستخبارات.[2] وتأتي الصين فى المرتبة الثانية، حيث تعد أقوى منافس تكنولوجي للولايات المتحدة، وتسعى من أجل الفوز فى هذا السباق وتعتقد الصين أن الذكاء الاصطناعي، وغيره من وسائل التكنولوجيا أمرًا بالغ الأهمية فى دعم جهودها الرامية إلى توسيع نفوذها على الصعيد العالمي ولتتجاوز القوة الاقتصادية والعسكرية للولايات المتحدة.[3]

---

[1] عباس، علا غازى فرحان، أسلحة الذكاء الاصطناعي فى ظل مبادئ القانون الدولى الإنسانى، مجلة الميزان للدراسات الإسلامية والقانونية، مجلد 9، العدد3،عمادة البحث العلمى، جامعة العلوم الإسلامية العالمية، أيلول، 2022م، ص410؛ عبد المجيد، ريم، تطبيقات الذكاء الاصطناعي وظاهرة الإرهاب، مجلة شئون دبلوماسية، مجلد 4، العددين 6 و7، معهد الدراسات الدبلوماسية، الجامعة البريطانية الليبية، يوليو 2020م، ص151: 152؛ عبد الله كريم، سلام، التنظيم القانونى للذكاء، مرجع سابق، ص47.

وانظر أيضًا:

Rofi Aulia Rahman, Rizki Habibulahو The Criminal Liability of Artificial Intelligence: Is It Plausible to Hitherto Indonesian Criminal System,? Legality : Jurnal Ilmiah Hukum, Vol. 27 No. 2 (2019): September.p.148.

[2] وفقاً للمؤشرات القياسية تستحوذ الولايات المتحدة على موقع الصدارة في سباق الذكاء الاصطناعي،راجع :

Artificial Intelligence Index Report,2023, p.11,Avilable at : https://aiindex.stanford.edu/wp-content/uploads/2023/04/HAI_AI-Index-Report_2023.pdf

[3] أحمد، رانية محمد طاهر، أثر الذكاء الاصطناعي على الأمن الدولى، مرجع سابق، ص256

وبلغ حجم استثمارات الصين فى مجال الذكاء الاصطناعي ما يقرب من 13,4 مليار دولار، بينما ظلت الولايات المتحدة فى القائمة باستثمارات قدرها 47,4 مليار دولار[1]، من ناحية أخرى يخصص الاتحاد الروسى ميزانية مستقلة للذكاء الاصطناعي فى المجال العسكرى، وتسعى كل من كندا واليابان ودول الاتحاد الأوروبى إلى المنافسة فى هذا المجال، أما اسرائيل فبلغت استثماراتها فى هذا المجال 1,5 مليار دولار، وهى تحتل مركز متقدم عالميًا، بينما تستحوذ على المركز الأول بين دول الشرق الأوسط.[2]

على المستوى العربي تسعى الإمارات العربية المتحدة إلى اللحاق بالركب، وفى سبيل ذلك قامت بتعيين أول وزير للذكاء الاصطناعي، كما أنشأت جامعة محمد بن زايد للذكاء الاصطناعي، وهى واحدة من الجامعات المتخصصة على مستوى العالم[3]، وتقوم حكومة دولة الإمارات كذلك بتجريب العديد من تطبيقات الذكاء الاصطناعي الرائدة، كما تشجع شركات التكنولوجيا العالمية على تنفيذ تطبيقات الذكاء القابلة للتوسع فى دولة الإمارات.

أما المملكة العربية السعودية فهى تسعى لإنشاء مشروع نيوم باستثمارات تقارب 500 مليار دولار ويتضمن المشروع إنشاء مدينة للذكاء الاصطناعي بتعاون مشترك مع مصر والأردن، كما تحاول السعودية الاهتمام بالذكاء الاصطناعي فى المجال العسكرى وتتعاون مع الصين فى هذا الجانب،[4] كما تسعى جاهدة للريادة فى مجال الذكاء الاصطناعي.[5]

وعلى الرغم من تلك الجهود تظل هناك فجوة بين عالمنا العربي ودول الغرب فى مجال الذكاء الاصطناعي خاصة فيما يتعلق بالتصنيع والتطوير واستغلال هذه التقنيات فى المجال العسكرى فى سبيل الحفاظ على الأمن القومى، ويبرر البعض ذلك بارتفاع تكلفة إنتاج وصناعة تقنيات الاصطناعي، فضلًا عن حاجتها للصيانة والتحديث بشكل دوري،[6] وأضف إلى ذلك نقص الكفاءات التى تملك المهارات اللازمة للتصنيع والإنتاج.

---

[3] Artificial Intelligence Index Report,op.cit,P.12

(2) أحمد، رانية محمد طاهر، أثر الذكاء الصناعى، المرجع ذاته، ص255.

(3) دليل الذكاء الاصطناعي، البرنامج الوطنى للذكاء الاصطناعي، ص 21، منشور على موقع وزير الدولة للذكاء الاصطناعي والاقتصاد الرقمى، على الرابط التالى: الزيارة2023/10/8م. https://ai.gov.ae/ar/publications-2/

(4) اتفاق سعودي صيني لبناء مصنع للطائرات بدون طيار بالمملكة، موقع قناة العربية على الإنترنت، بتاريخ 5 مارس 2022م الزيارة 2023/10/8م

(5) القحطانى، عايض على، دور الذكاء الاصطناعي في تحقيق التنمية المستدامة في إطار رؤية المملكة العربية السعودية ٢٠٣٠،المجلة العربية للمعلومات وأمن المعلومات، المجلد 3، العدد 9، أكتوبر 2020م، المؤسسة العربية للتربية والعلوم والآداب، ص101 وما بعدها

وقد حصلت المملكة العربية السعودية على المركز الأول عالميًا في مؤشر الاستراتيجية الحكومية للذكاء الاصطناعي، وهو أحد مؤشرات التصنيف العالمي للذكاء الاصطناعي الصادر عن تورتويس انتليجينس "Tortoise Intelligence" الذي يقيس أكثر من 60 دولة في العالم، فيما حلت ألمانيا ثانيًا والصين ثالثًا في هذا المؤشر.

ويقيس التصنيف العالمي للذكاء الاصطناعي أكثر من 100 معيار ضمن سبعة مؤشرات هي: الاستراتيجية الحكومية، والبحث والتطوير، والكفاءات، والبنية التحتية، والبيئة التشغيلية، والتجارة، الذي نالت المملكة فيه المركز الأول في مؤشر الاستراتيجية الحكومية للذكاء الاصطناعي، والمركز 31 في إجمالي مؤشرات التصنيف الصادر عن "تورتويس" وهي شركة عالمية لديها مجلس استشاري عالمي يضم خبراء في الذكاء الاصطناعي من أنحاء العالم. وحققت المملكة نسبة 100% في معايير المؤشر من أبرزها، وجود استراتيجية وطنية مخصصة ومعتمدة للذكاء الاصطناعي بالمملكة، ووجود جهة حكومية مخصصة للذكاء الاصطناعي، ووجود تمويل وميزانية خاصة بالذكاء الاصطناعي، وتحديد ومتابعة مستهدفات وطنية خاصة بالذكاء الاصطناعي. انظر: https://www.spa.gov.sa/a4ea79c31fm

(6) حسن، خالد عبد العال إسماعيل، المسئولية الدولية عن جرائم الأسلحة المستقلة ذاتية التشغيل، مجلة القانون والتكنولوجيا، مجلد 2، العدد1، كلية القانون، الجامعة البريطانية، القاهرة، إبريل2022م، ص256.

وفي رأينا الخاص أن كافة هذه المعوقات يمكن التغلب عليها، ففيما يخص الجانب الاقتصادي فيمكن التغلب عليه من خلال التعاون بين أكثر من دولة فى هذا المجال، وفيما يخص الكفاءات فهى ليست معدومة فهناك الكثير من الكفاءات العربية التى تمتلك كافة المهارات المطلوبة، وإن كانت تعمل فى الدول الأوروبية وتصنع لها المستقبل، وليس هناك ما يمنع من استقطابهم للقيام بذات الدور فى وطنهم الأم.

ورغم عدم وجود أسلحة فتاكة مستقلة بالكامل حتى الآن، إلا أن هناك توقعات باستخدام هذا الجيل من الأسلحة في معارك ميدانية في غضون السنوات القليلة القادمة، نظراً للتقدّم التقني السريع في هذا المجال والإنفاق المرتفع على الذكاء الاصطناعي وعلى أنواع أخرى من التقنيات فائقة التطور.[1]

وهو الأمر الذي يستدعى وضع ذلك فى الاعتبار أمام المسؤلين وصناع القرار فى الدول العربية فى سبيل الحفاظ على الأمن القومى، خاصة فى ظل الصراعات الدولية التى تشتعل من وقت لآخر، وانتشار سراع التسلح بين الدول الكبرى.

ويرى الخبراء أن التطور المتلاحق فى تقنيات الذكاء الاصطناعي قدم نتائج إيجابية فى خدمة البشرية إلا أنها فى ذات الوقت قد تؤدى إلى نتائج كارثية قد تترتب على سوء الاستخدام، أو نتيجة وقوع الحوادث[2] وكما يشير البعض إلى أن الباحثين قد ركزوا على الجانب الإيجابى والمضئ للذكاء الاصطناعي، بينما الجانب المظلم لم يجد ذات الاهتمام، فالذكاء الاصطناعي يمكن أن يكون خطيرًا للغاية إذا تم استخدامه بطرق غير مشروعة وهو ما يظهر بوضوح فى الجرائم السيبرانية، وتهديد الأمن القومى، ونشر العنف والكراهية وارتكاب جرائم الإرهاب.[3]

ومن خلال هذا البحث نحاول إلقاء الضوء على مخاطر تقنيات الذكاء الاصطناعي وعلاقتها بالإرهاب الإلكتروني وذلك من خلال التعرف على مدلول الإرهاب الإلكتروني، وإلى أى مدى تستطيع الجماعات الإرهابية الاستعانة بالذكاء الاصطناعي فى ارتكاب جرائمها، وإلى أى مدى يمكن مجابهة المخططات الإرهابية باستخدام الذكاء الاصطناعي.

إشكالية البحث:

تتمثل إشكالية البحث فى أن استخدام تقنيات الذكاء الاصطناعي ذات أثر مزدوج، ففى الوقت التى تحقق فيه العديد من المكاسب والإيجابيات، فإن سوء استخدامها قد يؤدى إلى كوارث، خصوصًا عند الاستحواذ عليها

---

(1) اوسوندا. أ أوسوبا، ويليام ويلسر الرابع، مخاطر الذكاء الاصطناعي على الأمن ومستقبل العمل، مؤسسة راند، منشور على الإنترنت الزيارة 2023/10/9م. ص5.
file:///C:/Users/dr%20tark/Downloads/RAND_PE237z1.arabic%20(1).pdf

(3) Risks from Artificial Intelligence,University of Cambridg, at: https://www.cser.ac.uk/research/risks-from-artificial-intelligence ; /
Markus Anderljung and Paul Scharre, Society Must Get Ready for Very Powerful Artificial Intelligence,Foreign Affairs, August 14, 2023, At:
https://www.foreignaffairs.com/world/how-prevent-ai-catastrophe-artificial-intelligence

(4) PUBLICATIONS Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes, United Nations Interregional Crime and Justice Research Institute (UNICRI), 2021 p.6 https://unicri.it/News/Algorithms-Terrorism-Malicious-Use-Artificial-Intelligence-Terrorist-Purposes

من قبل عصابات الإجرام المنظم، أو الجماعات الإرهابية؛ لذا توجب التعرف على وسائل الجماعات الإرهابية فى استخدام الذكاء الاصطناعي.

أهمية موضوع البحث:

تتمثل أهمية موضوع البحث فى كونه يأتى لتناول أحد المخاطر التى تمثلها تقنيات الذكاء الاصطناعي، فى الوقت الذي اتجه فيه معظم الباحثين إلى التركيز على الجوانب التنظيمية، والتطور المتلاحق لهذه التقنيات، كما أن الموضوع يتصل بفكرة الأمن القومى، خاصة فى ظل التحديات الراهنة، وسباق التسلح بين الدول للاستحواذ على هذه التقنيات.

أهداف البحث:

تتمثل أهداف البحث فى محاولة الإجابة عن عدة تساؤلات، وأهمها:

- ما هو الإرهاب الإلكتروني؟، وما العلاقة التى تربطه بالذكاء الاصطناعي؟
- ما مدى الخطورة المتوقعة حال استحواذ الجماعات الإرهابية على تقنيات الذكاء الاصطناعي؟
- ما هى سبل استخدام تقنيات الذكاء الاصطناعي من قبل الجماعات الإرهابية؟
- إلى أي مدى يمكن للجهات الأمنية استخدام تقنيات الذكاء الاصطناعي في التصدي للأعمال الإرهابية؟

منهج البحث:

يرتكز البحث بشكل أساسى على استخدام المنهج التحليلى، ومن خلاله نحاول تحليل كافة المعلومات والآراء لبناء وجهة نظر منطقية حول الموضوع، كما تتم الاستعانة بالمنهج المقارن، فى إجزاء من البحث.

خطة البحث: تم تقسيم البحث إلى مبحثين:

المبحث الأول: مدلول الإرهاب الإلكتروني ومخاطره

المبحث الثانى: سبل استخدام تقنيات الذكاء الاصطناعي من قبل الجماعات الإرهابية

المبحث الأول

فى مدلول الإرهاب الإلكتروني ومخاطره

حول أخطار الذكاء الاصطناعي والإرهاب الإلكتروني:

فى عام 1981 تم مقتل شاب يابانى يعمل بمصنع لصنع الدراجات النارية على يد روبوت يعمل بالذكاء الاصطناعي وقد اعتبر الربوت أن وجود هذا الشخص بالقرب منه يشكل تهديدًا لمهمته[1]، ومن هنا يثبت الواقع أن وقوع الجريمة من قبل أجهزة الذكاء الاصطناعي والروبوتات، أمر وارد الحدوث.

وبحلول عام 2021م فى ظل الجائحة التى شهدها العالم وجد العالم نفسه أمام نوع آخر من التهديدات، حيث استغلت الجماعات الإرهابية نقاط ضعف الشبكات وقامت بإطلاق عمليات قرصنة واسعة النطاق، كما تم التلاعب بالرأى العام فى العديد من القضايا وذلك من خلال استخدام الروبوتات الاجتماعية، كما تعرضت البنية التحتية فى بعض الدول للاعتداء، وكان للذكاء الاصطناعي حضوره فى تسهيل هذه الاعتداءات.[2]

وبرغم إسهامات الذكاء الاصطناعي فى تخفيف حجم المهام على جهات الأمن المعنية بالحفاظ على الأمن إلا أنه قد يشكل فى الوقت ذاته التهديد الأكبر، بل الأخطر، فكما يرى بعض الباحثين أن تقنيات الذكاء الاصطناعي حال استخدامها دون ضوابط، أو تعمد استخدامها بسوء نية قد يؤدى إلى الإضرار بالأمن القومى، والأمن السياسى والاقتصادي والاجتماعي على حد سواء[3]

ولا شك أن التطورات اللاحقة التى شهدتها تقنيات الذكاء الاصطناعي، خاصة ما يعرف بالذكاء الاصطناعي التوليدي الذي من المتوقع أن يعمل باستقلالية تامة بعيدًا عن إرادة المصنع والمبرمج، دعت البعض إلى التخوف من خروجه عن مسار الاستخدام النافع، وهذا التخوف لا يقتصر على الذكاء التوليدي وحده، خاصة بعد أن أثبت الواقع قيام بعض المبرمجين والمصنعين من استغلال الذكاء الاصطناعي فى ارتكاب العديد من الجرائم[4].

ونظرًا لأن الخوارزميات الذكية لا تتطلب مستويات عالية من المعرفة، كما يسهل الحصول عليها كونها مفتوحة المصدر، وهو ما يسهل استخدامها من قبل المنظمات الإرهابية بشكل مباشر، وفى السنوات الأخيرة تحول نشاط المجموعات الإرهابية عن الأساليب التقليدية، وبدأت فى السعى نحو الاستفادة من التكنولوجيا فى تنفيذ

---

(1) Hallevy, Gabriel (2010) "The Criminal Liability of Artificial Intelligence Entities,op.cit,P.172.

(2) Shasha Yu and Fiona Carroll, Implications of AI in National Security: Understanding the Security Issues and Ethical Challenges, In: Reza Montasari, Hamid Jahankhani Artificial Intelligence in Cyber Security: Impact and Implications Security Challenges, Technical and Ethical Issues, Forensic Investigative Challenges,p.158

(3) Bhatnagar S, Cotton T, Brundage M, Avin S, Clark J, Toner H, Eckersley P, Garfinkel B, Dafoe A, Scharre P, Zeitzoff T, Filar B, Anderson H, Roff H, Allen GC, Carrick JS, Sèan F, Hèigeartaigh O, Beard S, Belfield H, Farquhar S, Lyle C, Crootof R, Evans O, Page M, Bryson J, Yampolskiy R, Amodei D (2018) The Malicious use of artificial intelligence: forecasting, prevention, and mitigation authors are listed in order of contribution design direction, vol 101,Avilable at: https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf

(4) محمد أبو المعاطى صقر، وفاء، المسئولية الجنائية عن جرائم الذكاء الاصطناعي، مرجع سابق، ص7.

مخططاتها[1] ومن هنا تتضح مدى العلاقة التى تربط الذكاء الاصطناعي بالإرهاب بوجه عام وبشكله الإلكتروني بوجه خاص.

نظرًا لما تسببه الأعمال الإرهابية من خسائر بشرية ومادية، فضلًا عن أنها تشكل أكبر تهديد لأمن واستقرار المجتمعات، لذا حرصت كافة الدول على مستوى العالم على سن تشريعات خاصة فى محاولة التصدى له والقضاء عليه، كما كانت قضية الإرهاب وما زالت . موضع اهتمام المجتمع الدولى،[2] على اعتبار أن الآثار الخطيرة للارهاب لا تتوقف عند حدود دولة بعينها.

ويبدو أن الجماعات الإرهابية قد اعتادت على التعايش فى كافة الظروف، واستغلال كل ما هو متاح فى تنفيذ مخططاتها الإجرامية، فمع التطور التكنولوجى الذي شهده العالم فى بدايات هذا القرن، بدأت الجماعات الإرهابية التخلى عن النهج التقليدى فى تنفيذ مخططاتها من خلال استغلال التكنولوجيا وتقنية المعلومات، ومن هنا ظهر مفهوم الإرهاب الإلكتروني.[3]

ويعتبر الإرهاب الإلكتروني من أخطر جرائم الفضاء الإلكتروني فى الوقت الحاضر، إذ يمثل تهديدًا مباشرًا لأمن المجتمع الدولى واستقراره، فقد استغلت الجماعات الإرهابية التقدم التقنى فى تنفيذ مخططاتها ونشر أفكار التطرف والكراهية، والتحريض على القتل، والتخريب، كما استغلت وسائل التواصل الاجتماعي[4] فى تجنيد الإرهابيين، والبحث عن مصادر لتمويل نشاطها الإجرامى، كما استطاعت أيضًا الاستعانة بالتقنيات فى تمويل أنشطتها بعدة طرق.[5]

مفهوم الإرهاب الإلكتروني: يرتبط الإرهاب الإلكتروني ارتباطًا وثيقًا بالإنترنت وأجهزة الحاسوب، وفى هذا الصدد ذهب البعض إلى تعريفه بأنه: "استخدام شبكة الإنترنت لنشر الخوف، أو التهديد به، أو لإحداث تغييرات سياسية"[6] على اعتبار أنه أخطر أنواع الجرائم المستحدثة التى أفرزتها شبكة الإنترنت.

(1) Gadi Eshed, Is the Chatbot a Threat or an Opportunity for Security Organizations?, Report Part Title: Unveiling the Dark Side of Artificial Intelligence, International Institute for Counter-Terrorism, 27 Aug.2023,p.6:7

(2) تعتبر اتفاقية جنيف لعام 1937 أول اتفاقية دولية تعنتى بمكافحة الإرهاب؛ الاتفاقية الأوروبية لقمع الإرهاب عام 1977م، الاتفاقية العربية لمكافحة الإرهاب، 1998م، اتفاقية الأمم المتحدة لمكافحة الإرهاب، الاتفاقية الدولية لمنع تمويل الإرهاب لسنة 1999م، للاطلاع على الصكوك الدولية فى مكافحة الإرهاب، راجع الرابط التالى، الزيارة 2023/10/9
https://www.un.org/counterterrorism/ar/international-legal-instruments

(3) سليمان الخربى، إبراهيم، الإرهاب المعلوماتى وتمويله فى النظام السعودى، مجلة مصر المعاصرة، السنة 110، العدد 534، الجمعية المصرية للاقتصاد السياسى والتشريع والإحصاء، القاهرة، يناير 2019م، ص266 وما بعدها.

(4) Brian Blakemore, Policing Cyber Hate, Cyber Threats and Cyber Terrorism, First Published, eBook Published21 April 2012,p.8:10

(5) السعيد القزعة، محمد، التمويل الإلكتروني للإرهاب

(6) Adam Henschke, Terrorism and the Internet of Things: Cyber-Terrorism as an Emergent Threat, In: Adam Henschke ,Alastair Reed · Scott Robbins · Seumas Miller, Counter-Terrorism, Ethics and Technology Emerging Challenges at the Frontiers of Counter-Terrorism, Springer,2021,p.73

كما عرف البعض الإرهاب الإلكتروني بأنه، هجمات غير مشروعة، أو تهديدات بهجمات ضد الحاسبات أو الشبكات أو المعلومات المخزنة إلكترونيًا، توجه من أجل الانتقام أو ابتزاز أو إجبار أو التأثير فى الحكومات أو الشعوب، أو المجتمع الدولي بأكمله، لتحقيق أهداف سياسية أو دينية أو اجتماعية معينة"[1].

وفى رأى آخر يعرف الإرهاب الإلكتروني بأنه، " كل فعل يقوم به فرد أو جماعة منظمة باستخدام وسائل تقنية المعلومات أو الشبكات المعلوماتية من شأنه إحداث ضرر أو تعريض مصلحة يحميها القانون لخطر تنفيذاً لمشروع إرهابي"[2].

الإرهاب الإلكتروني يتخذ من السلوك الإجرامى مجموعة من الصور، منها اقتحام وتدمير المواقع، تغيير محتوى المواقع أو الدخول على الشبكات والعبث بمحتوياتها لإزالتها أو الاستيلاء عليها أو الدخول على شبكات الاتصالات والمعلومات لتعطيلها عن العمل لأطول فترة ممكنة[3].

ومن أكثر وسائل الإرهاب الإلكتروني شيوعاً هو استخدام التنظيمات الإرهابية للبريد الإلكتروني لنشر أهدافها وثقافاتها وتجنيد الأعضاء، وكذلك إنشاء مواقع خاصة على الإنترنت لخدمة أهدافها، وكذلك استغلال مواقع التواصل الاجتماعي فى ترويج أفكارها وتجنيد الشباب[4].

وعلى هذا الأساس يعرفه البعض بأنه: "الاستخدام المتعمد للأعمال التهديدية والتخريبية، أو الهجمات التى تشن من خلال الحواسيب وشبكة الإنترنت والشبكات أو الأنظمة القائمة على التكنولوجيا ضد المعلومات والبيانات والهياكل الأساسية التى تدعمها النظم الحاسوبية والبرامج والشبكات من أجل إحداث ضرر أو تحقيق أهداف سياسية، أو للتأثير على الجمهور[5].

---

[1] د. هشام بشير، الإرهاب الإلكتروني فى ظل الثورة التكنولوجية وتطبيقاته فى العالم العربى، مجلة آفاق سياسية العدد 6، المركز العربى للبحوث والدراسات، يونيو 2014م، ص77

[2] د. فتيحة عمارة، وعبد الرحمن عوض رجا، جريمة الإرهاب المعلوماتى، مجلة جامعة الأمير عبد القادر للعلوم الإسلامية– المجلد 34، العدد 1، قسنطينة، الجزائر، 2020م، ص1323.

[3] د. إسلام محروس ناجى، جرائم الإرهاب الإلكتروني دراسة تأصيلية تحليلية للتشريع السعودى، مجلة القانون والاقتصاد، ملحق العدد 93، كلية الحقوق، جامعة القاهرة، 2020م، ص50؛ إسراء طارق جواد كاظم الجابرى، جريمة الإرهاب الإلكتروني، دراسة مقارنة، رسالة ماجستير، كلية الحقوق، جامعة النهرين، العراق، 2012م، ص25 وما بعدها.

[4] باسل فايز حمد، المواجهة التشريعية لجرائم الإرهاب الإلكتروني: دراسة تحليلية، رسالة ماجستير، كلية الدراسات العليا، جامعة العلوم الإسلامية العالمية، الأردن، 2019م، ص55–56؛د. زين العابدين عواد كاظم، جرائم الإرهاب المعلوماتى دراسة مقارنة، الطبعة الأولى، منشورات الحلبى الحقوقية، بيروت، 2018م، ص79 وما بعدها؛ د. خالد حسن أحمد لطفى، الإرهاب الإلكتروني آفة العصر الحديث والآليات القانونية للمواجهة الطبعة الأولى دار الفكر الجامعى، الإسكندرية، 2018م، ص33–36، د. إبراهيم سليمان الحربى، الإرهاب المعلوماتى وتمويله فى النظام السعودي، مجلة مصر المعاصرة، مرجع سابق، ص280 وما بعدها.

[5] Mahmoud Eid, Cyber-Terrorism and Ethical Journalism A Need for Rationalism, University of Ottawa, Canada , 2012, P264;

وفى رأينا أن كافة ما تقدم من تعريفات على الرغم من اختلافها لفظًا إلا أن جميعها يتوافق فى المعنى والمضمون والمتمثل فى كون الإرهاب الإلكتروني سلوك إجرامى ينطوى على الاستخدام السيء للأجهزة الإلكترونية فى سبيل تنفيذ مخطط إرهابى أو تحقيق غرض يخدم مصالح الجماعات الإرهابية.

خصائص الإرهاب الإلكتروني وخطورته:

يختلف الإرهاب الإلكتروني عن الإرهاب التقليدى، ليس فقط فى وسيلة تنفيذ السلوك الإجرامى وإنما فى مجموعة من الخصائص التى يتميز بها الإرهاب الإلكتروني والتى تضاعف من خطورته على المجتمعات، وتتمثل تلك الخصائص فيما يلى:

- الإرهاب الإلكتروني لا يحتاج عند ارتكابه الى العنف والقوة بل يتطلب حاسب آلي متصل بالشبكة المعلوماتية ومزود ببعض البرامج اللازمة.[1]
- يتميز الإرهاب الإلكتروني بأنه جريمة إرهابية متعدية الحدود وعابرة للدول والقارات، وغير خاضعة لنطاق إقليمي محدود [2].
- صعوبة اكتشاف جرائم الإرهاب الإلكتروني ونقص الخبرة لدى بعض الأجهزة الأمنية والقضائية في التعامل مثل هذه الجرائم.[3]
- صعوبة الإثبات في الإرهاب الإلكتروني نظرًا لسرعة غياب الدليل الرقمي وسهولة إتلافه وتدميره.[4]
- يتميز الإرهاب الإلكتروني بأنه يتم بتعاون أكثر من شخص على ارتكابه.
- مرتكب جريمة الإرهاب الإلكتروني يكون من ذوي الاختصاص في مجال تقنية المعلومات أو من شخص لديه على الأقل قدر من المعرفة والخبرة في التعامل مع الحاسب الآلي والشبكة المعلوماتية. [5]

وفى مجال التصدى للإرهاب الإلكتروني هناك العديد من الاتفاقيات الدولية التى تجرم هذا السلوك وتضع مجموعة من التدابير لمكافحته، وعلى المستوى العربي تم إبرام الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ونصت الاتفاقية على مجموعة من التدابير فى سبيل التصدي لهذه الظاهرة[6].

ولا شك أن خطورة الإرهاب الإلكتروني تتزايد بمرور الوقت خاصة مع التطور الهائل الذي تشهده أنظمة الذكاء الاصطناعي، وظهور ما يعرف بإنترنت الأشياء،[7] حيث إن الأخير يعتمد على الأول فى التشغيل والبيانات

(1) Adam Henschke, Terrorism and the Internet of Things:Cyber-Terrorism, op.cit ,p.74

(2) طارق جواد الكاظمى، إسراء، جريمة الإرهاب الإلكتروني، دراسة مقارنة، رسالة ماجستير، كلية الحقوق، جامعة النهرين، العراق، 2012م، ص36.

(3) يوسف كافي، مصطفى، جرائم "الفساد، غسيل الأموال، السياحة، الإرهاب الإلكتروني، المعلوماتية"، الطبعة الأولى، مكتبة المجتمع العربي للنشر، والتوزيع، عمان، الاردن، 2014، من ص 143 وما بعدها.

(4) أحمد، رانية محمد طاهر، أثر الذكاء الاصطناعي على الأمن الدولي، مرجع سابق، ص246.

(5) حسن يوسف، يوسف، الجرائم الدولية للإنترنت، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2011م، ص135.

(6) مجاهد، توفيق، جريمة الإرهاب الإلكتروني فى ضوء الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010م، مجلة العلوم القانونية والسساسية، المجلد 9، العدد3، الجزائر، 2013م، ص89.

(7) إنترنت الأشياء مصطلح يطلق للدلالة على الآلات التى ترتبط بعضها والبعض الآخر من خلال شبكة الإنترنت، وتعرف بالأجهزة الذكية، ومن أمثلتها المنازل الذكية والمدن الذكية، والتلفاز الذكى.

ويؤكد البعض على أن هذا النوع من التقنية يفتقد الأمان، وممكن السيطرة عليه عن بعد، وهو الأمر الذي يثير القلق من ازدياد وتيرة الإرهاب السيبرانى.[1]

المبحث الثاني

سبل استخدام الذكاء الاصطناعي من قبل الجماعات الإرهابية

أثار التطور الهائل فى تقنيات الذكاء الاصطناعي إلى ارتفاع وتيرة القلق لدى الكثيرين، الأمر الذي دعا كبار المتخصصين فى هذا المجال إلى التحذير من خطورة السماح بتطوير تقنيات الذكاء الاصطناعي على البشرية ويربط البعض بين تطور الذكاء الاصطناعي وبين الإرهاب الإلكتروني، خاصة بعد أن استطاعت الجماعات الإرهابية استخدام تقنيات الذكاء الاصطناعي فى شن الهجمات.

فلا شك أن استخدام الذكاء الاصطناعي من قبل الجماعات الإرهابية في تحديث الأسلحة الإلكترونية، سيؤدى إلى شل قدرة الدولة على صد هذه الهجمات، ويزيد من تفاقم المخاطر الأمنية.[2] ويزداد التخوف من وصول الأسلحة الإلكترونية الفتاكة إلى أيدى الجماعات الإرهابية.

وفى مصر حذر مرصد الأزهر من مخاطر استغلال تقنيات الذكاء الاصطناعي فى نشر التطرف والإرهاب واعتبر أن المشكلة الحقيقية تكمن في أن هذا العقل الآلي الذي يُعد بمنزلة محاكاة للعقل البشري، يتغذى بروافد مصطنعة، قد تقود في النهاية لنتائج قويمة تنفع البشرية، أو سقيمة تضر بسلامة الحياة على كوكب الأرض الذي نحيا عليه، وعلى البشرية أن تتنبه لمخاطر الاستغلال السيئ لهذه التقنيات الحديثة في مجال الحروب، والصراعات.[3]

والحقيقة . فى رأينا _ أن مخاطر استغلال الذكاء الاصطناعي من قبل الجماعات الإرهابية له ما يبرره فى ظل سباق التسلح بين الدول الكبرى بهدف الاستحواذ على تقنيات تطوير الأسلحة الفتاكة التى تعمل بالذكاء الاصطناعي التوليدي وهو ما ورد صراحة فى تصريح الرئيس الروسى حينما قال إن من يكسب سباق الذكاء الاصطناعي سيستطيع أن يسيطر على العالم، ولا يقلل من هذه المخاطر الدعوى بأن هذه الأسلحة من الصعب وصولها إلى الجماعات الإرهابية، فهذا الادعاء لا يغير شيئاً خصوصًا مع تورط بعض الدول وأجهزة المخابرات فى دعم الإرهاب.[4]

---

(2) Adam Henschke, Terrorism and the Internet of Things:Cyber-Terrorism, op.cit, p.75 :78

(2) جمال عبد السلام زهران، سحر، الجوانب القانونية الدولية لجريمة الإرهاب الإلكتروني، مجلة السياسة والاقتصاد، العدد الرابع، كلية الاقتصاد والعلوم السياسية، جامعة بنى سويف، مصر، 2019م، ص66 وما بعدها.

(3) مخاطر استغلال الذكاء الاصطناعي في نشر التطرف والإرهاب، 2023/2/21م، مرصد الأزهر لمكافحة التطرف، رابط الموقع على شبكة المعلومات الدولية، تاريخ الزيارة، 2023/10/10م.

(4) توماس سواريز، دولة الإرهاب، ترجمة، عصفور، محمد، مجلة عالم المعرفة، العدد 460، الكويت، مايو 2018م

وقد حذر أحد كبار المتخصصين فى مجال الذكاء الاصطناعي من النهج المتسارع فى تطوير تقنيات الذكاء الاصطناعي معتبرًا أن ذلك سيؤدى إلى كارثة،[1] حيث أكد على أن الروبوتات ستؤدى كل ما يؤديه البشر وبشكل أسرع وأفضل، واستمرار سباق التسلح العالمي فى هذا المجال سوف يتسبب فى اندلاع الحرب العالمية الثالثة.

- **الحرب السيبرانية**:

الحرب السيبرانية عبارة عن هجمات إلكترونية تستهدف الحاسب الآلي، ومن خلالها يمكن شل البنية المعلوماتية، وهو الأمر الذي يؤدى إلى كم هائل من الخسائر بمختلف أنواعها، خاصة حينما تستهدف الهجمات البنية التحتية، وقطع أنظمة الاتصالات، كما قد تؤدى إلى مسح كامل للمعلومات والبيانات، وقد تقوم الجماعات الإرهابية باستئجار شبكات الروبوت لتنفيذ مثل هذه الهجمات.[2]

وتجدر الإشارة إلى أن الدول المتقدمة أكثر عرضة لهذه الهجمات الإرهابية، حيث ترتبط بنيتها التحتية بالحواسيب الآلية والشبكات المعلوماتية، مما يجعلها هدفاً سهل المنال، فبدلاً من استخدام المتفجرات تستطيع الجماعات الإرهابية من خلال الضغط على لوحة المفاتيح تدمير البنية المعلوماتية، وتحقيق آثار تدميرية تفوق مثيلتها المستخدم فيها المتفجرات، حيث يمكن شن هجوم إرهابي لإغلاق المواقع الحيوية وإلحاق الشلل بأنظمة القيادة والسيطرة والاتصالات، أو قطع شبكات الاتصال بين الوحدات والقيادات المركزية، أو تعطيل أنظمة الدفاع الجوي أو إخراج الصواريخ عن مسارها، أو التحكم في خطوط الملاحة الجوية والبحرية، أو اختراق النظام المصرفي وإلحاق الضرر بأعمال البنوك وأسواق المال.[3]

تتخذ الحرب السيبرانية ثلاث صور وهى: مهاجمة شبكات الحاسب الآلي عن طريق اختراق الشبكات وتغذيتها بمعلومات محرفة، تؤدى لإرباك المستخدمين، ونشر الفيروسات لتعطيل الشبكة، أو الدفاع عن الشبكات من خلال تأمين سبل الحماية من قبل حراس الشبكات، من خلال تطبيقات ذكية تراقب الزائرين غير المرغوب بهم والتعرف على هويتهم، فضلًا عن إجراء مسح شامل بصفة دورية بحثًا عن الفيروسات والألغام السيبرانية[4] والكشف عنها، وأخيرا قد تكون الحرب السيبرانية فى صورة استطلاع لشبكات الحاسب والقدرة على الدخول إليها بطريق غير مشروع فى محاولة للتجسس، أو الحصول على بيانات أو أسرار عسكرية، أو معلومات استخباراتية، ومن خلال هذه الوسيلة تستطيع الجماعات الإرهابية التعرف على الخطط الأمنية واختيار موعد الهجوم ومكانه.

---

[2] Catherine Clifford , 9 of the most Jaw-dropping things Elon Musk said about robots and alien 2017 , article , Nov 27 , 2017 , available at: https://www.cnbc.com/2017/12/18/9-mind-blowing-things-elon-musk-said-about-robots-and-ai-in-2017.html, accessed,7/10/2023; Deborah Housen-Couriel, The Evolving Law on Cyber Terrorism:: Dilemmas in International Law and Israeli Law, International Institute for Counter-Terrorism (ICT) 2013,p.5:8

[2] عبد المجيد، ريم، تطبيقات الذكاء الاصطناعي وظاهرة الإرهاب، مرجع سابق، ص150

[3] راجى يوسف محمود، البياتى، الإرهاب السيبرانى، نماذج من الجهود الدولية، مرجع سابق، ص90

[4] محمد طاهر أحمد، رانية، أثر الذكاء، مرجع سابق، ص266

وبعض الهجمات السيبرانية قد تؤدى إلى أخطار كارثية، ومن أبرز الأمثلة على ذلك فيروس ستاكسنت الذي طورته الولايات المتحدة بمساعدة إسرائيل[1] لشن هجوم على المواقع النووية فى إيران عام 2010م. ومن قبيل الحروب السيبرانية أيضًا قيام الجماعات الإرهابية باستخدام تقنيات برامج الفدية فى تدمير الشبكات أو حذف البيانات بالكامل.[2] وتقوم فكرة الفدية على مجموعة فرعية من البرامج الضارة تؤدى إلى تشفير ملفات الضحايا وفى مقابل إعادة التشغيل يتم طلب فدية من الضحايا، وهى وسيلة واسعة الانتشار فى الولايات المتحدة.[3]

يتضح مما تقدم أن الأمن الإلكتروني يعتبر أحد أهم المجالات التى يمكن تهديدها بتقنيات الذكاء الاصطناعي وكذلك قد تستخدم أنظمة الذكاء الاصطناعي من جهات خارجية لأساليب التدخل فى الشبكات، كما حدث فى الانتخابات الأمريكية عام 2016م.[4]

- **تقنية الخداع العميق:**

التزييف العميق هو نوع من الوسائط الاصطناعية التي تم اختراعها في عام 2017. وهي تنطوي على استخدام تقنيات الذكاء الاصطناعي للتلاعب أو إنشاء محتوى مرئي ومسموع مزيف لا يستطيع البشر أو حتى الحلول التكنولوجية أن تميزه عن المحتوى الأصيل على الفور.[5]

فمن خلال هذه التقنية يتم إنتاج مقاطع فيديو ونسبتها إلى أشخاص، وتعد من أخطر وسائل التضليل المعلوماتى[6]

ومن خلال الذكاء الاصطناعي يمكن التلاعب عبر وسائل التواصل الاجتماعي بشكل يؤثر على الرأى العام، ففى انتخابات الفلبين عام 2022حصل ماركوس على فوز ساحق فى الانتخابات، وكان قد جرى أثناء الانتخابات استخدام برنامج (تيك توك) فى نشر معلومات مضللة.[7]

- **استغلال الذكاء الاصطناعي فى تمويل الإرهاب إلكترونيًا:** يعتبر التمويل الإلكتروني للإرهاب صورة من صور الجرائم المستحدثة التى نتجت عن سوء استغلال التقدم العلمي فى مجال تقنية المعلومات.[8] واعتبر بعض رجال الفقه أن التمويل الإلكتروني للجماعات الإرهابية قد تنامى لدرجة وصفه بالاقتصاد الإرهابى، خاصة مع

---

3 https://www.bbc.com/arabic/worldnews/2011/01/110116_us_iran_israel_stuxnet_nuke

[2] Andy Greenberg. (Aug. 22, 2018). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Wired. Accessible at https://

[3] كريس ويلش، الجانب المظلم للتكنولوجيا، مجلة التمويل والتنمية، مرجع سابق، ص16

[4] اوسوندا. أ أوسوبا، ويليام ويلسر الرابع، مخاطر الذكاء الاصطناعي على الأمن ومستقبل العمل، مؤسسة راند، منشور على الإنترنت الزيارة 2023/10/9م. ص 5

2 Oscar Schwartz.. The Guardian. You thought fake news was bad? Deep fakes are where truth goes to die, (Nov. 12, 2018). Accessible at https://www.theguardian.com/technology/2018/nov/12/deep-fakes-fake-news-truth

[6] محمد طاهر أحمد، رانية، أثر الذكاء الاصطناعي، مرجع سابق، ص250

[3] Gadi Eshed, Is the Chatbot a Threat or an Opportunity for Security Organizations, op.cit, p.6

[8] فكرى إدريس، محمد، المواجهة الجنائية لاستخدام تقنية المعلومات فى ارتكاب جرائم المخدرات، المجلة الجنائية القومية، المجلد 63، العدد2، المركز القومى للبحوث الاجتماعية والجنائية، القاهرة، يوليو 2020م ص73.

الانتشار الواسع لاستخدام الإنترنت فى تمويل الإرهاب فى العديد من الدول الأوروبية، مع وجود دعم من مؤسسات وهيئات إعلامية كبرى.((1))

ومن خلال التكنولوجيا الرقمية يمكن نقل الأموال عبر الحدود بطرق غير مشروعة، ومن خلال استغلال الذكاء الاصطناعي يمكن التلاعب بأنظمة الحاسب لتسهيل ذلك، وفى الغالب تتجه الجماعات الإرهابية لاستخدام العملات المشفرة.(2)

- **الطائرات دون طيار:**

الطائرات بدون طيار هي مركبات محمولة جواً يتم توجيهها عن بعد أو مبرمجة مسبقًا أو يتم التحكم فيها. ويشار إليها أيضًا باسم المركبات الجوية بدون طيار، أو (الدرون)، وقد استُخدمت لأول مرة خلال الحرب العالمية الأولى ثم تطورت بشكل أكبر خلال الحرب الباردة، تم وصف الصراع الحالي بين روسيا وأوكرانيا بأنه "أول حرب واسعة النطاق بطائرات بدون طيار.(3)

وقد تمكنت بريطانيا من إنتاج طائرة بدون طيار ذاتية التشغيل، وتم تصميم الطائرة لتنفيذ المهام دون تدخل بشرى، فى جميع وسائل التنقل، وتم تزويدها بالقدرات الهجومية وكذلك مجهزة بإمكانيات تسهل لها المراوغة وتفادى الهجمات،(4) وقد استطاعت الصين إنتاج طائرة بدون طيار بتكلفة لا تتجاوز 200 دولار تملك القدرة على التحرك فى سرب أو بطريقة مستقلة، وهو الأمر الذي يوفر للجماعات الإرهابية بديلًا عن استخدام العنصر البشري فى تنفيذ الهجمات وقد تمكنت الجماعات الإرهابية فى العراق من تملك هذه النوعية من الطائرات وقامت بتزويدها بقنابل لمهاجمة القوات العراقية(5)، وقد استخدم ذات الأسلوب من قبل جماعة الحوثى فى شن هجمات على بعض المنشآت البترولية فى المملكة العربية السعودية،(6) وفى عام 2015 قامت طائرة بدون طيار وهى محملة بمواد مشعة من استهداف مكتب رئيس الوزراء اليابانى.(7) وفى عام 2018 كانت هناك محاولة لاغتيال الرئيس الفنزويلى نيكولاس مادوروا كما تعرض رئيس الوزراء العراقى لمحاولة اغتيال عام 2021م.

والحقيقة أن حصول الإرهابيين على هذه الطائرات يتم بسهولة، نظرًا لافتقاد الأسواق المدنية للتنظيم والرقابة فى هذا المجال، وفى كثير من الأحيان تلجأ الجماعات الإرهابية إلى مواقع الويب المظلم، وهى ساحة لارتكاب العديد من الجرائم.(8)

---

(1) عبد المجيد، مها، استعمال الإنترنت فى تمويل الإرهاب وتجنيد الإرهابيين، المجلة الجنائية القومية، المجلد 53، العدد 3، المركز القومى للبحوث الجنائية، القاهرة، نوفمبر 2010م،ص192.

(2) محمد طاهر أحمد، رانية، أثر الذكاء الاصطناعي، مرجع سابق، ص253

3 Christina Schori Liang," Terrorist Digitalis: Preventing Terrorists from Using Emerging Technologies,op.cit,p.72

(4) العشاس، إسحاق، نظم الأسلحة المستقلة، مرجع سابق، ص152

(5) عبد المجيد، ريم، مرجع سابق، تطبيقات الذكاء الاصطناعي، مرجع سابق، ص158

(6) محمد طاهر أحمد، رانية، أثر الذكاء، مرجع سابق، ص257

6 Gadi Eshed, Is the Chatbot a Threat or an Opportunity, op.cit,p.6

(8) حسن الموكلى، أحمد، بناء واختبار بوابة معلومات لجمع وتحليل المحتوى، مرجع سابق، ص8: 9.

وتستطيع الجماعات الإرهابية ارتكاب جرائم الاغتيال السياسى من خلال استخدام هذه الطائرات أو ما يعرف بالريبوت القاتل، إذ يتم ذلك بمجرد التقاط صورة للشخص المستهدف وعنوانه، وتحميلها على جهاز الروبوت القاتل ليتعرف عليها، بعد ذلك ينتقل الروبوت إلى وجهته وينفذ عملية الاغتيال، دون إمكانية التعرف على الفاعل.[1]

ويفرق البعض بين ثلاثة أنواع من الروبوتات: النوع الأول وتقتصر قدراته على اختيار الأهداف ومهاجمتها تحت رقابة وسيطرة بشرية من قبل المشغل، والثانى يتمثل فى الروبوتات التى تستطيع اختيار الأهداف وإصابتها تحت إشراف المشغل الذي يستطيع تغيير الهدف أو إبطال أداء الروبوت، أما النوع الثالث وهو الأخطر فهى روبوتات تعمل باستقلال كامل.[2]

وتتزايد قدرات هذه الطائرات من حيث المدى والدقة، تمكن الجماعات الإرهابية من ضرب أهداف بعيدة، حيث يمكن للطائرات بدون طيار السفر لمسافة تصل إلى 1500 كيلومتر، وهي مثالية للهجمات على الأهداف العسكرية في عمق أراضي الدولة. كما أن البنية التحتية المدنية، الواقعة بعيدًا عن مناطق النزاع، أصبحت الآن معرضة للخطر بشكل متزايد.[3]

منذ عام 2020، تم استهداف البنية التحتية للطاقة، والشحن الدولي، والمطارات الدولية، والمدن الكبرى بواسطة الطائرات بدون طيار، ومن هنا يعد استخدام الطائرات بدون طيار أحد أبرز التهديدات الإرهابية، وفقًا لما أكدته لجنة مكافحة الإرهاب التابعة لمجلس الأمن الدولى، ومع قابلية هذه الطائرات للتسليح تزداد الخطورة،[4] وهو الأمر الذي يفرض على الدول ضرورة اتخاذ التدابير التى تمكنها من المحافظة على أمنها القومى.[5]

من خلال ما سبق اتضح إلى أى مدى يمكن أن يشكل استغلال الذكاء الاصطناعي فى خدمة الإرهاب عاملًا رئيسيًا فى تدمير المجتمعات وزعزعة الاستقرار فى أى دولة، وهو ليس ببعيد عن عالمنا العربي، بل إن الدول العربية عرضة لهذا النوع من الإرهاب فى ظل المؤامرات الدولية التى تحاك ضدها، ولا يمكن التسليم بأن الدول المتقدمة هى الأكثر عرضة لهذا الخطر لأنها تربط بنيتها التحتية بالنظم الإلكترونية، فكافة الدول العربية تسعى الآن جاهدة إلى تبنى سياسة التحول الرقمى، وبدأت العديد من المؤسسات فى تطبيق نظام الحكومة الإلكترونية، ومعنى هذا أن كافة هذه المؤسسات عرضة لهجمات إرهابية من هذا النوع وهو الأمر الذي يستدعى

---

(1) عبد المجيد، ريم، تطبيقات الذكاء الاصطناعي، مرجع سابق، ص160.

(2) سلطان الشادى، سما، الأسلحة ذاتية التشغيل، مرجع سابق، ص346 وما بعدها.؛ حسن، خالد عبد العال، المسؤلية الدولية، مرجع سابق، ص259.

1 Christina Schori Liang, op.cit, p.75

2 PUBLICATIONS Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes, United Nations Interregional Crime and Justice Research Institute (UNICRI), 2021 p.7: 8 https://unicri.it/News/Algorithms-Terrorism-Malicious-Use-Artificial-Intelligence-Terrorist-Purposes

3 Shasha Yu and Fiona Carroll, Implications of AI in National Security: Understanding the Security Issues and Ethical Challenges, op.cit, 159 -160,

اليقظة. من ناحية أخرى فإن أجهزة المخابرات التى تتبع دولًا تدعم الإرهاب بإمكانها الدفع فى هذا الطريق الخطر فى محاولة لزعزعة النظام السياسى، أو تعريض أمن المواطنين للخطر، ولكل هذه الأسباب يجب الاستعداد الأمنى لكل هذه المخاطر.

خاتمة

من خلال هذه الورقة تعرضنا لإلقاء الضوء على مخاطر الذكاء الاصطناعي وعلاقته بالإرهاب الإلكتروني وعلى الرغم من أن هذا الموضوع يعد من أكثر الموضوعات الجديرة باهتمام الباحثين، وهو ما يستدعى تناوله باستفاضة وتحليل أعمق، إلا أننا حاولنا قدر المستطاع الإلمام بعناصره الرئيسية، بعد مطالعة أحدث المؤلفات والأبحاث التى تتصل بالموضوع، فى محاولة وضع تصور عام، ومن هنا جاء تقسيم الورقة إلى مقدمة تناولنا فيها التعريف بالذكاء الاصطناعي وأنواعه وخصائصه، وعرضنا لمقدار الفجوة بين عالمنا العربي ودول الغرب فى مجال إنتاج وصناعة تقنيات الذكاء الاصطناعي، ثم قسمنا دراسة الموضوع الأساسى لمبحثين: تناول الأول التعريف بالإرهاب الإلكتروني وخطورته، وخصصنا الثانى لدراسة سبل استخدام الذكاء الاصطناعي فى تنفيذ الهجمات الإرهابية، ومن خلال هذه الدراسة استخلصنا مجموعة من النتائج والتوصيات، نعرض لها على النحو التالى:

النتائج :

- على قدر إسهامات الذكاء الاصطناعي فى خدمة البشرية فى العديد من المجالات إلا أنه فى ذات الوقت يشكل تهديدًا للأمن والاستقرار
- هناك سباق تسلح يستهدف تطوير آليات وتقنيات الذكاء الاصطناعي فى المجالات العسكرية
- هناك العديد من تقنيات الذكاء الاصطناعي الذي لا تكلف كثيرًا فى إنتاجها وهو ما يسهل استحواذ المنظمات والجماعات الإرهابية عليها.
- إن نجاح المنظمات الإرهابية فى تنفيذ مخططاتها الإرهابية باستخدام الذكاء الاصطناعي من شأنه أن يؤدى إلى مخاطر كارثية.
- إن الدول التى تدعم الإرهاب سيصبح لها دور فاعل فى إمداد الجماعات الإرهابية بالإسلحة الذكية شديدة الفتك.
- هناك فجوة واسعة فى مجال صناعة وإنتاج تقنيات الذكاء الاصطناعي بين عالمنا العربي والعديد من الدول الأخرى.

التوصيات:

- على الدول العربية ألا تكتفى بدور المستهلك لتقنيات الذكاء الاصطناعي.
- على المستوى الإقليمى لا بد من التعاون بين الدول العربية فى مجال تصنيع وإنتاج تقنيات الذكاء الاصطناعي حتى تتمكن من مواجهة التحديات.
- على المستوى المحلى يجب على كل دولة أن تتخذ كافة التدابير اللازمة للحفاظ على أمنها القومى وعليها فى سبيل ذلك، الاهتمام بالعناصر البشرية العاملة فى المجالات الأمنية والعمل على رفع كفاءتهم.
- فى كل القطاعات الأمنية والقضائية يجب الاستعانة بالخبراء وذوى الكفاءة فى تخصصات الذكاء الاصطناعي.
- لا بد من البحث عن آلية يمكن من خلالها الموازنة بين حقوق الأفراد فى السرية وبين حق الدولة فى ضمان الأمن والاستقرار ومكافحة الجريمة.

المصادر والمراجع

1. عبد النور عبد النور، عادل، مدخل إلى عالم الذكاء الاصطناعي، مدينة الملك عبد العزيز للعلوم والتقنية، المملكة العربية السعودية، 1426هـ، 2005م
2. خليفة، إيهاب، هيمنة الآلات:دورة حياة الذكاء الاصطناعي من الإدراك إلى تهديد البشر، 8 يناير، 2019، مركز المستقبل للدراسات والأبحاث المتقدمة، متاح على الرابط التالى، بشبكة المعلومات الدولية، تاريخ الدخول، 2023/10/8م. https://futureuae.com/ar-AE/Mainpage/Item/4451
3. أندرو بيرغ وإدوارد بايف ولويس–فليبي زانا، الروبوت والنمو وعدم المساواة، مجلة التمويل والتنمية، عدد سبتمبر 2016م، صندوق النقد الدولي. متاح على الرابط التالي، تمت الزيارة 2023/10/8م https://www.imf.org/external/arabic/pubs/ft/fandd/2016/09/pdf/berg.pdf
4. الشادى، سما سلطان، بعض التحديات التي تثيرها أنظمة الأسلحة الفتاكة ذاتية التشغيل على الصعيدين القانون والأخلاقي، المجلة القانونية والقضائية، السنة 14، العدد2، وزارة العدل القطرية، 2020م.
5. أحمد، رانية محمد طاهر، أثر الذكاء الاصطناعي على الأمن الدولى، مجلة البحوث المالية والتجارية، العدد 3،كلية التجارة، جامعة بورسعيد، يوليو 2020م.
6. عباس، علا غازى فرحان، أسلحة الذكاء الاصطناعي فى ظل مبادئ القانون الدولى الإنسانى، مجلة الميزان للدراسات الإسلامية والقانونية، المجلد 9، عدد3،عمادة البحث العلمي، جامعة العلوم الإسلامية العالمية، عمان، الأردن، أيلول، 2022م.
7. عبد الله كريم، سلام، التنظيم القانونى للذكاء الاصطناعي، رسالة دكتوراه، كلية القانون، جامعة كربلاء، العراق، 2022م.
8. العميريين، وجيه محمد سليمان، الذكاء الاصطناعي في التحري والتحقيق عن الجريمة: دراسة مقارنة، مجلة الميزان للدراسات الإسلامية والقانونية، المجلد9، العدد3، جامعة العلوم الإسلامية العالمية – عمادة البحث العلمي، عمان، الأردن، أيلول،2022م.
9. سعد الدين محمد سعيد، وليد، المسؤولية الجنائية الناشئة عن تطبيقات الذكاء الاصطناعي، مجلة العلوم القانونية والاقتصادية، المجلد 64، العدد2، كلية الحقوق، جامعة عين شمس، يوليو2022م.
10. جلسة استماع في الكونجرس الأمريكي، اللجنة الفرعية للاستخبارات ومكافحة الإرهاب، لجنة الأمن القومى متاح على الرابط التالى بشبكة المعلومات الدولية، الزيارة 2023/10/9م. https://www.congress.gov/116/chrg/CHRG-116hhrg38781/CHRG-116hhrg38781.pdf

11. محمد أبو المعاطي صقر، وفاء، المسؤولية الجنائية عن جرائم الذكاء الاصطناعي، دراسة تحليلية، مجلة روح القوانين، العدد 96، كلية الحقوق، جامعة طنطا، أكتوبر 2021م.
12. عباس، علا غازى فرحان، أسلحة الذكاء الاصطناعي في ظل مبادئ القانون الدولي الإنساني، مجلة الميزان للدراسات الإسلامية والقانونية، مجلد 9، العدد3،عمادة البحث العلمي، جامعة العلوم الإسلامية العالمية، أيلول، 2022م.
13. عبد المجيد، ريم، تطبيقات الذكاء الاصطناعي وظاهرة الإرهاب، مجلة شئون دبلوماسية، مجلد 4، العددين 6 و7، معهد الدراسات الدبلوماسية، الجامعة البريطانية الليبية، يوليو 2020م.
14. وفقاً للمؤشرات القياسية تستحوذ الولايات المتحدة على موقع الصدارة في سباق الذكاء الاصطناعي
15. دليل الذكاء الاصطناعي، البرنامج الوطنى للذكاء الاصطناعي، ص 21، منشور على موقع وزير الدولة للذكاء الاصطناعي والاقتصاد الرقمى، على الرابط التالى: الزيارة2023/10/8م. https://ai.gov.ae/ar/publications-2/
16. اتفاق سعودي صيني لبناء مصنع للطائرات بدون طيار بالمملكة، موقع قناة العربية على الإنترنت، بتاريخ 5 مارس 2022م الزيارة 2023/10/8م
17. القحطانى، عايض على، دور الذكاء الاصطناعي في تحقيق التنمية المستدامة في إطار رؤية المملكة العربية السعودية ٢٠٣٠،المجلة العربية للمعلومات وأمن المعلومات، المجلد 3، العدد 9، أكتوبر 2020م، المؤسسة العربية للتربية والعلوم والآداب.https://www.spa.gov.sa/a4ea79c31fm
18. حسن، خالد عبد العال إسماعيل، المسئولية الدولية عن جرائم الأسلحة المستقلة ذاتية التشغيل، مجلة القانون والتكنولوجيا، مجلد 2، العدد1، كلية القانون، الجامعة البريطانية، القاهرة، إبريل2022م.
19. اوسوندا. أ أوسويا، ويليام ويلسر الرابع، مخاطر الذكاء الاصطناعي على الأمن ومستقبل العمل، مؤسسة راند، منشور على الإنترنت الزيارة 2023/10/9م. file:///C:/Users/dr%20tark/Downloads/RAND_PE237z1.arabic%20(1).pdf
20. تعتبر اتفاقية جنيف لعام 1937 أول اتفاقية دولية تعتنى بمكافحة الإرهاب؛ الاتفاقية الأوروبية لقمع الإرهاب عام 1977م، الاتفاقية العربية لمكافحة الإرهاب، 1998م، اتفاقية الأمم المتحدة لمكافحة الإرهاب، الاتفاقية الدولية لمنع تمويل الإرهاب لسنة 1999م، للاطلاع على الصكوك الدولية فى مكافحة الإرهاب، راجع الرابط التالى، الزيارة 2023/10/9 https://www.un.org/counterterrorism/ar/international-legal-instruments
21. سليمان الخربى، إبراهيم، الإرهاب المعلوماتى وتمويله فى النظام السعودى، مجلة مصر المعاصرة، السنة 110، العدد 534، الجمعية المصرية للاقتصاد السياسى والتشريع والاحصاء، القاهرة، يناير 2019م.
22. السعيد القزعة، محمد، التمويل الإلكتروني للإرهاب
23. د. هشام بشير، الإرهاب الإلكتروني فى ظل الثورة التكنولوجية وتطبيقاته فى العالم العربي، مجلة آفاق سياسية العدد 6، المركز العربي للبحوث والدراسات، يونيو 2014م.
24. د. فتيحة عمارة، وعبد الرحمن عوض رجا، جريمة الإرهاب المعلوماتى، مجلة جامعة الأمير عبد القادر للعلوم الإسلامية– المجلد 34، العدد 1، قسنطينة، الجزائر، 2020م.

25.د. إسلام محروس ناجى، جرائم الإرهاب الإلكتروني دراسة تأصيلية تحليلية للتشريع السعودى، مجلة القانون والاقتصاد، ملحق العدد 93، كلية الحقوق، جامعة القاهرة، 2020م.
26.إسراء طارق جواد كاظم الجابرى، جريمة الإرهاب الإلكتروني، دراسة مقارنة، رسالة ماجستير، كلية الحقوق، جامعة النهرين، العراق، 2012م.
27. باسل فايز حمد، المواجهة التشريعية لجرائم الإرهاب الإلكتروني: دراسة تحليلية، رسالة ماجستير، كلية الدراسات العليا، جامعة العلوم الإسلامية العالمية، الأردن، 2019م
28.د. زين العابدين عواد كاظم، جرائم الإرهاب المعلوماتى دراسة مقارنة، الطبعة الأولى، منشورات الحلبى الحقوقية، بيروت، 2018م.
29.د. خالد حسن أحمد لطفى، الإرهاب الإلكتروني آفة العصر الحديث والآليات القانونية للمواجهة الطبعة الأولى دار الفكر الجامعى، الإسكندرية، 2018م
30.طارق جواد الكاظمى، إسراء، جريمة الإرهاب الإلكتروني، دراسة مقارنة، رسالة ماجستير، كلية الحقوق جامعة النهرين، العراق، 2012م.
31.يوسف كافي، مصطفى، جرائم "الفساد، غسيل الأموال، السياحة، الإرهاب الإلكتروني، المعلوماتية"، الطبعة الأولى، مكتبة المجتمع العربي للنشر، والتوزيع، عمان، الأردن، 2014.
32.حسن يوسف، يوسف، الجرائم الدولية للإنترنت، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة 2011م.
33.مجاهد، توفيق، جريمة الإرهاب الإلكتروني فى ضوء الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010م، مجلة العلوم القانونية والسساسية، المجلد 9، العدد3، الجزائر، 2013م.
34. جمال عبد السلام زهران، سحر، الجوانب القانونية الدولية لجريمة الإرهاب الإلكتروني، مجلة السياسة والاقتصاد، العدد الرابع، كلية الاقتصاد والعلوم السياسية، جامعة بنى سويف، مصر، 2019م.
35. مخاطر استغلال الذكاء الاصطناعي في نشر التطرف والإرهاب، 2023/2/21م، مرصد الأزهر لمكافحة التطرف، رابط الموقع على شبكة المعلومات الدولية، تاريخ الزيارة، 2023/10/10م.
36. توماس سواريز، دولة الإرهاب، ترجمة، عصفور، محمد، مجلة عالم المعرفة، العدد 460، الكويت، مايو 2018م
37.اوسوندا. أ أوسوبا، ويليام ويلسر الرابع، مخاطر الذكاء الاصطناعي على الأمن ومستقبل العمل، مؤسسة راند منشور على الإنترنت الزيارة 2023/10/9م.
38.فكرى إدريس، محمد، المواجهة الجنائية لاستخدام تقنية المعلومات فى ارتكاب جرائم المخدرات، المجلة الجنائية القومية، المجلد 63، العدد2، المركز القومى للبحوث الاجتماعية والجنائية، القاهرة، يوليو 2020م.
39.عبد المجيد، مها، استعمال الإنترنت فى تمويل الإرهاب وتجنيد الإرهابيين، المجلة الجنائية القومية، المجلد 53، العدد 3، المركز القومى للبحوث الجنائية، القاهرة، نوفمبر 2010م.

المراجع الإنجليزية

1. Adam Henschke, Terrorism and the Internet of Things: Cyber-Terrorism as an Emergent Threat, In: Adam Henschke ,Alastair Reed · Scott Robbins · Seumas Miller, Counter-Terrorism, Ethics and Technology Emerging Challenges at the Frontiers of Counter-Terrorism, Springer,2021.
2. Moritz Goldener, Cornelius Herstatt, Frank TIietze, "The emergence of care robotics – A patent and publication analysis", Technological Forecasting and Social Change, Vol. 92, March 2015, pp.115 et seq
3. Andy Greenberg. (Aug. 22, 2018). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Wired. Accessible at https://
4. Artificial Intelligence Index Report,2023, p.11,Avilable at : https://aiindex.stanford.edu/wp-content/uploads/2023/04/HAI_AI-Index-Report_2023.pdf
5. Bhatnagar S, Cotton T, Brundage M, Avin S, Clark J, Toner H, Eckersley P, Garfinkel B, Dafoe A, Scharre P, Zeitzoff T, Filar B, Anderson H, Roff H, Allen GC, Carrick JS, Sèan F, Hèigeartaigh O, Beard S, Belfield H, Farquhar S, Lyle C, Crootof R, Evans O, Page M, Bryson J, Yampolskiy R, Amodei D (2018) The Malicious use of artificial intelligence: forecasting, prevention, and mitigation authors are listed in order of contribution design direction, vol 101,Avilable at: https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf
6. Brian Blakemore, Policing Cyber Hate, Cyber Threats and Cyber Terrorism, First Published, eBook Published21 April 2012.
7. Catherine Clifford , 9 of the most Jaw-dropping things Elon Musk said about robots and alien 2017 , article , Nov 27, 2017 , available at: https://www.cnbc.com/2017/12/18/9-mind-blowing-things-elon-musk-said-about-robots-and-ai-in-2017.html, accessed,7/10/2023; Deborah Housen-Couriel, The Evolving Law on Cyber Terrorism:: Dilemmas in International Law and Israeli Law, International Institute for Counter-Terrorism (ICT) 2013.

8. Christian Montag, Harald Baumeister, Digital Phenotyping and Mobile Sensing New Developments in Psychoinformatics,2 Edition, SpringerNature Switzerland AG 2023.
9. Gadi Eshed, Is the Chatbot a Threat or an Opportunity for Security Organizations?, Report Part Title: Unveiling the Dark Side of Artificial Intelligence, International Institute for Counter-Terrorism, 27 Aug.2023.
10. Hallevy, Gabriel (2010) "The Criminal Liability of Artificial Intelligence Entities - from Science Fiction to Legal Social Control," Akron Intellectual Property Journal: Vol. 4 : Iss. 2 , Article 1.https://www.bbc.com/arabic/worldnews/2011/01/110116_us_iran_israel_stuxnet_nuke https://www.mcit.gov.sa/node/15
11. kevin warwick, Artificial Intelligence The Basics, First published 2012 by Routledge, USA, New York.
12. Luger G F. Artificial intelligence: structures and strategies for complex problem solving, 6th Ed, Pearson Education, Harlow, England , 2009.
13. Mahmoud Eid, Cyber-Terrorism and Ethical Journalism A Need for Rationalism, University of Ottawa, Canada , 2012.
14. Markus Anderljung and Paul Scharre, Society Must Get Ready for Very Powerful Artificial Intelligence,Foreign Affairs, August 14, 2023, At:https://www.foreignaffairs.com/world/how-prevent-ai-catastrophe-artificial-intelligence
15. Oscar Schwartz.. The Guardian. You thought fake news was bad? Deep fakes are where truth goes to die, (Nov. 12, 2018). Accessible athttps://www.theguardian.com/technology/2018/nov/12/deep-fakes-fake-news-truth
16. PUBLICATIONS Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes, United Nations Interregional Crime and

Justice Research Institute (UNICRI), 2021https://unicri.it/News/Algorithms-Terrorism-Malicious-Use-Artificial-Intelligence-Terrorist-Purposes

17. PUBLICATIONS Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes, United Nations Interregional Crime and Justice Research Institute (UNICRI), 2021https://unicri.it/News/Algorithms-Terrorism-Malicious-Use-Artificial-Intelligence-Terrorist-Purposes
18. Risks from Artificial Intelligence,University of Cambridg, at: https://www.cser.ac.uk/research/risks-from-artificial-intelligence ; /
19. Rofi Aulia Rahman, Rizki Habibulahو The Criminal Liability of Artificial Intelligence: Is It Plausible to Hitherto Indonesian Criminal System,? Legality : Jurnal Ilmiah Hukum, Vol. 27 No. 2 (2019).
20. Shasha Yu and Fiona Carroll, Implications of AI in National Security: Understanding the Security Issues and Ethical Challenges, In: Reza Montasari, Hamid Jahankhani Artificial Intelligence in Cyber Security: Impact and Implications Security Challenges, Technical and Ethical Issues, Forensic Investigative Challenges.