مجلـة مدارات سياسية
EISSN: 2710 - 8341 ISSN: 2588 - 1825
المجلد (10) / العــدد: (01)، (2026)
ص 180 - 202

مستقبل مكافحة الإرهاب في عصر الذكاء الاصطناعي: الآليات الرقمية وسياسات الردع الذكي

The Future of Counter-Terrorism in the Age of Artificial Intelligence: Digital Mechanisms and Smart Deterrence Policies

حكيم غريب [1]*، السعيد بن عزه[2]
[1] المدرسة الوطنية العليا للعلوم السياسية، (الجزائر)، gheriebhakim@gmail.com
[2]جامعة الشهيد حمة لخضر، الوادي، (الجزائر)، benazzasaid2019@gmail.com

تاريخ الاستلام: 2026/01/31 تاريخ قبول النشر: 2026/05/23 تاريخ النشر: 2026/06/08

ملخص:

يشهد العالم تحولًا نوعيًا في طبيعة التهديدات الإرهابية مع تطور التقنيات الرقمية وانتشار الذكاء الاصطناعي، الأمر الذي أدى إلى تعقيد أشكال التجنيد، والدعاية المتطرفة، وتمويل العمليات وتنسيقها عبر الفضاء السيبراني، وفي المقابل، أسهم الذكاء الاصطناعي في بناء آليات جديدة للرصد المبكر والتحليل الاستخباراتي العميق، من خلال تقنيات التعلم الآلي، ومعالجة البيانات الضخمة، والتعرف البيومتري، وتحليل شبكات التواصل. وقد سمحت هذه الأدوات بتوقع أنماط العنف والتطرف، وتتبع الخلايا الإرهابية العابرة للحدود، والتعرف على السلوكيات المشبوهة في الفضاء الرقمي ضمن منظومة ردع وقائي ذكي، غير أن هذا التحول يطرح تحديات قانونية وأخلاقية وتقنية، أبرزها: حماية الخصوصية، إدارة المخاطر المرتبطة بخوارزميات التنبؤ الأمني، ضعف التنسيق الدولي، واختلاف التشريعات الوطنية. وبناءً عليه، يتجه مستقبل مكافحة الإرهاب نحو بناء مزيج يجمع بين تقنيات الذكاء الاصطناعي وسياسات ردع سيبراني مرن، يعتمد على تعزيز التعاون الاستخباراتي الدولي، وتقوية قدرات الدول في مجال الحوكمة الرقمية، وتطوير منظومات ردع ذكية قائمة على الاستباق، لا على المواجهة التقليدية وحدها.

الكلمات مفتاحية: الذكاء الاصطناعي؛ مكافحة الإرهاب؛ التجنيد الرقمي؛ الرصد الاستباقي الردع السيبراني الذكي.

Abstract:

The rapid evolution of artificial intelligence (AI) and digital technologies has fundamentally reshaped the landscape of modern terrorism. Extremist groups increasingly exploit cyberspace for recruitment, ideological influence, financial transactions, and operational coordination, leveraging AI-driven tools such as behavioral analytics, identity masking, and automated propaganda. In response, governments and security agencies are adopting AI-enabled strategies to enhance predictive surveillance, biometric identification, and network analysis as part of a broader "smart deterrence" paradigm aimed at preventing attacks before they occur. This paper analyzes the interplay between AI and counterterrorism, examining the technological, ethical, and legal implications of AI-based security strategies. It further evaluates global practices in combating AI-enhanced terrorism and proposes a policy framework for sustainable "smart deterrence" that balances data governance, privacy protection, and international cooperation. The study concludes that the future of global security will depend on hybrid systems that integrate AI, ethical regulation, and collective digital intelligence to confront evolving terrorist threats.

Keywords: Artificial intelligence; counterterrorism; digital recruitment; proactive monitoring; intelligent cyber deterrence.

***المؤلف المرسل**

1. مقدمة :

يعرف العالم في الآونة الأخيرة تحولًا جذريًا في طبيعة التهديدات الإرهابية، سببها الانتشار الواسع لمختلف التقنيات الرقمية والذكاء الاصطناعي، حيث أصبحت الجماعات المتطرفة تستغل هذا الفضاء السيبراني للقيام بعمليات التجنيد والاستقطاب، ونشر الدعاية الرقمية، وتنظيم شبكات التمويل العابر للحدود، حيث استغلت التطور الخوارزمي في تحليل البيانات وإخفاء الهوية وخلق شبكات غير مرئية[1]، وفي المقابل، تتجه العديد من الدول والمؤسسات الأمنية إلى محاولة توظيف الذكاء الاصطناعي كوسيلة استراتيجية لمواجهة الإرهاب، من خلال تعزيز قدرات الرصد المبكر والتحليل الاستخباراتي والتنبؤ بالتحركات المحتملة للجماعات الإرهابية[2].

وبالنظر الى تزايد قوة التفاعل بين التقنية والأمن، أصبحت عملية مكافحة الإرهاب تتجاوز حدود المواجهة الأمنية التقليدية، إلى نماذج ردع ذكي تعتمد على التحليل التنبؤي، والبيانات الضخمة، والهوية البيومترية والسلوكية للفاعلين داخل الفضاء الرقمي[3]، غير أن هذا الاستخدام طرح عدة إشكالات تتعلق أساسا بحماية الخصوصية، وحقوق الإنسان، وسيادة البيانات الرقمية، الشيء الذي يجعل من توظيف الذكاء الاصطناعي في مواجهة الإرهاب موضوعًا معقدًا يتطلب توازنًا بين الأمن والحقوق القانونية[4] .

وانطلاقا من هذه المعطيات، تسعى هذه الدراسة إلى تحليل مستقبل مكافحة الإرهاب في ظل الذكاء الاصطناعي، واستشراف سياسات الردع الذكي التي يمكن للدول اعتمادها، ومن جانب آخر العمل على تحديد حدود الاستخدام الأمني للخوارزميات، وإمكانات التعاون الدولي في مواجهة الإرهاب المعزز بالتكنولوجيا.

1-1- مشكلة الدراسة:

يعرف مجال الأمن العالمي تغيير غير مسبوق بفضل تزايد اعتماد الجماعات الإرهابية على التقنيات الرقمية والذكاء الاصطناعي، فالفضاء السيبراني أصبح بيئة خصبة لنشاطات التجنيد والاستقطاب، ونشر الدعاية المتطرفة، وإدارة التمويل والاتصالات بسرية عالية وذلك عبر الخوارزميات وتقنيات إخفاء الهوية.

وقد شرعت مختلف الدول في توظيف الذكاء الاصطناعي كآلية لتعزيز قدراتها الأمنية سواء كان في الرصد والتحليل أو التنبؤ بالخطر، وهو ما يفتح الباب أمام نموذج متقدم من الردع الذكي القائم على الاستباق بدلًا من المواجهة التقليدية، إلا أن هذا التحول يثير إشكالات متعددة تتعلق بحدود استخدام الخوارزميات في الأمن، واحتمالات المساس بالخصوصية، وضعف الأطر القانونية المنظمة، إضافة إلى الحاجة الماسة للتعاون الدولي في مواجهة تهديدات رقمية عابرة للحدود، وبناء على هذه التحديات، يمكن ضبط مشكلة الدراسة من خلال التساؤل الرئيس: كيف يمكن للذكاء الاصطناعي أن يسهم في بناء سياسات ردع ذكي فعّالة في مكافحة الإرهاب، مع ضمان الحوكمة الرقمية وحماية الحقوق في المرحلة المقبلة؟

1-2-تساؤلات الدراسة:

يتفرع عن السؤال الرئيسي مجموعة من التساؤلات التي تسعى إلى توضيح أبعاد الظاهرة في سياقها الرقمي والأمني والقانوني. ومن ثم، يتناول البحث تساؤلًا حول أبرز التحولات التي أحدثها الذكاء الاصطناعي في طبيعة العمليات الإرهابية داخل الفضاء الرقمي،

بما في ذلك أساليب التجنيد والدعاية والتخفي. كما يستفسر عن أهم الآليات والتقنيات الرقمية التي يوفرها الذكاء الاصطناعي في مجال الرصد والتحليل والتوقع الأمني، باعتبارها أدوات استخبارية استباقية قادرة على الكشف المبكر عن الخطر، كما يطرح البحث تساؤلًا حول حدود الاستخدام الأمني للذكاء الاصطناعي من منظور قانوني وأخلاقي، وما إذا كان توسيع نطاق الرقابة الرقمية قد يمثل تهديدًا للخصوصية والحقوق الفردية. وعلى مستوى آخر، تتناول الدراسة تساؤلًا متعلقًا بصناعة القرار الأمني وهو: كيف يمكن للدول بناء سياسات ردع ذكي مستدامة تعتمد على الذكاء الاصطناعي مع ضمان الحوكمة الرقمية وحماية الحقوق؟

3-1 -فرضيات البحث:

هناك مجموعة من الفرضيات التي تمثل توقعات علمية أولية تهدف إلى توجيه مسار التحليل، حيث تعتبر الفرضية الأولى على الاعتقاد بأن الذكاء الاصطناعي يسهم في تعزيز فعالية الرصد الاستباقي والتنبؤ بالتهديدات الإرهابية بدرجة تفوق الوسائل الأمنية التقليدية، وذلك بفضل قدرته على تحليل كميات هائلة من البيانات في مدة زمنية وجيزة.

أما الفرضية الثانية فترى أن منظومات الردع الذكي المعتمدة على الذكاء الاصطناعي تزيد من قدرة الدول على تفكيك الشبكات الإرهابية العابرة للحدود، من خلال كشف الروابط الخفية وخطوط التواصل السرية التي يصعب رصدها بالطرق التقليدية، وتفترض الفرضية الثالثة أن قيود حماية الخصوصية وضعف الإطار القانوني الدولي يشكلان عائقين أساسيين أمام توظيف الذكاء الاصطناعي في مكافحة الإرهاب، خاصة في ظل غياب التشريعات الموحدة وشحّ الرقابة على الخوارزميات.

وتستند الفرضية الرابعة إلى أن تحقيق ردع سيبراني عالمي فعّال يتطلب تنسيقًا دوليًا واسعًا في مجالات تبادل البيانات، توحيد المعايير التقنية، وتطوير تشريعات مشتركة تضمن الاستخدام الآمن والمسؤول للتكنولوجيا. وأخيرًا، تفترض الفرضية الخامسة أن المستقبل الأمني العالمي يتجه نحو نموذج هجين يجمع بين الذكاء الاصطناعي والحوكمة الرقمية والسياسات القانونية الاستباقية، مما يسهم في بناء منظومة أمنية أكثر مرونة وقدرة على مواجهة الإرهاب الرقمي.

4-1-أهمية الدراسة:

تنبع أهمية هذه الدراسة من التحولات العميقة التي يشهدها المجال الأمني في ظل انتشار الذكاء الاصطناعي، وما يرافقه من انتقال الجماعات الإرهابية إلى فضاءات رقمية تستغل فيها الخوارزميات، والبيانات الضخمة، وتقنيات التخفي لصياغة أساليب جديدة في التجنيد والتمويل والتأثير، فهي تُسهم في تفسير التطور النوعي للإرهاب المعزّز بالتكنولوجيا، وفي إبراز دور الذكاء الاصطناعي بوصفه أداةً مركزية في بناء ردع استباقي ذكي قادر على توقع المخاطر قبل وقوعها، وتكتسب الدراسة أهميتها كذلك من تحليلها للتحديات القانونية والأخلاقية المرتبطة باستخدام الخوارزميات الأمنية، ومن سعيها إلى الموازنة بين مقتضيات الأمن الرقمي وحماية الحقوق والخصوصية الفردية. كما تُعد هذه الدراسة ذات قيمة علمية على مستوى صناع القرار والأجهزة الأمنية، لأنها تقدم تصورًا مستقبليًا حول سياسات الردع الذكي والتعاون الدولي في مكافحة الإرهاب الرقمي، بما يجعلها مرجعًا في فهم كيفية توظيف التكنولوجيا ضمن إطار أمني منظم ومستدام.

1-5-أهداف الدراسة: تهدف هذه الدراسة إلى:
*تحليل مستقبل التصدي للإرهاب في ظل التطور المتزايد لتقنيات الذكاء الاصطناعي، وهذا من خلال الكشف عن طبيعة التحولات التي طرأت على أساليب النشاط الإرهابي داخل الفضاء الرقمي، وتحديد الكيفية التي يمكن بها توظيف الخوارزميات والتقنيات الذكية في الرصد والتحليل والتنبؤ بالتهديدات.
*تسعى إلى تقويم فعالية الذكاء الاصطناعي كأداة للردع الاستباقي، من خلال دراسة وظيفته في تفكيك الشبكات الإرهابية العابرة للحدود والتعرف على مختلف عمليات التجنيد والتمويل المستتر.
*العمل على استجلاء الحدود القانونية والأخلاقية للاستخدام الأمني للذكاء الاصطناعي، من أجل تحقيق توازن بين حماية الأمن وحفظ خصوصية الأفراد.
*اقتراح تصور لسياسات ردع ذكي مستدامة، دون إغفال أهمية التعاون الدولي وتنسيق الجهود الأمنية لمواجهة الإرهاب المعزز بالتكنولوجيا في المستقبل.

2-الإطار المنهجي:

2-1-منهج الدراسة:

تم الاعتماد في هذه الدراسة على منهج مركب أساسه المقاربة التحليلية-الاستشرافية، وهذا طبعا بالنظر لطبيعة الموضوع الذي يتداخل فيه البعد التقني مع الأمني والقانوني، فقد استخدامنا المنهج الوصفي التحليلي بهدف تفسير التحولات التي أحدثها الذكاء الاصطناعي في أنماط الإرهاب داخل الفضاء الرقمي، وذلك من خلال تحليل الأدبيات والدراسات المتخصصة التي تناولت تقنيات الرصد، والبيانات الضخمة، والهوية البيومترية، والأساليب الاستخباراتية الرقمية، كما اعتمدنا على المنهج المقارن من أجل دراسة اختلاف النماذج الدولية والعربية في توظيف الذكاء الاصطناعي لمكافحة الإرهاب من جهة، ومقارنة أساليب الردع السيبراني والتشريعات والحوكمة الرقمية عبر تجارب متعددة من جهة أخرى. وإضافة إلى ذلك، ارتكزت الدراسة على المنهج الاستشرافي بهدف استكشاف مستقبل الردع الذكي في مكافحة الإرهاب، بناءً على الاتجاهات الحالية لتوظيف الخوارزميات والأطر القانونية والتعاون الدولي في المجال الأمني، وقد ساهم هذا المنهج في تقديم رؤية مستقبلية لآفاق تطوير سياسات ردع مستدامة تجمع بين حماية الأمن الوطني، وصون الخصوصية الرقمية، وضمان السيادة على البيانات، وبذلك يجمع هذا المنهج بين تحليل الواقع الرقمي، وتشخيص الفجوات القانونية، واستشراف مستقبل الردع الذكي، بما يسمح بفهم أعمق لكيفية توظيف الذكاء الاصطناعي ضمن منظومة أمنية متكاملة لمواجهة الإرهاب في المرحلة المقبلة.

2-2-أدوات جمع البيانات والمعلومات:

اعتمدنا في هذه الدراسة على المصادر الثانوية بوصفها الأداة الرئيسة لجمع البيانات والمعلومات، نظرًا لطبيعة الموضوع المرتبط بالذكاء الاصطناعي ومكافحة الإرهاب، وما يستلزمه من تحليل سياسات، وتجارب دولية، وتشريعات وتقنيات لا يمكن إخضاعها لبرامج ميدانية تقليدية ، كما تم جمع البيانات من خلال تحليل المحتوى العلمي والأمني والذي تم نشره في كتب متخصصة، ومجلات علمية محكمة، وتقارير دولية صادرة عن مؤسسات بحثية تعنى

بالأمن السيبراني ومكافحة التطرف الرقمي، إضافة الى الاستفادة من قواعد البيانات العلمية وقواعد المعرفة الرقمية التي توفر مستجدات الذكاء الاصطناعي والتقنيات الأمنية الحديثة.

واستخدمنا تحليل الوثائق الرسمية والتشريعات الوطنية والدولية ذات الصلة بالذكاء الاصطناعي والأمن السيبراني ومكافحة الإرهاب، بهدف فهم الإطار القانوني الذي يحدد حدود الاستخدام الأمني للخوارزميات، وإبراز جوانب القصور في البيئة التشريعية العربية مقارنة بالتجارب الدولية. واعتمدت الدراسة أيضًا على التقارير الفنية الصادرة عن الهيئات الحكومية ومراكز مكافحة التطرف والمؤسسات الدولية مثل منظمات التعاون الأمني، ومراكز الدراسات الرقمية، لما توفره من بيانات مُحدّثة حول الشبكات الإرهابية، وتقنيات التجنيد الرقمي، وأثر الذكاء الاصطناعي في عمليات الكشف المبكر.

وقد تنوعت أدوات جمع البيانات في هذه الدراسة بين تحليل الأدبيات العلمية، واستقراء التشريعات والوثائق، وفحص التقارير التقنية والأمنية، وهو ما يضمن تكوين رؤية شمولية متوازنة تمكن من فهم العلاقة بين التكنولوجيا والردع الذكي في مواجهة الإرهاب المعزز بالذكاء الاصطناعي.

2-3-حدود الدراسة:

إن التداخل بين هذا الموضوع ومجالات أخرى متعددة تطلب تحديد حدود معينة تمنع اتساعه خارج الإطار العلمي المطلوب، حيث تم تضييق مجال التحليل على الآليات الرقمية وسياسات الردع الذكي، مع التركيز على الأمن السيبراني والحوكمة القانونية والتعاون الدولي، كما أن الدراسة لا تُعالج الجوانب العسكرية التقليدية أو العمليات الميدانية، بل تركز على البيئة الرقمية والتقنيات الخوارزمية فقط في مواجهة الإرهاب المعزز بالتكنولوجيا ، وباعتبار أن الإرهاب السيبراني ظاهرة عابرة للدول، فقد تناولت الدراسة للنطاق الجغرافي من خلال نماذج دولية وعربية بهدف استنتاج تصور يمكن من خلاله بناء منظومة ردع ذكية مستدامة وذلك وفق الحدود الآتية :

2-3-1-الحدود الموضوعية:

هذه الدراسة ترتكز أساسا حول تحليل دور الذكاء الاصطناعي في مكافحة الإرهاب من منظور استراتيجي والذي يركز على سياسات الردع الذكي في الفضاء السيبراني ، حيث تشمل الدراسة تحليل الآليات الرقمية المستخدمة في الرصد والتوقع والتحليل الاستخباراتي، مثل البيانات الضخمة، والتقنيات البيومترية، والتحليل الخوارزمي للشبكات الإرهابية ، كما تهتم بدراسة البحث بالجوانب القانونية والأخلاقية المرتبطة باستخدام الذكاء الاصطناعي في المجال الأمني، من حيث حماية الخصوصية، سيادة البيانات، ومبدأ الحوكمة الرقمية، إضافة إلى استشراف مستقبل التعاون الدولي لمواجهة الإرهاب المعزز بالتكنولوجيا ، كما أن هذه الدراسة لا تشمل الجوانب العسكرية المباشرة أو العمليات التقليدية على الأرض، بل تقتصر على الممارسات الرقمية وتطبيقاتها الأمنية في نطاق الأمن السيبراني والردع الوقائي.

2-3-2- الحدود الجغرافية:

تبدأ هذه الدراسة من نطاق جغرافي واسع يتجاوز الحدود الوطنية، فالإرهاب المعزز بالذكاء الاصطناعي لا يقتصر على منطقة معينة، بل ينتشر عبر فضاءات رقمية عالمية يصعب ضبطها أمنيًا على مستوى دولة واحد، ولذلك فهذه الدراسة ترتكز على تحليل نماذج

وتجارب دولية وعربية في توظيف الذكاء الاصطناعي لمكافحة الإرهاب، من خلال مقارنة بعض الممارسات في الولايات المتحدة، والاتحاد الأوروبي، والصين، مقابل التجارب العربية خاصة في الخليج العربي، هذا ويجب أن يُستثمر هذا التنوع في المجال الجغرافي من أجل تقييم فرص بناء نموذج عربي للردع الذكي يستفيد من الخبرات العالمية ويستجيب لخصوصية البيئة التشريعية والأمنية في المنطقة العربية.

3-الإطار النظري للدراسة:

ترتكز دارستنا المقدمة على مجموعة من الأسس النظرية التي تفسّر العلاقة بين الذكاء الاصطناعي ومكافحة الإرهاب في الفضاء الرقمي، وهذا من خلال مدخل الأمن التكنولوجي ومفهوم الردع الذكي، حيث تشير نظرية الأمن المعزّز بالتكنولوجيا إلى أن التطور التقني لم يعد مجرد دعم لآليات الحماية التقليدية، بل أصبح عنصرًا بنيويًا في تشكيل السياسات الأمنية، من خلال اعتماده على تحليل البيانات الضخمة والتعرف على أنماط السلوك الخطر داخل المنصات الرقمية [10].ويُبرز هذا المدخل الدور المتصاعد للذكاء الاصطناعي كفاعل أمني قادر على توقع الأخطار قبل تحولها إلى تهديد فعلي، مما يدعم التحول من المواجهة إلى الوقاية[11]، كما يستند الإطار النظري إلى نظرية الأمن السيبراني متعدد المستويات، التي تفترض أن مواجهة الإرهاب الرقمي لا تعتمد على أداة واحدة، بل على منظومة تشمل حماية البنية الرقمية، تحليل الشبكات الإرهابية، ومراقبة الهويات البيومترية والسلوكية[12]، ويُضاف إلى ذلك مفهوم الردع الذكي الذي يجمع بين التقنيات التنبؤية، والحوكمة القانونية، والتعاون الدولي من أجل السيطرة على التهديدات العابرة للحدود، إذ لا يمكن مواجهة الإرهاب السيبراني في نطاق دولة واحدة ووُجهات تقنية متفرقة[13].

ويُؤكّد هذا الإطار على أهمية التحليل الخوارزمي للخطاب المتطرف بوصفه وسيلة لاكتشاف أنماط التجنيد والدعاية قبل تداولها وانتشارها داخل المجتمعات الرقمية[14] ، إضافة إلى دور البيانات الضخمة في بناء استخبارات رقمية قادرة على فهم ديناميات التطرف، والتمويل غير المرئي، والتواصل بين عناصر الشبكات الإرهابية[15]، ومن هذا المنطلق، يربط الإطار النظري بين الدور الأمني للذكاء الاصطناعي والحاجة إلى قوانين تحمي الخصوصية والسيادة الرقمية، تفاديًا لتحوّل الردع الذكي إلى أداة رقابية تمس الحقوق الفردية.[16]

وبناء على ما سبق، يوفر هذا الإطار أساسًا نظريًا يسمح بفهم كيف يمكن للذكاء الاصطناعي أن يتحول إلى منظومة ردع متكاملة تجمع بين التكنولوجيا والقانون والتعاون الدولي، بهدف مكافحة الإرهاب بصورة مستدامة تستبق الخطر دون المساس بالحقوق الرقمية.

3-1-الممارسات الدولية لاستخدام الذكاء الاصطناعي في مكافحة الإرهاب:

تعرف السنوات الأخيرة توسعًا ملحوظًا في اعتماد الدول للذكاء الاصطناعي كوسيلة مركزية لمكافحة الإرهاب في الفضاءين الرقمي والمادي، فقد اتجهت القوى الدولية الكبرى إلى اعتماد مجموعات من الأساليب ومن بينها: خوارزميات الرصد التنبؤي، والتقنيات البيومترية، وتحليل الشبكات الإرهابية العابر للحدود، حيث تُوظّف أنظمة الذكاء الاصطناعي من طرف أعظم قوة عالمية الممثلة في الولايات المتحدة الامريكية في تحليل البيانات الضخمة المتدفقة من وسائل التواصل والبصمة الرقمية للمشتبه بهم بهدف التنبؤ بمخاطر التطرف قبل تجسيدها في هجمات فعلية [17].

وهو ما مكّن الأجهزة الأمنية من الانتقال من مرحلة رد الفعل إلى مرحلة الوقاية عبر تتبع التحويلات المالية المشبوهة والخطاب التحريضي في المنصات المغلقة، وفي الاتحاد الأوروبي ركّزت سياسات مكافحة الإرهاب على استخدام التحليل الخوارزمي لتفكيك شبكات الدعاية والتجنيد الإلكتروني، مع دمج أدوات الذكاء الاصطناعي في مراقبة المحتوى العنيف الذي يُرَوّج له عبر الوسائط الرقمية، بالإضافة الى وضع قوانين تحاصر انتشار خطاب التطرف في المجال السيبراني دون تجاوز الحدود القانونية لحرية التعبير [18]

ومن جهتها قامت بعض الدول الأوروبية بتفعيل تقنيات التعرف البيومتري داخل المطارات والمعابر الحدودية لتعقب العناصر المشتبه بها، في ظل تزايد تدفق العابرين من مناطق الصر[19] ، وتُظهر التجربة في الصين من خلال الاعتماد المكثف على أنظمة المراقبة الذكية والهوية السلوكية، حيث يتم تحليل أنماط الحركة والشراء والتواصل، في إطار منظومة رقابية تهدف إلى التحكم الاستباقي في المخاطر الداخلية[20]. وقد أثار هذا النمط نقاشًا واسعًا حول حدود استخدام الذكاء الاصطناعي في الأمن، لما يحمله من تهديد محتمل للحقوق الشخصية إذا لم يخضع لقوانين صارمة تحمي الخصوصية الرقمية.

وتكشف هذه الأساليب الدولية المتنوعة عن اتجاه عام نحو نموذج الردع الذكي الذي لا يعتمد على القوة العسكرية التقليدية في مواجهة المخاطر، بل يعتمد على استثمار الخوارزميات والقوانين والتعاون الدولي في مواجهة الإرهاب العابر للحدود الرقمية، إلا أن فعالية هذا النموذج تتوقف على تحقيق توازن بين حماية الأمن والسيادة الرقمية من جهة، وصون الحريات والحقوق الرقمية من جهة أخرى، وهو ما يمثل تحديًا يقف كحاجز أمام مختلف الدول التي تتبنى الذكاء الاصطناعي في منظوماتها الأمنية.[21].

3-2-تحليل الممارسات الدولية الرائدة في مكافحة الإرهاب بالذكاء الاصطناعي:

أظهر تحليل الممارسات الدولية في توظيفها للذكاء الاصطناعي من أجل مكافحة الإرهاب، أن الدول لا تتبنى التقنية على نحو واحد، بل وفق نماذج متباينة ترتبط بسياساتها الأمنية والقانونية والرقابية، فالتجربة الأميركية كنموذج يقوم على الذكاء الاصطناعي كوسيلة استخباراتية تنبؤية الهدف منها التحليل العميق للبيانات الضخمة من أجل رصد النشاط الإرهابي قبل حدوثه فعلا[22] ،ويقوم هذا النموذج المتبع على بناء منظومات تحليل شبكاتية تستخدم تقنيات الذكاء الاصطناعي لتتبع التحويلات المالية المشبوهة وخرائط التجنيد الرقمي، وهو ما أسهم في الوقاية من مخاطر التطرف الإلكتروني، واعتمد الاتحاد الأوروبي نموذجًا يتأسس على الدمج بين المراقبة الرقمية من جهة والتشريع الوقائي من جهة أخرى، بحيث تُوظّف الخوارزميات في متابعة المحتوى العنيف، دون السماح بتجاوز قوانين حماية الخصوصية وحرية التعبير [23] هذا النموذج يعتبر هو الأكثر توازنًا بين الأمن والحريات الرقمية، غير أن فعاليته تظل رهينة سرعة تحديث التشريعات وتكييف قواعد الذكاء الاصطناعي معها، وقدمت الصين نموذجًا آخر مغايرًا يقوم على الذكاء الاصطناعي كأداة رقابية واسعة النطاق تعتمد على تحليل الهوية البيومترية والسلوكية داخل المجتمع .[24]حيث يتم استخدام تقنيات مراقبة ذكية تشمل الوجه، الصوت، وتتبع الحركة الرقمية، مما يؤدي إلى تحييد المخاطر الأمنية المحتملة بشكل مبكر، لكنه يفتح بابًا واسعًا للنقاش حول السيادة على البيانات،

وتأثير الرقابة التقنية على الحريات الفردية، وهذه النماذج تبرز لنا ثلاثة اتجاهات رئيسة في مكافحة الإرهاب عبر الذكاء الاصطناعي وهي:

1 - الذكاء الاصطناعي كوسيلة استخباراتية تنبؤية للردع الوقائي (النموذج الأمريكي).

2 - الذكاء الاصطناعي ضمن إطار تشريعي قانوني هدفه المحافظة على الخصوصية الرقمية (النموذج الأوروبي).

3 - الذكاء الاصطناعي كمنظومة رقابة كلية على الفضاء العام والخاص (النموذج الصيني).

قد بين لنا هذا التحليل المقدم أن نجاح الذكاء الاصطناعي في مكافحة الإرهاب لا يعتمد فقط على جودة التقنية، بل على آليات عديدة ولعل من بينها: الحوكمة القانونية، وآليات حماية الخصوصية، ومستوى التعاون الدولي في مواجهة الإرهاب العابر للحدود الرقمية .[25] لذلك فإن مستقبل الردع الذكي يرتبط بقدرة الدول على بناء منظومات أمنية تشاركية تجمع بين الاستخبارات الرقمية، وحماية الحقوق، وتبادل البيانات وفق ضوابط قانونية دولية.

4-تطبيقات لمكافحة الإرهاب:

يمكن استخدام الذكاء الاصطناعي بمختلف تطبيقاته من أجل عمل تنبؤات حول الإرهاب وذلك من خلال تحليل البيانات الوصفية للاتصالات والمعلومات عن مختلف المعاملات المالية وأشكال السفر وأنشطة تصفح الإنترنت، فضلًا عن المعلومات المتاحة للجمهور مثل نشاط وسائل التواصل الاجتماعي، والذي يُمكِّن من تحديد الإرهابيين عبر التفرقة بين ما يميز نشاط مجموعة فرعية معينة على هذه الوسائط تتيح أساليب التعلّم الآلي قدرات متقدمة على تحليل الأنماط الخفية في البيانات الضخمة التي يتعذر الوصول إليها بالطرق التقليدية، حيث تعمل على تفسير العلاقات بين العناصر المختلفة، وتحليل الإشارات الأكثر تعقيدًا مثل الصورة والصوت، بما يعزز من دقة التوقعات الأمنية [27]، وتكشف التطبيقات الحديثة عن مجموعة من النماذج التنبؤية التي تُظهر كيف يمكن للذكاء الاصطناعي أن يرفع الجهود الأمنية بأدوات استشرافية ذات فعالية عالية ومن ذلك:

4-1- التنبؤ بمكان وزمن الهجمات:

قامت بعض الشركات بتطوير نماذج تستند إلى آلاف النقاط البيانية لاستشراف توقيت الأنشطة الإرهابية ومواقعها وتشير التقارير إلى أنّ أحد النماذج التي استُخدمت عام 2015، والمبني على أكثر من 170 مؤشرًا، وصل إلى دقّة تقديرية بلغت نحو 72% في التنبؤ بالهجمات الإرهابية على شكل انتحار، وهذا طبعا يعكس طبيعة القيمة التنبؤية العالية للبيانات المتكاملة [28]، ومن جانب آخر اعتمدت مشاريع أخرى على بيانات المصادر المفتوحة لرصد الأنماط السلوكية للأفراد في الفضاء الرقمي، والتي من أبرزها نظام « الإنذار المبكر » ، الذي يدمج مخرجات عدة نماذج استشرافية للتنبؤ بحوادث كبرى مثل الاضطرابات الاجتماعية أو تفشي الأمراض. [29]

4-2-قياس الهشاشة القيمية وقابلية الانزلاق إلى التطرف: العديد من المؤسسات التقنية عملت على تطوير أدوات لتحليل قابلية الأفراد للانجذاب نحو الأفكار المتطرفة، وذلك عبر تتبّع السلوكيات الرقمية المرتبطة بالبحث عن المحتوى العنيف، هذا ويُعدّ مشروع «إعادة التوجيه» الذي تبنّته إحدى المؤسسات العالمية المختصة من أهم النماذج حيث يقوم على توجيه

المستخدمين الذين يُظهرون ميولًا نحو المحتوى المتطرف إلى مواد مرئية بديلة تحمل سرديات مناهضة للعنف، وتُظهر رؤية أكثر توازنًا[30]

4-3-التعرف على العناصر الخطِرة: بعض التقارير المتعلقة ببرامج أمنية استخدمت تحليل البيانات الوصفية لملايين المستخدمين تشير إلى قدرات الذكاء الاصطناعي في تحديد الأفراد الذين يُحتمل ارتباطهم بشبكات متطرفة، وعلى الرغم من محدودية فعالية بعض هذه النماذج، فإنها تُظهر أهمية البيانات الضخمة في الكشف عن العلاقات الدقيقة التي يصعب تحديدها بالتحليل التقليدي. فنتائج عام 2007، التي اعتمدت على تحليل بيانات أكثر من خمسين مليون مستخدم، أوضحت أن نسبة الخطأ في تحديد العناصر الخطرة كانت منخفضة للغاية، وهو ما يؤكد القيمة التنبؤية للبيانات في مجال مكافحة الإرهاب.[31]

5-نحو سياسات ردع ذكي لمكافحة الإرهاب في عصر الذكاء الاصطناعي:

دخول الذكاء الاصطناعي إلى المنظومة الأمنية العالمية أدى الى تحول كبير في مفهوم الردع الأمني، حيث لم يعد الردع قائمًا على القوة الميدانية أو الإجراءات العقابية اللاحقة، بل أصبح يعتمد على المنع الاستباقي عبر الرصد والتحليل والتنبؤ بالخطر قبل تحوّله إلى تهديد فعلي [32].

إن الردع الذكي لا يُسيّر التقنية بمعزل عن القانون، بل يقوم على تكامل ثلاثي يشمل:

5-1- التكنولوجيا الأمنية الذكية: تشكل التكنولوجيا الأمنية الذكية الركيزة التقنية الأساسية لبناء منظومة الردع الذكي ضد الإرهاب في عصر الذكاء الاصطناعي، حيث ترتكز على دمج الخوارزميات التحليلية، والتعلم العميق، والتقنيات البيومترية، وأدوات المراقبة السلوكية، في إطار أمني قادر على كشف التهديدات قبل وقوعها، حيث يقوم هذا النموذج الأمني على الرصد الاستباقي بدلًا من رد الفعل، وهو ما يسمح بتحديد أنماط السلوك المشبوهة، وتتبع الروابط الشبكية للخطاب المتطرف، وتحليل الدعاية الإرهابية في بيئات رقمية مفتوحة أو مغلقة.[33]

حيث تستند التكنولوجيا الأمنية الذكية على منظومات تحليلية متعددة المستويات تشمل بيانات شخصية، وسلوكية، واتصالية؛ وتتيح الخوارزميات إمكانية تحديد المستخدمين الذين يشكّلون تهديدًا محتملًا من خلال تقييم سلوكهم داخل المنصات الرقمية، سواء عبر محتوى منشور، أو تفاعل مع جماعات متطرفة، أو محاولات الوصول إلى محتويات مغلقة تُستخدم في التدريب الأيديولوج[34] ،حيث تسمح هذه التكنولوجيا بمتابعة التنقلات الرقمية والمالية للمشتبه بهم، مما يعزز القدرة على مراقبة شبكات التمويل الإرهابي غير المرئية التي تعتمد على العملات الرقمية ومنصات المدفوعات المشفرة.[35]

وتعتبر التقنيات البيومترية والسلوكية من أكثر وسائل الأمن الذكي فعالية، والتي تعتمد على بصمة الوجه والصوت والعين، إضافة إلى التحليل السلوكي الذي يقيس أنماط النقر، سرعة الكتابة، وحركة الجهاز، وهو ما يساهم في كشف الهوية الحقيقية حتى في حالات تغيير المعرفات أو استخدام [36] ويُسهم هذا الاستخدام للتكنولوجيا التقنية في تقليل الاعتماد على الأدلة التقليدية، ويعزز من الاستخبارات الرقمية عبر تقنيات التعرف الخوارزمي على المشتبه بهم في الحدود والمطارات والمنصات الرقمية.

وبالرغم من هذه المزايا، فإن التكنولوجيا الأمنية الذكية تحتاج دائما إلى حوكمة قانونية صارمة لمنع تحولها إلى أداة انتهاك للخصوصية أو مراقبة جماعية خارج الأطر القانونية،

ولهذا لا يمكن فصل التقنية عن التشريع، لأن حماية الأمن دون ضمان الحقوق الرقمية قد يؤدي إلى نماذج رقابية مُفرطة تقلّص من الحرية الفردية وتثير إشكالات أخلاقية في الدول الديمقراطية[37]، ومن ثمّ فإن فعالية التكنولوجيا الأمنية الذكية تقترن بمدى قدرة الدول على مواءمة الأمن مع سيادة القانون، وحوكمة البيانات، والتعاون الدولي في تبادل المعلومات الأمنية.

5-2-البيئة القانونية الضامنة لحقوق الأفراد:

من أجل نجاح منظومة الردع الذكي كطريقة لمكافحة الإرهاب يشترط وجود بيئة تشريعية متوازنة والتي تضمن حماية حقوق الأفراد في ظل الاستخدام الأمني للتقنيات الرقمية، ومع توسع توظيف الذكاء الاصطناعي في عمليات الرصد والتحليل والمراقبة البيومترية، ظهرت الحاجة إلى قوانين واضحة تمنع تحول هذه التقنيات إلى وسيلة سيطرة أو مراقبة جماعية تمس حريات وحقوق الأفراد في الخصوصية الرقمية[38] فالأمن السيبراني لا يمكن تحقيقه دون إطار قانوني يحفظ الحدود الفاصلة بين الاستخدام الوقائي للتقنيات والاعتداء على الحرية الشخصية وحق المواطن في سرية بياناته ، هذا ويمكن التأكيد على أن البيئة القانونية الضامنة لحقوق الأفراد تتمثل في مجموعة من القواعد القانونية والتي تنظم:

1. أسلوب جمع المعلومات الرقمية وطرق معالجتها.
2. أسس حفظ المعلومات الشخصية وكيفية حمايتها.
3. نظم مشاركة البيانات بين مختلف الهيئات الوطنية والدولية.
4. طرق ووسائل الرقابة على استخدام الذكاء الاصطناعي أمنياً.[39]

وتستخدم هذه الضوابط ضمن ما يسمى بـ حوكمة البيانات التي تشترط أن يتم التعامل مع المعلومات الشخصية وفق مختلف الطرق أهمها:

مبادئ الشفافية، المشروعية، والتناسب بين الغرض الأمني من جهة والمصلحة العامة من جهة أخرى، رغم أن بعض الدول تعتبر نموذجًا متقدمًا في هذا المجال، والتي من بينها الاتحاد الأوروبي هذا الذي نجح في أن يوازن بين المراقبة الرقمية والأطر القانونية لحماية الخصوصية، كما دول تعتمد أخرى نموذجًا رقابيًا واسعًا والذي يهدد أحيانا الحرية الشخصية في سبيل تحقيق الأمن، كما في التجربة الصينية التي توسعت في أدوات المراقبة السلوكية والبيومترية دون أطر قانونية شفافة تحدد سقف الاستخدام الأمني.[40]

ويكشف لنا هذا التفاوت أن القانون في أي دولة هو العامل الرئيسي والحاسم الذي يضبط حدود الذكاء الاصطناعي داخل أي منظومة الأمنية، كما ان التقنية بمفردها لا تضمن الأمن إذا لم يتم تقييدها وفق تشريعات التي تحمي بدورها السيادة الرقمية وحقوق المواطنين داخل الدولة، وتظهر مكانة ودور البيئة التشريعية في تنظيم التعاون الدولي في مكافحة الإرهاب السيبراني، خاصة فيما يتعلق بعملية التبادل بين الدول للبيانات الحساسة، لأنه يمكن أن يؤدي غياب الأطر القانونية إلى سوء استغلال المعلومات أو تسربها لجهات غير مخول لها [41]، لهذا فإنّ المستقبل الأمني العالمي يتطلب تشريعات وقوانين دولية موحدة أو متقاربة تهدف الى تنظيم استخدام الذكاء الاصطناعي في مكافحة العمليات الإرهابية من أجل تحقيق التوازن بين حماية الأمن من جهة وسيادة البيانات والحقوق الأساسية للمواطنين.

5-3-أسس مشاركة البيانات والتعاون الدولي:

إن استراتيجية التعاون الدولي في مجال مكافحة الإرهاب والتي تعززت واستندت إلى الذكاء الاصطناعي أصبحت ضرورة ملّحة، بالنظر لطبيعة عمل الإرهاب السيبراني وشبكات التجنيد والتمويل والاتصال، بحيث لا يمكن لأي دولة ـ مهما وصلت قدراتها التقنية ـ التصدي لهذه التحديات وحيدة، بل يتطلب ذلك عملية تبادل للبيانات والأدلة الرقمية وتعزيز العمل المشترك بين الحكومات والمؤسسات الأمنية العالمية[42] ،لكن هذا التعاون يجب أن يخضع لضوابط قانونية دقيقة تمنع سوء استخدام البيانات أو تحولها إلى أداة انتهاك للخصوصية أو سيادة الدول على معلوماتها الرقمية حيث تتضمن ضوابط عملية مشاركة البيانات بين مختلف الدول المتعاونة ثلاثة مستويات رئيسية وهي:

5-3-1-ضوابط سيادة البيانات: ومفادها بأنه يجب أن تكون مشاركة المعلومات الأمنية خاضعة لموافقة الدولة صاحبة البيانات، حتى يتم منع انتهاك سيادتها الرقمية أو تسريب لبيانات حساسة لأطراف قد يتم استخدامها خارج إطار مكافحة الإرهاب.[43]

5-3-2-ضوابط حماية الخصوصية: هذه الضوابط تلتزم بقواعد الشفافية والحد الأدنى المطلوب من جمع البيانات اللازمة، والتي من خلالها لا يتم تبادل معلومات الأفراد إلا في إطار مرتبط بصورة مباشرة تتعلق في الأساس في كل تهديد إرهابي وبموافقة تشريعية صريحة [44].

5-3-3-ضوابط استعمال الأدلة الرقمية: والتي تؤكد على أن مشروعية جمع الأدلة والقيام بتخزينها على أسس ومعايير واضحة تسمح باستخدامها قضائيًا بما يضمن عدم مخالفتها لحقوق الأفراد أو الإجراءات القضائية، وبما يضمن تحقيق الأمن دون إهدار ضمانات المحاكمة العادل[45] .

إن نجاح التعاون الأمني المشترك بين الدول يعتمد على إطار تشريعي دولي يحدد قواعد تبادل البيانات، وآليات الرقابة عليها، والجهات المخولة بالوصول إليها، إضافة إلى بناء بروتوكولات موحدة تشمل مؤسسات الشرطة الدولية والمراكز المتخصصة في مكافحة التطرف الرقمي.[46]

6-مستقبل مكافحة الإرهاب في عصر الذكاء الاصطناعي: من ثورة المعرفة إلى سياسات الردع الذكي:

يعرف العالم حاليا تحوّلًا نوعيًّا خاصة في طريقة إنتاج المعارف وكيفية معالجتها، والذي تسيّره الطفرة الراهنة في الذكاء الاصطناعي التوليدي، خاصة نماذج اللغة الضخمة والتي أصبحت قادرة على محاكاة ومعايشة الحوار البشري، إضافة الى القيام بحلّ مختلف المسائل مهما كان نوعها قانونية أو طبية، بالإضافة على اجتياز الامتحانات المهنية المؤهلة للترقية، وكتابة نصوص أدبية وبرمجية معقدة، وتلخيص كميات هائلة من المعلومات في ثوانٍ معدودة[47]، وقد ظهرت أنماط أخرى من الذكاء الاصطناعي التوليدي - إلى جانب ما ذكرناه سابقا - بإمكانها إنتاج صور ومقاطع فيديو وأصوات رقمية قريبة جدا من الإنتاج البشري[48]، ومنذ أحداث 11 من سبتمبر 2011، لجأت مختلف الدول والحكومات وخاصة في الدول الغربية، إلى استخدام التحليلات المتقدمة والتعلم الآلي والذكاء الاصطناعي من أجل دعم جهود مكافحة الإرهاب من خلال جمع ومعالجة كميات ضخمة من البيانات الاستخباراتية المتناثرة،

كمحاولة للعثور على "الإبرة في كومة القش" داخل فوضى الاتصالات البشرية، والإشارات التقنية[49]، وتم استخدام مختلف المنصات غير المأهولة –كالطائرات المسيّرة – مع هذه الأدوات من أجل التخطيط للقيام بضربات دقيقة ضد الجماعات الإرهابية.[50]

ولكن وبالرغم إتاحة هذه التطورات من قدرات استباقية عالية في مكافحة الإرهاب إلا أن نظام مكافحة الإرهاب ظلّ في جوهره مشروعًا بشريًا دون منازع؛ حيث بقي الإنسان هو الذي يضع معايير التعلم وبذلك يقوم بتصميم مختلف نماذج الذكاء الاصطناعي، وهو الذي يتحقق من صلاحية المخرجات، ويقوم بالموازنة بين النتائج الإيجابية والسلبية الكاذبة، ويقرّر متى تكون الأداة مقبولة أخلاقيًا وقانونيًا.[51] ، أما اليوم فإن الذكاء الاصطناعي التوليدي ونماذج اللغة الضخمة تفتح الباب واسعا أمام نقلة جديدة، والتي لا تقتصر على تحسين بعض المهام، بل أنها تسعى لتلامس إمكانية انهاء أجزاء واسعة من "سلسلة القيمة المعرفية" في مكافحة الإرهاب، وذلك من مرحلة جمع البيانات إلى مرحلة التحليل، ومن مرحلة إنتاج الرؤى إلى مرحلة اقتراح مسارات الفعل، الى غاية الوصول إلى توجيه المنصات الروبوتية القتالية ، وفي المقابل، فقد تصاعدت المخاوف لدى البعض من إساءة استخدام هذه التقنيات من قبل الدول ، بل من طرف الجماعات المتطرفة أو بفعل أخطاء تصميمية وتحيزات كامنة في البيانات [52].

7-الذكاء الاصطناعي كمنظومة تعلم احتمالية:

أنظمة الذكاء الاصطناعي والتعلم الآلي المعتمدة حاليا من طرف الدول تعرف بوصفها برامج تتعلّم من البيانات من أجل إنجاز مهام والتي كانت تستلزم عادةً قدرات معرفية بشرية متمثلة في التصنيف، التنبؤ، اكتشاف الأنماط، واتخاذ القرار الصحيح[53]هذا وتعتمد هذه الأنظمة المعتمد عليها على خوارزميات متعددة تستخلص من مجموعات البيانات "معرفة ضمنية"، والتي تحوّلها إلى احتمالات شرطية تسمح لها بإنتاج تخمينات عالية الدقة حول ما يتوقع أن يحدث، حيث لا تكمن قوة هذه الأدوات في الخوارزميات ذاتها، بل في حجم البيانات وجودتها، وفي تصميم النموذج وتحديد نطاق عمله [54] فهذا المنطق يتسع ليشمل تطبيقات مختلفة وعديدة صحية منها كانت أو أمنية؛ بحيث بإمكان خوارزميات القياسات الحيوية، مثلًا، أن تحدد ارتباطات دقيقة بين أنماط معينة في الصور الطبية وبين أمراض محددة مضبوطة تنطبق عليها، وهو ما يساعد الأطباء على تشخيص الامراض وبالتالي تخفيف العبء الذهني الناتج عن معالجة عدد كبير من الحالات خاصة المستعصية منها والنادرة الحدوث [55] لكن هذا "الذكاء" يبقى دائما مقيّدًا بالكامل بما تتيحه البيانات والتصميم البشري؛ فالآلة المبرمجة لا يمكنها ان تتجاوز أبدًا نطاق ما بُرمجت من أجله سواء من حيث صياغة الأهداف او الوظائف التي تقوم بها، وعندما يتم انتاج معلومات خاطئة، فإن أصل المشكلة يعود إلى طريقة تدريبها وبناء معماره.[56]

8-العقل البشري كنموذج إدراكي بديل يتجاوز البيانات:

لقد طرح عدد من الباحثين – مثل جوديا بيرل – في مقابل العقل الخوارزمي فكرة أن الوظيفة الإدراكية البشرية أكثر تعقيدًا من الآلات؛ لأن البشر لا يعتمدون فقط على البيانات الجاهزة، بل بإمكانهم بناء استدلالات سببية حول ما لم يحدث فعليًا، واستحضار عوالم افتراضية وبدائل محتملة.[57] دون أن ننسى تحكم السلوك البشري منظومة قيمية وأخلاقية

معقدة؛ بحيث يتخذ الأفراد قراراتهم ليس بالنظر لتفضيلات غير قابلة للقياس الكمي، مثل الإيمان، والهوية، والعدالة[58].

إن المتتبع لهذه التفضيلات يدرك مدى إمكانية تُحوّل البشر إلى وكلاء أخلاقيين بإمكانهم التمييز بين الصواب والخطأ، إضافة الى تحمل مسؤولية أفعالهم، وعلى النقيض من ذلك فإن أنظمة الذكاء الاصطناعي لا تمتلك أي وعي ذاتي؛ باعتبار أن كلّ ما تفعله هو ترجمة ما صممته أيدي البشر من بيانات وتصميمات [59].

فقد انتقد "جيلبرت رايل" الفكرة التي قدمها الفيلسوف الفرنسي ديكارت والتي من خلالها يفصل بين ‘‘العقل’’ و’’الجسد’’، وقد صاغ مفهوم ‘‘الشبح في الآلة’’ وهذا دلالة منه على وهم وجود كيان عقلي مستقل يحرّك الجسد من خارجه .[60]

9 ـطبيعة الحرب العالمية على الإرهاب:

لقد شكّلت هجمات 11 سبتمبر 2001 بداية التحوّل الحقيقي في مسار الأمن القومي الأمريكي والعالمي حيث كشفت عن قصور كبير في بنية الاستخبارات والقرارات من خلال نقص في اللغويين والمحللين المتخصصين، وانقسامات بيروقراطية كبيرة حالت دون تبادل المعلومات، وعدم استثمار كافٍ في فهم وإدراك لمعنى البيئات التي نشطت فيها تنظيمات مثل القاعدة .[61]

وهذا السياق بيّن أن المشكلة ليست في غياب البيانات، بل في عجز الجهاز البشري عن استيعابها وتحويلها إلى رؤية استراتيجية؛ وبالتالي يمكن ان نقول إنها كانت أزمة معرفية – تنظيمية، بدل أن تكون أزمة تقنية فحسب، ومع اندلاع الحرب العالمية على الإرهاب، وجدت الأجهزة نفسها مجبرة على إعادة تعريف أولوياتها، وتطوير مناهج جديدة للتجنيد والتدريب، ومن ثم توسيع نطاق جمع المعلومات وتحليلها.[62]

10- إعادة هيكلة المنظومة الاستخباراتية والعسكرية : تم أُنشاء مكتب مدير الاستخبارات الوطنية في منتصف العقد الأول من الألفية من أجل تنسيق جهود وكالات الاستخبارات وتقديم رؤية مشتركة للتهديدات، حتى وإن كان استقرار هذا الدور قد تطلب سنوات من الصراع البيروقراطي [63]، أما على المستوى العملياتي أو الميداني، فقد طوّرت قيادة العمليات العسكرية الخاصة المشتركة نموذجًا شبكيًا للحرب يقوم على دمج الاستخبارات والعمليات في دورة مستمرة من ‘‘استهداف – تنفيذ – استغلال – تحليل’’، مع مراكز عمليات مشتركة تجمع محللين لغويين وخبراء شبكات اجتماعية وطياري طائرات مسيّرة في فضاء تنسيقي واحد [64]وقد مكنّ هذا النموذج المعتمد في تقليص مختلف الثغرات والفجوات الزمنية بين مجال جمع المعلومات ومجال اتخاذ القرار والضربة العسكرية، وبالتالي خلق قدرة عالية على ملاحقة الشبكات الإرهابية المتحركة، ومع ذلك ظلّ تعريف ‘‘النصر’’ مبهما، واستمر توسيع العمليات الميدانية لمكافحة الإرهاب دون استراتيجية نهائية واضحة تتجاوز قتل الإرهابيين أو اعتقالهم.[65]

11- تحوّل المشهد الإرهابي وتعددية التهديدات: لقد تغيّر تنظيم القاعدة كأحد المنظمات الإرهابية من نواة مركزية أساسها أفغانستان إلى شبكة من الفروع الإقليمية الممتدة المتكيفة مع السياقات المحلية، كما نتج عنه لاحقًا تنظيم آخر الذي يعرف بتنظيم الدولة الإسلامية والذي يفوق الأول بقدرات عسكرية وإدارية أكثر تطورًا، حيث امتدت آثارها إلى الساحات الغربية عبر هجمات الذئاب المنفردة والخلايا الصغيرة النائمة.[66]

12- الدرس المركزي: لا أمن بلا بنية معرفية سليمة: لقد أوحت أحداث 11 سبتمبر الإرهابية أن الإخفاق لم يكن نتيجة غياب التكنولوجيا، بل نتيجة عجز في تنظيم المعرفة وتنسيقها، فقد كانت لدى الأجهزة معلومات من مصادر موثوقة كافية لتعطيل المؤامرة التي تم التنسيق والتخطيط لها، لكن الأجهزة الاستخبارية فشلت في قراءة المعلومات في الوقت المناسب لعدة أسباب من بينها: الإرهاق، والتجزئة المؤسسية، وضعف الخيال الاستراتيجي.[67]

13-التطبيقات التكتيكية والعملياتية للذكاء الاصطناعي في مكافحة الإرهاب:

13-1- مكافحة التطرف وإزالة التطرف:

يعتبر التطرف أحد السلوكات التي ينشأ عليها الفعل الإرهابي حيث يقوم على منظومة من المعتقدات الجامدة التي تبرّر استخدام العنف كوسيلة من أجل تحقيق مجموعة من الأهداف سياسية أو عقائدية كانت، وتعتبر مختلف الأدبيات الحديثة إلى أنّ التطرف ليس ظاهرة أحادية البعد، بل أنه يتشكل ضمن بنية مركّبة تتداخل فيها الأبعاد الفكرية والدافعية والنفسية ، لذلك يمكن التمييز بين أنواع من الطرف والتي من بينها : التطرف الأيديولوجي الذي يعتبر مرتبطًا بطبيعة المحتوى الفكري الذي يتبنّاه الفرد، أما التطرف الدافعي أو الانفعالي فيمثل الاستعداد النفسي لاستخدام العنف بوصفه أداة مشروعة، وهو بُعد يزداد خطورته في البيئات المشحونة بالاحتقان أو الظلم المتصوَّر في حين يرتبط التطرف النفسي بمستوى التعصب، ورفض المراجعة، والانغلاق المعرفي الذي يمنع الفرد من تقييم معتقداته بموضوعية أو قبول التعددية الفكرية.[68]

هذا وتتيح تقنيات المستخدمة في الذكاء الاصطناعي اليوم إمكانات متطورة لمعالجة هذه الأبعاد الثلاثة بصورة متكاملة، سواء عبر تحليل المحتوى الرقمي من أجل ضبط المؤشرات الفكرية والسلوكية الدالة على الانزلاق نحو التطرف، أو من خلال نماذج التنبؤ والتوقع بالتحول الانفعالي والسلوكي للأفراد ومختلف الجماعات.، كما تُستخدم الأنظمة الذكية في انشاء مسارات مخصّصة لإزالة التطرف (Deradicalization)، وهذا لن يكون إلا من خلال تصميم محتوى مضاد يتوافق مع طبيعة الانحراف الفكري والسلوكي للفرد، ومن ثم العمل على توجيهه نحو بدائل معرفية أكثر توازنًا وانفتاحًا، حيث تشمل هذه الآليات توصيات تستند إلى تحليلات خوارزمية دقيقة تستقرئ أشكال التفكير، وحيوية التفاعل الإنساني ومختلف الرموز والتعابير الخطابية التي يعتمدها المتطرفون في استقطاب الأنصار وتوسيع مساحة التأثير.

13-2- الذكاء الاصطناعي والاستخبارات:

تعتبر الاستخبارات الشاملة عنصرًا أساسياً وفعّالا في نجاح أي مقاربة مهما كان نوعها لمكافحة الإرهاب، فهي التي تسمح بتجميع بيانات دقيقة وفهم أعمق لبنية التهديدات وأساليبها وفي هذا الإطار، يوفّر الذكاء الاصطناعي وأساليب الاعلام الآلي قدرات ومؤهلات متقدمة تساعد الأجهزة الأمنية من تعزيز كفاءتها وقدراتها على مستويات متعددة؛ حيث يساعد على تحليل كميات ضخمة من البيانات في وقت وجيز، كما يكشف عن الأنماط الخفية في السلوك، ويحدّد لنا الإشارات المبكرة التي تدلّ على انتقال فرد أو جماعة نحو تيار التطرف أو العنف المنظّم.[69]

كما أن الخوارزميات المتقدمة تسمح ببناء تنبؤات دقيقة بشأن طبيعة التهديدات المقبلة، واستقراء التحركات المحتملة في نشاط الجماعات المتطرفة، والعمل على رصد العلاقات

الداخلية التي تربط بين عناصرها، ويمكن اعتبارها بمثابة مهام جوهرية تبرز في الأدبيات المعنية بتحليل المخاطر باستخدام الأنظمة الذكية. [70] حيث تساعد هذه القدرات والمؤهلات على تطوير «الاستخبارات الاستباقية»، أي ما يعرف بالقدرة على منع حدوث الخطر قبل وقوعه فعليا عوض الاكتفاء بردّ الفعل بعد وقوعه، وهو الشيء الذي يعتبره الباحثون إطارًا جديدًا لرفع فعالية منظومات الأمن الوطني في مواجهة التهديدات الذكية والعابرة للحدود.[71] ، كما يتم تنفيذ تحليل واسع النطاق من أجل رصد توجهات الرأي العام تجاه الجماعات المتطرفة أو سبل مكافحتها[72] هذا وتبقى الاستخبار البشري مجالًا حيويا بحيث لا يمكن استبدال العنصر البشري فيه بالكامل؛ بحيث تعتمد على بناء الثقة والعلاقات مع المجتمعات وقدرة الضباط على فهم السياقات المحلية المعقدة [73].

كما أن القراءة النظرية تبيّن لنا أنّ القيمة الجوهرية للذكاء الاصطناعي في مجال مكافحة الإرهاب تنبع في الأساس من قدرته على تخفيف العبء المعرفي عن الأجهزة الأمنية، وهذا من خلال تحمل كميات ضخمة من البيانات والمعلومات وتحليلها وتلخيصها في زمن قياسي، من أجل تسريع دورة اتخاذ القرار ورفع فعالية الاستجابة الميدانية[74]، وظلت المنصّات الذكية قادرة على الاضطلاع بجملة من المهام التكتيكية والعملياتية من جهة المادي والرقمي، مثل مراقبة الفضاءات ، ورصد التهديدات المتنامية، وتفعيل التدابير الوقائية والمضادة من جهة أخرى. [75]

لكن هذه الإمكانات التقنية لا تتحوّل، تلقائيًا، إلى نتائج استراتيجية أو أخلاقية إيجابية لأن الاستراتيجية مرتبطة بواقع المجتمع ومحيط الدولة وبالتالي لا تُنتجها الخوارزميات، بل تُحدّدها القيم المجتمعية، وطبيعة النظام السياسي، ومدى الالتزام بحقوق الإنسان وسيادة القانون، لهذا فلو تم إدماج الذكاء الاصطناعي ضمن مقاربة أمنية قمعية، فإن مكافحة الإرهاب تصبح غطاءً لتوسيع المراقبة، وتعميق التحكم الاجتماعي، وبالتالي استدامة العنف[76]، إلا أنه حين يُدمج ضمن رؤية ونظرة استباقية استشرافية ديمقراطية متوازنة، فيمكن أن يؤدي دورًا إيجابيًا في تقليل الأذى، وبالتالي تعزيز الردع الذكي، وتحسين كفاءة استخدام القوة [77] .

يمكن القول بأن الذكاء الاصطناعي ليس إلا انعكاسًا للخيارات الأخلاقية والمؤسساتية للمجتمع، وهنا يتحدد المسار: وهو إمّا أن يتحوّل الذكاء الاصطناعي إلى امتداد للوعي الأخلاقي والاستراتيجية الرشيدة، وإمّا أن يصبح الذكاء الاصطناعي وسيلة عمياء تزيد الأخطاء وتعمّق الأزمات ، ولهذا فإن مستقبل مكافحة الإرهاب في عصر الذكاء الاصطناعي لا يمكن أن ترسمه وتخطط له التكنولوجيا لوحدها، بل يمكن ان تحدده نوع الأسئلة التي يطرحها صانعو القرار، ومدى قدرة المجتمعات على فرض أنظمة تحمي الإنسان من أعدائه ... ومن وسائله في آن واحد .[78]

14-البنية التقنية للردع الاستباقي:

لقد أصبح الردع المستخدم في مكافحة الإرهاب الرقمي قائمًا على أنظمة تقنية متقدمة ومتطورة قادرة على الرصد والتحليل للتنبؤ المبكر لكل التهديدات الإرهابية، فلم يعد الأمن حاليا مرتبطًا فقط بالوسائل التقليدية التي تتعامل مع الخطر بعد حدوثه، بل أصبح يعتمد على تكنولوجيا استباقية تعمل على فهم أنماط السلوك الإرهابي داخل الفضاء السيبراني، وتفكيك شبكات الدعاية والتجنيد والتمويل قبل دخولها مرحلة التنفيذ ومن ثم يصعب التحكم فيها [79]

وتمثل هذه البنية التقنية أحد أهم بوادر التحول نحو ما يسمى الردع الذكي، وترتكز هذه البنية على ثلاث ركائز تقنية أساسية وهي: البيانات الضخمة، التحليل التنبؤي والرصد البيومتري والسلوكي، والذكاء الاصطناعي في كشف الدعاية والتجنيد الإلكتروني، كما أن تحليل هذه الركائز ضروري جدا باعتبارها أدوات ووسائل مركزية أساسية في بناء منظومة أمنية قادرة على الوقاية من المخاطر الإرهابية، ومن ثم تعزيز الاستخبارات الرقمية، دون تجاوز الحدود القانونية التي تحمي سيادة البيانات والخصوصية الفردية.[80]

كما أن تجمع هذه الركائز الثلاث يساعد في بناء منظومة ردع ذكية تعتمد على الاستباق والتحليل الوقائي عوض المواجهة بعد وقوع الهجوم. [81]

15 -استشراف مستقبل الردع الإرهابي عالميًا واستراتيجية توظيف تقنيات الذكاء الاصطناعي في مكافحة الإرهاب:

تم توجيه المنظومة الأمنية العالمية حاليا نحو مرحلة جديدة في مواجهة الإرهاب، حيث تقوم على الردع الذكي بدل الردع التقليدي، فلم يعد الاعتماد على القوة الصلبة كافيًا لمواجهة التنظيمات الإرهابية التي باتت تستثمر الفضاء الرقمي بصورة مكثفة، ويُظهر هذا التحول في طريقة المواجهة أن الذكاء الاصطناعي سيشكل، خلال العقدين القادمين، أساسًا بنيويًا في منظومات الأمن السيبراني والاستخبارات الرقمية، وهو ما يساعد على توقع السلوك الإرهابي، وبالتالي إمكانية توجيه استجابة أمنية دقيقة ووقائية تساعد على التحكم فيه[82]

هذا ويتأسس الاستشراف الأمني لمستقبل مكافحة الإرهاب على ثلاثة اتجاهات رئيسة وهي:

-الاتجاه الأول يتمثل في تعزيز الأنظمة الاستباقية القائمة على التحليل التنبؤي للبيانات الضخمة، من أجل صياغة نماذج رياضية بإمكانها تقييم احتمالات التطرف مستقبلا.[83]

-الاتجاه الثاني مرتبط بتوسيع استخدام البصمة البيومترية والتحليل السلوكي داخل الحدود ومختلف المنصات الرقمية، بهدف منع تنقّل الإرهابيين واستخدام الهويات المزيفة. [84]

- الاتجاه الثالث يتعلق بقدرة الدول على تحليل الدعاية المتطرفة داخل منصات الوسائط الاجتماعية باستخدام خوارزميات اكتشاف المحتوى المتطرف ومتابعة شبكات التأثير الرقمي[85].

لكن نجاح هذه الاتجاهات والرؤى لن يتحقق ما لم تُدمج ضمن استراتيجية عالمية للحوكمة القانونية الرقمية، تقوم على تبادل البيانات والمعلومات على أساس اعتبارات الخصوصية وسيادة الدول، مع سنّ قوانين دولية موحدة تُحكم استخدام تقنيات الذكاء الاصطناعي في المجال الأمني[86]

يمكن القول بطبيعة الحال أن مستقبل الردع الإرهابي يتجه نحو نموذج هجين يجمع بداخلة بين التكنولوجيا والقانون والتعاون الدبلوماسي الأمني، يعتمد على بناء شبكات عالمية لتبادل المعارف والبيانات الاستخباراتية وفق ضوابط قانونية، وتعزيز منظومات الرصد التنبؤي، وحماية الحقوق الرقمية في الآن ذاته، وعليه فقد انتقل مسار الذكاء الاصطناعي من مجرد وسيلة تقنية إلى شريك استراتيجي في صياغة السياسات الأمنية العالمية من أجل خلق بيئة ردعية مستدامة قادرة على احتواء مخاطر الإرهاب في فضاء رقمي غير ثابت ومتشعب.

16-الخاتمة:

نتائج هذه الدراسة تكشف لنا أن تطور الإرهاب في البيئة الرقمية لم يعد مجرد امتداد لأساليب العنف التقليدية، وإنما أصبح ظاهرة جديدة تستثمر الذكاء الاصطناعي وفضاءات التواصل في التجنيد والتمويل ونشر الدعاية المتطرفة بطرق معقدة يصعب ضبطها بالوسائل الأمنية الكلاسيكية ،حيث بيّن لنا تحليل التجارب الدولية أن مواجهة هذا الإرهاب المتطور تتطلب الانتقال من نموذج وأسلوب المواجهة بعد وقوع الهجوم إلى نموذج وأسلوب الردع الذكي القائم على الوقاية الاستباقية للخطر ، بالاعتماد على الخوارزميات التحليلية والبيانات الضخمة والتقنيات البيومترية والسلوكية ، حيث تبيّن أن فعالية مكافحة الإرهاب بالتقنيات الذكية ليست رهنًا بجودة الأدوات الأمنية وحدها، بل هي مرتبطة بوجود حوكمة قانونية واضحة تضمن حماية الخصوصية وسيادة البيانات، وتنظم عملية تبادل المعلومات بين الدول في إطار من الشفافية وعدم استغلال البيانات في التجسس أو التمييز أو المراقبة الواسعة ، ولهذا فإن مستقبل الردع العالمي ضد الإرهاب يتطلب بناء منظومة هجينة تجمع بين التكنولوجيا المتقدمة، والتشريع الوطني والدولي، والدبلوماسية الأمنية التعاونية.

ويمكن الإشارة الى أن الذكاء الاصطناعي لم يعد مجرد وسيلة مساعدة للجهات الأمنية، بل أصبح فاعلية استراتيجية في صياغة السياسات الأمنية المستقبلية، حيث يتيح استباق الخطر بدلًا من التعامل معه بعد وقوعه، ويتوقع أن يشكل محورًا رئيسًا في حماية الأمن القومي والرقمي للدول، وتخلص الدراسة بناء على ما سبق إلى ضرورة اعتماد نموذج عالمي موحد يقوم على الردع الذكي كمنظومة مستدامة توازن بين حماية المجتمعات وصون الحقوق الرقمية، لمواجهة إرهاب متحول يزداد تعقيدًا يوم بعد يوم مع كل تطور تقني جديد.

17-النتائج والتوصيات :

17-1-النتائج :

توصلت هذه الدراسة إلى أن مكافحة الإرهاب في عصر الذكاء الاصطناعي لم تعد تعتمد على الأساليب التقليدية التي تركز على مواجهة الخطر بعد وقوعه، بل شهدت تحولًا نحو نموذج الردع الاستباقي القائم على الوقاية قبل التنفيذ. فقد أتاح الذكاء الاصطناعي للأجهزة الأمنية القدرة على تحليل البيانات الضخمة والتنبؤ بالأنشطة الإرهابية المحتملة، ما يساعد في تفكيك الشبكات الإرهابية قبل انتقالها من مرحلة التخطيط إلى مرحلة التنفيذ الفعلي.

فقد تأكد بأن المنظومات الأمنية العالمية باتت تعتمد على أدوات تحليلية ذكية مثل التحليل الخوارزمي، التتبع البيومتري، والمراقبة السلوكية، مما أسهم في كشف الهوية الحقيقية للعناصر الإرهابية سواء داخل الفضاء الرقمي أو عبر الحدود المادية، وهو ما جعل هذه الوسائل جزءًا لا يتجزأ من البنية الأمنية الحديثة ، حيث يواكب ذلك تصاعد خطير في مظاهر الإرهاب السيبراني، إذ تستخدم الجماعات المتطرفة الذكاء الاصطناعي في نشر الدعاية الرقمية، تدريب العناصر الجديدة، وتمويه هوياتها عبر تقنيات التشفير والتزييف العميق، الأمر الذي يجعل الفضاء الرقمي بيئة خصبة لإنتاج تهديدات أمنية معقدة.

ورغم هذا الاستخدام التدريجي للتقنيات الذكية في الردع الأمني، كشفت الدراسة عن حاجة ملحّة لوجود حوكمة قانونية تنظم توظيف الذكاء الاصطناعي في مكافحة الإرهاب، إذ إن غياب تشريعات واضحة قد يؤدي إلى تحويل هذه الأدوات الأمنية إلى وسائل للرقابة

المفرطة وانتهاك الخصوصية وسيادة البيانات، وأظهرت النتائج كذلك أن مواجهة الإرهاب المعزز بالتكنولوجيا تتجاوز قدرة الدول منفردة، مما يجعل التعاون الدولي وتبادل البيانات الرقمية والاستخباراتية شرطًا أساسيًا للردع العالمي ضد التهديدات الإرهابية العابرة للحدود.

وفي ضوء ذلك، تؤكد الدراسة وجود توجه عالمي نحو نموذج ردعي هجين يجمع بين التكنولوجيا المتقدمة، التشريعات القانونية الوطنية والدولية، والدبلوماسية الأمنية المشتركة، بما يحقق معادلة دقيقة بين حماية الأمن وحماية الحقوق الرقمية. وتخلص إلى أن الذكاء الاصطناعي لم يعد مجرد وسيلة دعم للمؤسسات الأمنية، بل تحول إلى فاعل استراتيجي في صياغة سياسات الأمن الوطني والعالمي، وسيتنامى دوره مستقبلًا في تشكيل بيئة ردعية أكثر فاعلية واستدامة.

تشير النتائج المتوصل إليها في هذه الدراسة إلى أن الذكاء الاصطناعي أحدث نقلة نوعية في مفهوم مكافحة الإرهاب، حيث لم يعد الأمن قائمًا على التدخل بعد وقوع الخطر، بل انتقل نحو نموذج استباقي يركز على المنع قبل التنفيذ. وتتوافق هذه النتيجة مع الدراسات الحديثة التي عززت فكرة الرصد التحليلي والتنبؤ بالخطر بوصفها جوهر منظومات الأمن المتقدمة، مما يعكس تحوّلًا جوهريًا من ثقافة رد الفعل إلى ثقافة الوقاية. ويُظهر هذا التحول أن البيئة الرقمية باتت مصدرًا غنيًا للمعلومات التي تسمح بفهم ديناميات التطرف قبل تحولها إلى تهديد عملي، ما يدعم تبني استراتيجيات أكثر فاعلية وأقل تكلفة من الناحية الأمنية.

وتكشف النتائج كذلك أن الأدوات التحليلية الذكية التي تعتمد على البيانات الضخمة، القياسات البيومترية، والتحليل السلوكي، أصبحت ركيزة أساسية في كشف الهوية الحقيقية للعناصر الإرهابية التي كانت تستفيد سابقًا من طبيعة الفضاء الرقمي المفتوح للتمويه والاختفاء. غير أن هذا التطور التقني يطرح، في المقابل، تحديات أخلاقية وقانونية معقدة، لاسيما فيما يخص حماية الخصوصية والسيادة على البيانات الشخصية. فكلما ازداد توغل هذه التقنيات في حياة الأفراد، زادت احتمالات تجاوزها للحدود القانونية وتهديد الحقوق الرقمية، مما يؤكد أن مكافحة الإرهاب لا يمكن فصلها عن منظومة الحوكمة القانونية.

وقد أظهر التحليل أن التعاون الدولي في تبادل المعلومات لم يعد خيارًا إضافيًا، وإنما أصبح ضرورة أمنية ناتجة عن الطبيعة العابرة للحدود للإرهاب السيبراني. حيث أثبتت النتائج أن أي دولة تعمل بشكل منفرد ستظل معرضة لثغرات أمنية تستغلها مختلف التنظيمات الإرهابية المنتشرة في فضاءات رقمية لا تخضع لحدود سياسية. ومع ذلك، يظل هذا التعاون مرهونًا بتوافق تشريعي يحمي البيانات الوطنية والحقوق الفردية، وهو ما يستدعي وضع معايير دولية موحدة تحكم استخدام الذكاء الاصطناعي في المجال الأمني.

17-2-التوصيات : توصي الدراسة بضرورة :

- العمل على تبني واتباع سياسات أمنية متوازنة تُمكّن الدول من الاستفادة من دور الذكاء الاصطناعي في مكافحة الإرهاب دون الإخلال بالحقوق والحريات الرقمية.
- ضرورة سن قوانين وطنية واضحة تنظم الاستخدام الأمني للذكاء الاصطناعي، بحيث تُحدد آليات جمع البيانات الشخصية، وضوابط معالجتها، وقواعد حمايتها من الاستغلال غير المشروع، بما يمنع الاعتداء على سيادة الأفراد الرقمية أو المساس بخصوصيتهم، ويضمن في نفس الوقت توظيفًا مشروعًا للتقنيات الذكية في المجالات الأمنية.

- العمل على بناء منظومات وطنية للرصد والتحليل التنبؤي تُعنى بكشف أنماط التطرف مبكرًا، وذلك عبر إنشاء مراكز وطنية متخصصة تعتمد على تقنيات تحليل البيانات الضخمة والخوارزميات الذكية، للمساعدة في تفكيك الشبكات الإرهابية قبل انتقالها إلى مرحلة التنفيذ.
-ضرورة تعزيز التعاون بين الدول في مجال تبادل الاستخبارات الرقمية، وذلك من خلال اتفاقيات ثنائية أو متعددة الأطراف تضمن مشاركة البيانات المتعلقة بالإرهاب الرقمي وفق ضوابط قانونية تشريعية تحمي سيادة الدول وتضمن سلامة إجراءات تبادل المعلومات.
- العمل على تطوير معايير أخلاقية مُلزمة لاستخدام الذكاء الاصطناعي في المجال الأمني، تُحدد قواعد الاستهداف، وتمنع التمييز أو إساءة استخدام البيانات، وتقيّد السلطات الرقابية حتى لا تتحول التقنيات الحديثة إلى أدوات مراقبة واسعة تطال الأفراد دون مسوغ قانوني.
- ضرورة الاستثمار في تدريب الكوادر الأمنية الرقمية عبر إعداد متخصصين في الذكاء الاصطناعي والتحليل السيبراني، وتعزيز الشراكات بين المؤسسات الأمنية والجامعات ومراكز البحث لتكوين قدرات وطنية قادرة على التصدي للإرهاب التقني دون الاعتماد الكامل على التكنولوجيا الأجنبية.
- تشدد الدراسة على أهمية دمج البعد السلوكي والاجتماعي في مكافحة الإرهاب الرقمي، عبر تحليل الخطابات المتطرفة والمنصات الدعائية من منظور نفسي اجتماعي يساعد في تحديد الفئات المستهدفة والشرائح الأكثر عرضة للاستقطاب، ويُستكمل ذلك بإطلاق مبادرات وطنية للتثقيف الرقمي تهدف إلى رفع وعي الشباب بمخاطر الدعاية الإرهابية على الإنترنت وبأهمية حماية بياناتهم الشخصية، ما يسهم في تقليل فرص التجنيد الرقمي وتعزيز الأمن المجتمعي ضد التطرف الإلكتروني.

18-الهوامش :

1- Jayakumar, S. (2023). Cyberterrorism in the age of artificial intelligence: Digital radicalization and global security threats. Journal of Cybersecurity Studies, 12(2), 55–72.
2- -Bukhari, A. (2021). Artificial intelligence in counterterrorism: Predictive analytics and early threat detection. International Review of Security & Intelligence, 8(1), 25–40.
3- -Iftikhar, S. (2024). AI-enabled counterterrorism: Biometric surveillance and data-driven intelligence. Journal of Digital Security, 5(1), 11–29.
4- Qureshi, F. (2024). Legal and ethical implications of AI in counterterrorism: Balancing privacy and national security. International Journal of Law & Digital Governance, 9(3), 101–120.
5- -Russell, S., & Norvig, P. (2021). Artificial intelligence: A modern approach (4th ed.). Pearson Education.
6- -Baines, P., & Jones, E. (2023). Artificial intelligence and predictive counterterrorism: Ethical implications in digital surveillance. Journal of Security and Intelligence Studies, 18(2), 101–120.
7- -Jain, A. K., Ross, A., & Nandakumar, K. (2016). Introduction to biometrics. Springer.
8- Mueller, J., & Stewart, M. (2022). Cyber deterrence and smart security against terrorism. Security Studies Review, 15(2), 80–99.
9- -Conway, M. (2020). Understanding cyberterrorism: Analysis and implications. Journal of Terrorism and Political Violence, 32(3), 556–573.
10- -Hoffman, B. (2017). Inside terrorism. Columbia University Press.
11- -Jayakumar, S. (2023). Cyberterrorism in the age of artificial intelligence: Digital radicalization and global security threats. Journal of Cybersecurity Studies, 12(2), 55–72.

12- -Baines, P., & Jones, E. (2023). Artificial intelligence and predictive counterterrorism: Ethical implications in digital surveillance. Journal of Security and Intelligence Studies, 18(2), 101–120.
13- Conway, M. (2020). Understanding cyberterrorism: Analysis and implications. Journal of Terrorism and Political Violence, 32(3), 556–573.
14- Jain, A. K., Ross, A., & Nandakumar, K. (2016). Introduction to biometrics. Springer.
15- -Jayakumar, S. (2023). Cyberterrorism in the age of artificial intelligence: Digital radicalization and global security threats. Journal of Cybersecurity Studies, 12(2), 55–7
16- Mueller, J., & Stewart, M. (2022). Cyber deterrence and smart security against terrorism. Security Studies Review, 15(2), 80–99.
17- Baines, P., & Jones, E. (2023). Artificial intelligence and predictive counterterrorism: Ethical implications in digital surveillance. Journal of Security and Intelligence Studies, 18(2), 101–120.
18- Conway, M. (2020). Understanding cyberterrorism: Analysis and implications. Journal of Terrorism and Political Violence, 32(3), 556–573.
19- . Mueller, J., & Stewart, M. (2022). Cyber deterrence and smart security against terrorism. Security Studies Review, 15(2), 80–99.
20- UNICRI. (2021). Countering terrorism online with artificial intelligence – An overview for law enforcement and counter-terrorism agencies in South Asia and -South-East Asia. United Nations Interregional Crime and Justice Research Institute
21- -Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., et al. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. Oxford University.
22- -UNOD. (2021). Use of data and artificial intelligence in counter-terrorism. United Nations Office on Drugs and CrimeAJSS
23- - Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., et al. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. Oxford University.
24- -UNICRI. (2021). Countering terrorism online with artificial intelligence – An overview for law enforcement and counter-terrorism agencies in South Asia and -South-East Asia. United Nations Interregional Crime and Justice Research Institute
25- -Crawford, K., & Paglen, T. (2019). Excavating AI: The politics of images in machine learning training sets. The AI Now Institute.
26- Conway, M. (2020). Understanding cyberterrorism: Analysis and implications. Journal of Terrorism and Political Violence, 32(3), 556–573.
27- Mueller, J., & Stewart, M. (2022). Cyber deterrence and smart security against terrorism. Security Studies Review, 15(2), 80–99.
28- Jain, A. K., Ross, A., & Nandakumar, K. (2016). Introduction to biometrics. Springer.
29- -Jayakumar, S. (2023). Cyberterrorism in the age of artificial intelligence: Digital radicalization and global security threats. Journal of Cybersecurity Studies, 12(2), 55–72.
30- Conway, M. (2020). Understanding cyberterrorism: Analysis and implications. Journal of Terrorism and Political Violence, 32(3), 556–573.
31- -Jayakumar, S. (2023). Cyberterrorism in the age of artificial intelligence: Digital radicalization and global security threats. Journal of Cybersecurity Studies, 12(2), 55–72.
32- -Jayakumar, S. (2023). Cyberterrorism in the age of artificial intelligence: Digital radicalization and global security threats. Journal of Cybersecurity Studies, 12(2), 55–72.
33- Mueller, J., & Stewart, M. (2022). Cyber deterrence and smart security against terrorism. Security Studies Review, 15(2), 80–99.

34- Mueller, J., & Stewart, M. (2022). Cyber deterrence and smart security against terrorism. Security Studies Review, 15(2), 80–99.
35- -Jayakumar, S. (2023). Cyberterrorism in the age of artificial intelligence: Digital radicalization and global security threats. Journal of Cybersecurity Studies, 12(2), 55–72.
36- Conway, M. (2020). Understanding cyberterrorism: Analysis and implications. Journal of Terrorism and Political Violence, 32(3), 556–573.
37- Baines, P., & Jones, E. (2023). Artificial intelligence and predictive counterterrorism: Ethical implications in digital surveillance. Journal of Security and Intelligence Studies, 18(2), 101–120
38- Mueller, J., & Stewart, M. (2022). Cyber deterrence and smart security against terrorism. Security Studies Review, 15(2), 80–99.
39- Aldausari, A., et al. (2022). Advances in generative AI for multimodal data. Journal of Artificial Intelligence Research, 45(3), 201–227.
40- -UNOD. (2021). Use of data and artificial intelligence in counter-terrorism. United Nations Office on Drugs and CrimeAJSS
41- Abanes, M. (1996). Counterterrorism policies and state responses. Cambridge University Press.
42- -الزبيدي، م. (2020). الإرهاب السيبراني وضرورة بناء منظومة قانونية عربية مشتركة. مجلة القانون والأمن الرقمي، 4(1)، 15–36.
43- -Baker, D., & Renz, B. (2020). The impact of artificial intelligence on intelligence analysis. Intelligence and National Security, 35(7), 891–908.
44- -Baker, D., & Renz, B. (2020). The impact of artificial intelligence on intelligence analysis. Intelligence and National Security, 35(7), 891–908.
45- -منصور، أ. (2022). الذكاء الاصطناعي والأمن السيبراني في مكافحة الإرهاب. مجلة دراسات أمنية معاصرة، 5(2)، 33–58.

46- -Bartlett, J., & Miller, C. (2012). The edge of violence: Towards telling the difference between violent and non-violent radicalization. Terrorism and Political Violence, 24(1), 1–21.
47- -UNICRI. (2021). Countering terrorism online with artificial intelligence – An overview for law enforcement and counter-terrorism agencies in South Asia and -South-East Asia. United Nations Interregional Crime and Justice Research Institute

48- -Bartlett, J., & Miller, C. (2012). The edge of violence: Towards telling the difference between violent and non-violent radicalization. Terrorism and Political Violence, 24(1), 1–21.
49- Biddle, S., et al. (2012). Understanding armed groups: Structure, strategy, and adaptation. RAND Corporation.
50- -Baker, D., & Renz, B. (2020). The impact of artificial intelligence on intelligence analysis. Intelligence and National Security, 35(7), 891–908.
51- -Bartlett, J., & Miller, C. (2012). The edge of violence: Towards telling the difference between violent and non-violent radicalization. Terrorism and Political Violence, 24(1), 1–21.
52- Baker, D., & Renz, B. (2020). The impact of artificial intelligence on intelligence analysis. Intelligence and National Security, 35(7), 891–908.

53- Crawford, K., & Paglen, T. (2019). Excavating AI: The politics of images in machine learning training sets. The AI Now Institute.
54- Crawford, K., & Paglen, T. (2019). Excavating AI: The politics of images in machine learning training sets. The AI Now Institute.
55- Qureshi, F. (2024). Legal and ethical implications of AI in counterterrorism: Balancing privacy and national security. International Journal of Law & Digital Governance, 9(3), 101–120.
56- Mueller, J., & Stewart, M. (2022). Cyber deterrence and smart security against terrorism. Security Studies Review, 15(2), 80–99.
57- -Marr, B. (2021). Artificial intelligence in practice: How 50 successful companies used AI and machine learning to solve problems. Wiley.
58- Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., et al. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. Oxford University.
59- Crawford, K., & Paglen, T. (2019). Excavating AI: The politics of images in machine learning training sets. The AI Now Institute.
60- -Scharre, P. (2018). Army of none: Autonomous weapons and the future of war. W. W. Norton & Company.
61- -Crawford, K. (2021). The atlas of AI: Power, politics, and the planetary costs of artificial intelligence. Yale University Press.
62- Baines, P., & Jones, E. (2023). Artificial intelligence and predictive counterterrorism: Ethical implications in digital surveillance. Journal of Security and Intelligence Studies, 18(2), 101–120.
63- Conway, M. (2020). Understanding cyberterrorism: Analysis and implications. Journal of Terrorism and Political Violence, 32(3), 556–573.
64- Mueller, J., & Stewart, M. (2022). Cyber deterrence and smart security against terrorism. Security Studies Review, 15(2), 80–99
65- Baines, P., & Jones, E. (2023). Artificial intelligence and predictive counterterrorism: Ethical implications in digital surveillance. Journal of Security and Intelligence Studies, 18(2), 101–120.
66- Mueller, J., & Stewart, M. (2022). Cyber deterrence and smart security against terrorism. Security Studies Review, 15(2), 80–99
67- ain, A. K., Ross, A., & Nandakumar, K. (2016). Introduction to biometrics. Springer.
68- Conway, M. (2020). Understanding cyberterrorism: Analysis and implications. Journal of Terrorism and Political Violence, 32(3), 556–573.
69- -Bergman, R., & Goldman, A. (2023). The 7 October intelligence failure. Haaretz Investigations.

19-المراجع :

19-1-المراجع العربية :

-الزبيدي، م. (2020). الإرهاب السيبراني وضرورة بناء منظومة قانونية عربية مشتركة. مجلة القانون والأمن الرقمي، 4(1).
-منصور، أ. (2022). الذكاء الاصطناعي والأمن السيبراني في مكافحة الإرهاب. مجلة دراسات أمنية معاصرة، 5(2).

19-2- المراجع الأجنبية :

-Abanes, M. (1996). Counterterrorism policies and state responses. Cambridge University Press.

-Aldausari, A., et al. (2022). Advances in generative AI for multimodal data. Journal of Artificial Intelligence Research, 45(3).
-Anderson, J. (2015). Neural networks in security operations. Security Studies Review, 12(4).
-Awad, E., et al. (2018). The moral machine experiment. Nature, 563(7729).
-Avdan, N., & Uzonyi, G. (2017). The security dilemma in counterterrorism. Journal of Global Security Studies, 2(1).
-Baker, D., & Renz, B. (2020). The impact of artificial intelligence on intelligence analysis. Intelligence and National Security, 35(7).
-Bartholomees, J. B. (2008). The theory of war and strategy. U.S. Army War Collegem,18-19.
-Bartlett, J., & Miller, C. (2012). The edge of violence: Towards telling the difference between violent and non-violent radicalization. Terrorism and Political Violence, 24(1).
-Bergman, R., & Goldman, A. (2023). The 7 October intelligence failure. Haaretz Investigations.
-Biddle, S., et al. (2012). Understanding armed groups: Structure, strategy, and adaptation. RAND Corporation.
-Bobbitt, P. (2003). Terror and consent: The wars for the twenty-first century. Knopf.
-Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., et al. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. Oxford University.
-Bukhari, A. (2021). Artificial intelligence in counterterrorism: Predictive analytics and early threat detection. International Review of Security & Intelligence, 8(1).
-Caliskan, A., Bryson, J. J., & Narayanan, A. (2017). Semantics derived automatically from language corpora contain human-like biases. Science, 356(6334).
-Cassam, Q. (2022). Extremism: A philosophical analysis. Routledge.
-Crawford, K. (2021). The atlas of AI: Power, politics, and the planetary costs of artificial intelligence. Yale University Press.
-Crawford, K., & Paglen, T. (2019). Excavating AI: The politics of images in machine learning training sets. The AI Now Institute.
-Gardell, M. (2003). Gods of the blood: The pagan revival and white separatism. Duke University Press.
-Hoffman, B. (2017). Inside terrorism. Columbia University Pres.
-Iftikhar, S. (2024). AI-enabled counterterrorism: Biometric surveillance and data-driven intelligence. Journal of Digital Security, 5(1).
-Jayakumar, S. (2023). Cyberterrorism in the age of artificial intelligence: Digital radicalization and global security threats. Journal of Cybersecurity Studies, 12(2).
-Kfir, I. (2020). Understanding and countering violent extremism: The role of de-radicalization programmes. Journal of Policing, Intelligence and Counter Terrorism, 15(1).
-Marr, B. (2021). Artificial intelligence in practice: How 50 successful companies used AI and machine learning to solve problems. Wiley.
-Qureshi, F. (2024). Legal and ethical implications of AI in counterterrorism: Balancing privacy and national security. International Journal of Law & Digital Governance, 9(3), 101–120.
-Scharre, P. (2018). Army of none: Autonomous weapons and the future of war. W. W. Norton & Company.
-UNICRI. (2021). Countering terrorism online with artificial intelligence – An overview for law enforcement and counter-terrorism agencies in South Asia and -South-East Asia. United Nations Interregional Crime and Justice Research Institute.
-UNOD. (2021). Use of data and artificial intelligence in counter-terrorism. United Nations Office on Drugs and CrimeAJSS.