Security Policy Papers
أوراق السياسات الأمنية
https://spp.nauss.edu.sa/index.php/spp
ورقة تحليل سياسات أمنية

استخدام التقنيات الحديثة في الإرهاب

Utilization of Modern Technologies in Terrorism

المخرجات الرئيسة

- التكيف السريع من جانب أجهزة إنفاذ القانون والأجهزة الأمنية بتوفير التعليمات والتشريعات بشأن جمع الأدلة الرقمية وحفظها واستخدامها في القضايا المرتبطة باستخدام التكنولوجيا في العمليات الإرهابية.
- تصميم وتطوير البرامج التدريبية للعاملين في الأجهزة الأمنية في المجالات الأساسية المرتبطة باستخدام التقنيات الحديثة والفضاء السيبراني «مثل: الأدلة الجنائية الرقمية، والأمن السيبراني، والجريمة السيبرانية، والاستخبارات السيبرانية، وعلم البيانات».
- تعزيز آليات التعاون العربي لإيجاد حلول ابتكارية لمكافحة التهديدات التقنية المستخدمة من الجماعات الإرهابية.

ملخص

لقد تطورت التكنولوجيا بسرعة كبيرة في السنوات الأخيرة؛ حتى إنها أثَّرت على الكثير من جوانب الحياة، ومن ذلك استخدام التكنولوجيا من قبل الجماعات الإرهابيَّة. وفي حين أن التقدم التكنولوجي له فوائد كثيرة، فإنه ينطوي أيضًا على مخاطر كبيرة، خاصة في ضوء التهديد الإرهابي؛ حيث أصبحت الطائرات بدون طيار والشبكة العنكبوتية والذكاء الاصطناعي أدوات شائعة بشكل متزايد تستخدمها الجماعات الإرهابيَّة

Abstract

This paper examines the rapid advancement of technology and its implications for global security, particularly in the context of its use by terrorist organizations. While technological progress, such as the development of drones, the internet, and artificial intelligence, offers numerous benefits, it simultaneously presents significant security risks. Terrorist groups increasingly exploit these technologies to carry out

لتنفيذ عملياتها. وتتناول الدراسة آثار هذه التقنيات، مع تأكيد أهمية تحديد المخاطر التي تشكلها على الأمن العالمي ومواجهتها. وتسلط الدراسة الضوء على أنه في حين أن تحسينات التكنولوجيا قد تعزِّز عمليات مكافحة الإرهاب، فإنها أيضًا تعقد القضية، وتحتاج إلى التكيف السريع من جانب أجهزة إنفاذ القانون والأمن. وتؤكد الدراسة ضرورة إيجاد حلول إبداعية، والعمل الجماعي لمكافحة هذه التهديدات المتطورة باستمرار من خلال فحص الكثير من التقنيات التي يستخدمها الإرهابيون. ومن أجل الحفاظ على سلامة المجتمع، فإن معالجة العلاقة بين التكنولوجيا والإرهاب تتطلب نهجًا متعدد الأوجه يشتمل على تدابير وقائية إلى جانب حلول مبتكرة.

sophisticated operations, posing new challenges for counterterrorism efforts. The research underscores the importance of identifying and mitigating these risks, while recognizing the dual role of technology in both enhancing and complicating counterterrorism strategies. The paper calls for a swift adaptation by law enforcement and security agencies, highlighting the necessity of innovative solutions and collaborative efforts to address the evolving nature of these threats. A multifaceted approach, incorporating both preventive and innovative measures, is deemed essential for effectively managing the intersection of technology and terrorism and safeguarding global security.

1. المقدمة

تتطور التقنيات الحديثة بوتيرة سريعة؛ ممَّا يغير حياتنا اليومية، ويخلق آفاقًا جديدة مليئة بالتحديات والفرص. فقد أصبحت التقنيات الحديثة؛ مثل: الذكاء الاصطناعي، والاتصالات، والطائرات بدون طيار، جزءًا لا يتجزأ من نسيج المجتمع الحديث؛ حيث تُستخدم في جميع جوانب الحياة، من التعليم والرعاية الصحية إلى التجارة والأمن. ومع ذلك، فإن هذه الابتكارات، على الرغم من فوائدها الكثيرة، فإنها تحمل في طياتها أيضًا مخاطر كبيرة، خصوصًا عندما تُستخدم لأغراض غير أخلاقية أو ضارة. حيث تمتلك كل "تقنية" تقنية مضادة؛ ممَّا يجعلها أداة ذات حدين.

إن امتلاك كل "تقنية" لجوانب مضادة يُبرز التحديات التي تواجهها المجتمعات في العصر الرقمي. التوسع الهائل في تكنولوجيا المعلومات ساعد المنظمات الإرهابيَّة إلى حدٍ كبيرٍ في مساعيها وتنفيذ أنشطتها. وقد أثبتت هذه التقنية فائدتها للإرهابيين والمتطرفين والناشطين على حد سواء؛ حيث أصبحت أدوات فعَّالة لتعزيز جهودهم. وعلى الرغم من أن الجماعات الإرهابيَّة تستخدم الإنترنت لنشر أفكارها وتجنيد أعضائها والتواصل، فإنه لا يمكن الاستهانة بأنه في المستقبل القريب، يمكن استخدام الإنترنت لارتكاب هجوم إرهابي يتسبب في تأثير هائل على المجتمع من خلال الاستهداف المباشر للبنية التحتية الحيوية [1].

يُعدُّ الإنترنت بمنزلة ساحة حيوية لنشر الأفكار المتطرفة؛ حيث تستخدم جميع الجماعات الإرهابيَّة تقريبًا الإنترنت لتنفيذ عملياتها، ومن ذلك نشر الدعاية، وتسهيل الاتصالات، وتجنيد أعضاء جدد لمجموعاتهم، وجمع الأموال.

فقد اتسع المجال، نتيجة لإساءة استخدام الإنترنت، ليس فقط ليشمل المجال الوطني، ولكن أيضًا إلى المجالات غير الوطنية والعالمية. على سبيل المثال، يواجه تحالف الناتو مجموعة من التحديات في مجالات الصراع الناشئة؛ حيث الاستخدام الواسع النطاق لوسائل التواصل الاجتماعي والشبكات الاجتماعية والرسائل الاجتماعية وتقنيات الأجهزة المحمولة يتيح الآن مجالًا جديدًا يعرف بالحرب المعرفية [2]، على سبيل المثال، تُستخدم هذه الجماعات منصات التجارة الإلكترونية لشراء السلع غير المشروعة؛ مثل: الأسلحة والمتفجرات، وغالبًا عبر الشبكة المظلمة؛ ممَّا يعقد جهود إنفاذ القانون في تعقب الأنشطة غير القانونية. كما أن الذكاء الاصطناعي يتيح لهم تحليل البيانات بشكل أكثر فاعلية؛ ممَّا يساعدهم على تنفيذ إستراتيجيات معقدة للدعاية والتجنيد. ووفقًا لدراسات متعددة، فإن استخدام هذه التقنيات الحديثة يُعدُّ خطوة إستراتيجية في تعزيز العمليات الإرهابيَّة؛ حيث تتمكن الجماعات من توجيه رسائلهم بشكل دقيق نحو الأفراد المعرضين للتطرف.

علاوة على ذلك، فإن استخدام الطائرات بدون طيار يُمثل تهديدًا جديدًا؛ حيث يُمكن استخدامها للمراقبة، والهجمات الدقيقة؛ ممَّا يُقلل من المخاطر التي تواجه العناصر الإرهابيَّة أثناء تنفيذ عملياتهم. وقد أسهم هذا التطور التكنولوجي في جعل التهديدات أكثر تعقيدًا؛ ممَّا يتطلب من الأجهزة الأمنية تكثيف جهودها لمواكبة هذه التغيرات.

في هذا الصدد، تقدم هذه الورقة دراسة عن التقنيات الرئيسة التي يستخدمها الإرهابيون بشكل متزايد لتحقيق أهدافهم وكيفية تطوير إستراتيجيات فعَّالة لمواجهة التهديدات المرتبطة بها.

إن إدراك المخاطر المرتبطة بالتكنولوجيا الحديثة وتطبيقها في سياق مكافحة الإرهاب يُعدُّ أمرًا حيويًّا؛ لتحسين الأمان العالمي. فالتعاون بين الدول، وكذلك بين القطاعين العام والخاص، سيكون ضروريًّا لتطوير حلول مبتكرة تحد من استخدام هذه التقنيات في الأنشطة الإرهابيَّة، وتساعد في الحفاظ على الأمن والاستقرار في المجتمع. بالإضافة إلى ذلك، فإن هذه التقنيات تفرض تحديات كبيرة على الجهود الأمنية الدولية الرامية إلى تحييد مثل هذه التهديدات. ويشكل فهم هذه التقنيات أمرًا ضروريًّا لخلق تدابير فعَّالة لمكافحة الإرهاب المعاصر.

2. استخدامات التقنيات الحديثة في الإرهاب

تستخدم الجماعات الإرهابيَّة التقنيات الحديثة مثل: الذكاء الاصطناعي، والطائرات بدون طيار، والإنترنت، والفضاء السيبراني لتعزيز أنشطتها وعملياتها الإرهابيَّة. حيث يسهل الذكاء الاصطناعي مهام مثل: تحليل البيانات للتخطيط الإستراتيجي وتطوير الدعاية المغرية للتجنيد والتطرف. كما تُستخدم الطائرات بدون طيار للمراقبة والضربات المستهدفة؛ ممَّا يسمح للعناصر بتنفيذ العمليات بدقة أكبر، وتقليل المخاطر على أنفسهم. علاوة على ذلك، تعمل شبكة الإنترنت كوسيلة رئيسة للاتصال ونشر الدعاية وجمع الأموال؛ ممَّا يسمح لهذه المنظمات بالعمل

على نطاق عالمي، وتتناول هذه الدراسة تلك الموضوعات بشكل أكثر تعمقًا وتدرس كيفية إسهام هذه التقنيات في تطور سيناريو الإرهاب وتداعياته.

1.2 الذكاء الاصطناعي

اكتسب الذكاء الاصطناعي مكانة مرموقة في مجموعة متنوعة من المجالات؛ ممَّا أسفر عن تقدم ملموس في تكنولوجيا المعلومات والأنظمة الوظيفية. وفقًا لمنظمة التعاون الاقتصادي والتنمية، يُعتبر الذكاء الاصطناعي "تقنية متعددة الاستخدامات، تمتلك القدرة على تحسين رفاهية الأفراد والمساهمة في النشاط الاقتصادي العالمي بشكل إيجابي ومستدام، وزيادة الابتكار والإنتاجية، والمساعدة في مواجهة التحديات العالمية الكبرى" تهدف هذه الأنظمة إلى تحقيق مستويات عالية من الأتمتة؛ ممَّا يعزِّز من كفاءتها وفاعليتها.

علاوة على ذلك، أصبح الذكاء الاصطناعي أحد أبرز أدوات التطور التكنولوجي التي تصدرت النقاشات العامة والأكاديمية والسياسية في السنوات الأخيرة؛ نظرًا لتأثيره الواسع على مختلف جوانب الحياة اليومية.

يتجلى الذكاء الاصطناعي في أشكال متنوعة، ومن أبرز هذه الأشكال هو الذكاء الاصطناعي التوليدي، الذي أظهر إمكانات هائلة في الكثير من التخصصات في الآونة الأخيرة. يُمكن للذكاء الاصطناعي التوليدي، على وجه الخصوص، إنتاج محتوى جديد استجابة للأوامر؛ ممَّا يمكّنه من إحداث ثورة في مجالات متعددة، مثل: البحث العلمي، والترفيه، والرعاية الصحية، والتعليم.

من الضروري أن ندرك أن الذكاء الاصطناعي التوليدي قادر على إنشاء نصوص وصور وأصوات وفيديوهات ومحاكاة متعددة الاستخدامات باستخدام تقنيات التعلم الآلي؛ حيث يعمل هذا النوع من الذكاء الاصطناعي عن طريق الاستفادة من مجموعات بيانات ضخمة ومعلمات تم تصميمها؛ لتكون مشابهة للتواصل البشري؛ ممَّا يعزِّز من قدرته على إنتاج محتوى يعكس الأفكار والأنماط البشرية. حيث يتمثل التمييز الأساسي بين الذكاء الاصطناعي التوليدي وأنواع أخرى من الذكاء الاصطناعي في أنه على عكس أنظمة التعلم الآلي الأخرى، فإن أنظمة الذكاء الاصطناعي التوليدي قادرة على إنتاج مخرجات جديدة، بالإضافة إلى التنبؤات والتصنيفات البسيطة.

يقدم الذكاء الاصطناعي التوليدي مجموعة واسعة من الفوائد، خاصة عند استخدامه بطرق خبيثة؛ حيث يتراوح تأثيره من التجنيد التفاعلي إلى إنتاج الدعاية، وتغيير سلوك الأفراد عبر وسائل التواصل الاجتماعي. وتتبنى المنظمات الإرهابيَّة هذه التقنيات الجديدة باهتمام متزايد؛ إذ تسعى جاهدة لاستغلال الفرص التي تتيحها التطورات التكنولوجية لصالحها.

في ضوء الأحداث الأخيرة، تُبرز هذه الورقة بعض المخاطر المرتبطة باستخدام الذكاء الاصطناعي التوليدي من قبل هذه الجماعات، وتفحص كيف تؤثر هذه

الأدوات على سلوك الأفراد، وهو هدف رئيس لهذه المنظمات. نظرًا للإمكانات الكبيرة التي تتمتع بها هذه الأداة، من المحتمل أن تجد المنظمات الإرهابيَّة طرقًا جديدة للاستفادة منها في المستقبل؛ ممَّا يستدعي ضرورة الانتباه إلى المخاطر المرتبطة بذلك.

في الوقت الراهن، يتركز الاهتمام بشكل كبير على كيفية استغلال الجماعات الإرهابيَّة للتقنيات المعتمدة على الذكاء الاصطناعي في المستقبل. وتشمل هذه الاستخدامات الذكاء الاصطناعي، والتجنيد التفاعلي، والدعاية المكثفة، وإستراتيجيات الخداع، وحتى العمليات الحربية. وتُعدُّ الدعاية إحدى الوسائل الأساسية التي تستخدمها هذه الجماعات لنشر مبادئها وأفكارها المتطرفة، وتسهم التقنيات الحديثة بشكل كبير في تعزيز فاعلية هذه الرسائل.

من خلال الاستفادة من الذكاء الاصطناعي التوليدي، تتمكن الجماعات الإرهابيَّة من نقل رسائل الدعاية بشكل أكثر سلاسة وتأثيرًا؛ ممَّا يجعلها تتناسب بشكل أكبر مع أهدافها الإستراتيجية. يُمكن استخدام هذه الدعاية كوسيلة لنشر خطاب الكراهية والأيديولوجيات المتطرفة؛ حيث يُعزز استخدام الصور ومقاطع الفيديو، بالإضافة إلى الأصوات الاصطناعية، من قدرة الجماعات على الوصول إلى جمهور واسع. فعلى سبيل المثال، يمكن استخدام صور مزيفة لضحايا أو أطفال جرحى لإحداث تأثير عاطفي قوي على المشاهدين؛ ممَّا يسهم في توسيع نطاق الدعاية وزيادة تأثير الرسائل على مواقف الناس وعواطفهم.

إن إدماج الذكاء الاصطناعي التوليدي في عمليات الدعاية يمكن أن يخلق واقعًا زائفًا؛ ممَّا يمكّن الجهات الفاعلة المهددة من زرع الفوضى والاضطراب من خلال المعلومات المضللة؛ فقد يؤدي تحميل محتوى تم إنتاجه باستخدام الذكاء الاصطناعي على منصات التواصل الاجتماعي إلى زيادة نسبة الوصول؛ ممَّا يتيح لملايين المستخدمين مشاركة هذه المعلومات بسرعة. نتيجة لذلك، يمكن اعتبار وسائل التواصل الاجتماعي سلاحًا قويًّا في حروب التضليل؛ حيث يصبح من الصعب على الأفراد الاعتماد على المعلومات التي يتلقونها؛ نظرًا لقدرة الذكاء الاصطناعي التوليدي على خلق الكثير من التحديات في مجال الاتصالات والإعلام عبر الإنترنت، خاصة فيما يتعلق بالتضليل والمعلومات المضللة.

إن الانتقال من الدعاية إلى التجنيد التفاعلي ليس سوى مرحلة أخرى في استغلال الإرهابيين للذكاء الاصطناعي التوليدي. ويمكن ربط الاثنين بشكل وثيق للغاية؛ حيث يمكن لبرامج الدردشة المدعومة بالذكاء الاصطناعي التفاعل مع المجندين المحتملين من خلال تقديم معلومات مخصصة لهم؛ بناءً على اهتماماتهم ووجهات نظرهم؛ ممَّا يجعل رسائل المجموعة المتطرفة تبدو أكثر صلة باهتماماتهم. في عملية التجنيد، يمكن استخدام الروبوت لجذب انتباه الضحايا المحتملين من خلال التواصل معهم والرد على ملاحظاتهم. وفي وقت لاحق، قد يتولى إنسان الدردشة ويشارك بشكل أكثر شخصية. من ناحية أخرى، تسمح التكنولوجيا

الحديثة، مثل: برامج الدردشة التفاعلية مثل ChatGPT، للجماعات الإرهابيَّة بتقديم تجربة شبيهة بالإنسان حتى في غياب التدخل البشري.

إن هذا الوضع يتطلب استجابة حازمة من المجتمع الدولي؛ حيث يجب أن تكون هناك إستراتيجيات فعَّالة لمراقبة المحتوى الذي يتم تداوله عبر هذه المنصات. ويجب أن تتعاون الحكومات، ومنظمات المجتمع المدني، والقطاع الخاص لمواجهة هذه التحديات، والعمل على تعزيز الوعي حول مخاطر المعلومات المضللة وكيفية التصدي لها.

2.2 الفضاء السيبراني والإرهاب السيبراني

مع ظهور التقنيات الأكثر تقدمًا، أصبحت الشبكات تتمتع بنطاق عالمي؛ ممَّا يتيح للناس التواصل بشكل أسرع وأكثر كفاءة وبصورة شبه مجهولة مع مجموعة واسعة من الناس في جميع أنحاء العالم. وبفضل قدرتها الخاصة على تسهيل تبادل الأفكار والمعلومات، وهو ما يُعترف به كحق أساسي من حقوق الإنسان، تقدم تقنيات الإنترنت الكثير من المزايا. حيث شهد الإنترنت نموًا كبيرًا في الحجم وإمكانية الوصول في السنوات الأخيرة، وقد أدَّى هذا إلى زيادة كمية المحتوى الرقمي الذي يتم إنشاؤه ومشاركته على مواقع الويب؛ مثل: المدونات والبوابات الإلكترونية ومواقع التواصل الاجتماعي وتطبيقات المراسلة الفورية. ومع ذلك، يجب الاعتراف بأن نفس التكنولوجيا التي تجعل هذا النوع من الاتصالات ممكنًا يمكن استخدامها أيضًا لارتكاب أعمال إرهابية؛ حيث أصبح الإنترنت أداة حيوية للإرهاب الدولي. حيث يستخدم الإرهابيون شبكات الاتصالات التجارية وتطبيقات الرسائل المشفرة والاستخبارات مفتوحة المصدر للحصول على معلومات حول المباني المستهدفة، وتتبع التحركات وإجراء المراقبة. كما أصبحت الجماعات الإرهابيَّة قادرة الآن على تنسيق وتنفيذ أعمال كانت غير قابلة للتحقيق في السابق [3].

هناك الكثير من الأعمال الإرهابيَّة، بما في ذلك تمويل الإرهاب والتجارة الإلكترونية، يمكن تنفيذها بفضل الإنترنت ووسائل التواصل الاجتماعي؛ حيث سلط المؤتمر العالمي في مراكش، المغرب، الذي شارك فيه 220 متخصصًا في الأمن الكيميائي من أكثر من 70 دولة، والذي عقد في مؤتمر الإنتربول العالمي الثالث للأمن الكيميائي والتهديدات الناشئة؛ الضوء على استخدام الإرهابيين للتجارة الإلكترونية. كما بحث المؤتمر التدابير الرامية إلى مكافحة المخاطر المتزايدة؛ مثل: استخدام الإرهابيين للتجارة الإلكترونية والتقنيات الجديدة للحصول على المواد الخطرة والسلائف. كانت هناك أمثلة على تقنيات التحقيق التي قد تستخدمها وكالات إنفاذ القانون لتعقب وتوجيه الاتهام إلى الأشخاص الذين يشترون أو يبيعون مواد بشكل غير قانوني على الشبكة المظلمة. وقد وفرت هذه المحادثات للمشاركين آليات التكيف مع تطبيق التقنيات المعقدة لأغراض خبيثة [4].

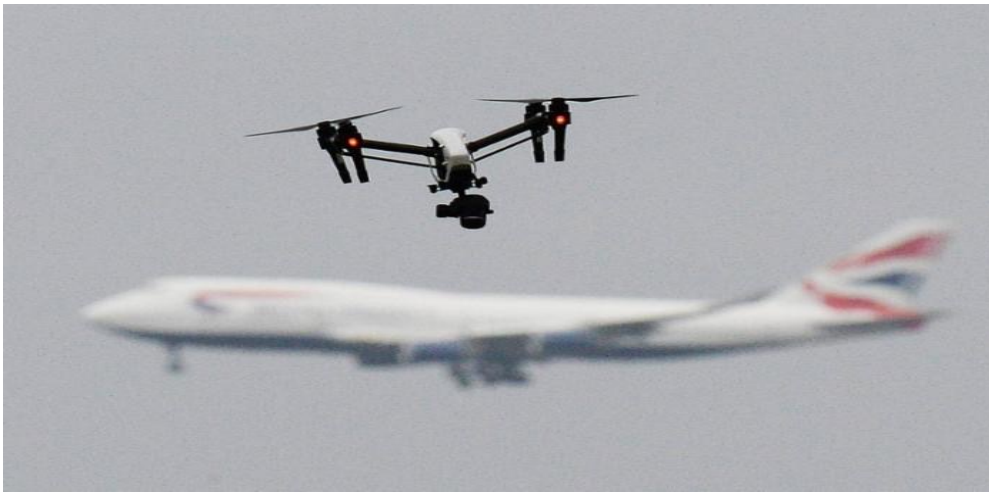
فعلى سبيل المثال، أصبحت المعلومات والاتصالات والتكنولوجيا تشكل أهمية بالغة في جنوب شرقي

أوروبا، كما هي الحال في مختلف أنحاء العالم. وقد دفعت الرغبة في التحديث، والسعي إلى التكامل الأوروبي الأطلسي، والحاجة التي لا يمكن إنكارها للاستثمار الأجنبي المباشر، بلدان جنوب شرقي أوروبا إلى الاستثمار في التنمية السيبرانية. وعلاوة على ذلك، تطور هذا المجال كموقع أساسي للتفاعلات الاجتماعية والاقتصادية والسياسية في منطقة جنوب شرقي أوروبا. ومع ذلك، فإن الديناميكية التي تحركها تكنولوجيا المعلومات والاتصالات كانت لها عواقب إيجابية وأخرى ضارة. ولم يصاحب الاعتماد المتزايد على الفضاء السيبراني والتكنولوجيا في جنوب شرقي أوروبا التركيز على الأمن. حيث أثبتت الممارسات الأخيرة أن عالم الفضاء السيبراني تطور إلى ساحة معركة للحرب الإيديولوجية والمعلوماتية للإرهابيين المعاصرين، فضلًا عن كونه وسيلة للتطرف العالمي. وقد أكد حلف شمال الأطلسي في كثير من الأحيان وجود مخاطر حقيقية من التكنولوجيا والفضاء السيبراني ضد أعضائه وحلفائه. ومن المهم أن نتذكر أنه في حين أن البوسنة والهرسك، ومقدونيا، والجبل الأسود، وصربيا أعضاء في شراكة من أجل السلام، فإن سلوفينيا وكرواتيا وألبانيا وبلغاريا دول في جنوب شرقي أوروبا وأعضاء في حلف شمال الأطلسي. لذلك، في سياق الأمن الحالي، من الأهمية أكثر من أي وقت مضى معالجة قضية الإرهابيين الذين يستخدمون التكنولوجيا والإنترنت. وعلاوة على ذلك، هناك مخاوف كبيرة بشأن استخدام التكنولوجيا والفضاء السيبراني من قبل الإرهابيين في جنوب شرقي أوروبا بسبب العدد المتزايد من عمليات التجنيد القائمة على الإنترنت والتطرف المزعوم عبر الإنترنت المرتبط بالمنطقة قبل الهجمات في جميع أنحاء العالم. إن الاتجاه المتزايد نحو التطرف والتجنيد والهجوم من خلال الإنترنت والتكنولوجيا يحمل في طياته إمكانية تحويل جهود جنوب شرقي أوروبا لإنشاء منصة إلكترونية لزيادة التنمية إلى أرض تدريب ومنصة إطلاق للهجمات السيبرانية على جنوب شرقي أوروبا والتحالف وشركائها وآخرين إذا لم يتم أخذ هذا التطور على محمل الجد. وبالتالي، فمن الضروري إجراء تحقيق موسع في الأنشطة الإرهابيَّة في الفضاء السيبراني. وعادة ما تتخذ الحكومات إجراءات قانونية لمنع الاستخدام غير القانوني للإنترنت من خلال اللجوء إلى المحاكم الوطنية. ولكن المرونة في صيانة موقع على شبكة الإنترنت من خلال تغيير الخوادم والعلامات والوكلاء وما إلى ذلك لا تردع أو تمنع المنظمات الإرهابيَّة من استغلال الإنترنت. وعلى هذا فإن السلطات الأمنية الوطنية والدولية قادرة على استغلال وتقييم تصميم وسياق مواقع الويب التابعة للمنظمات المؤيدة للإرهاب من أجل توضيح سياق تصرفات المنظمات الإرهابيَّة. ومن أجل منع المنظمات الإرهابيَّة من استخدام الإنترنت، هناك حاجة إلى التعاون والتنسيق الكاملين في الإجراءات. ولإنشاء آلية مراقبة في هذا الموقف، لا بُدَّ من إضفاء الطابع المؤسسي على التعاون على المستويين الحكومي وغير الحكومي. وقد حولت كل حكومة انتباهها إلى عبارة "التعاون" لأن الإرهاب وغيره من الأنشطة الإجرامية العابرة للحدود الوطنية احتلت مركز الصدارة في الساحة الدولية [5].

3.2 الطائرات بدون طيار والأنظمة المستقلة

لقد حققت الأنظمة الجوية بدون طيار والروبوتات بشكل عام تقدمًا كبيرًا في العامين الأخيرين. ومع ذلك، فإن غالبية الاستخدامات لم تأتِ بعد. خلال السنوات الخمس المقبلة، من المرجح أن تُستخدم الطائرات بدون طيار المدنية على نطاق واسع لمجموعة متنوعة من الأغراض، ومن ذلك الإمدادات الطارئة وإدارة الأزمات والتعافي من الكوارث والتنقل الحضري وخدمات التوصيل (NATO Review، 2020).

حاول الإرهابيون استخدام مجموعة متنوعة من التقنيات والتلاعب بها في عملياتهم، ومن ذلك المعدات الجاهزة. وقد اعتبرت الطائرات بدون طيار، على وجه الخصوص، تهديدًا. ونتيجة لذلك، في فبراير 2019، اتفق وزراء دفاع حلف شمال الأطلسي على إطار عملي لمواجهة أنظمة الطائرات بدون طيار. وفي عام 2023، تم الاتفاق على برنامج عمل جديد لتنسيق التدابير بشكل أفضل وتحديد خطوات أخرى لمكافحة هذه المشكلة التي يتم تنفيذها حاليًا. بالإضافة إلى ذلك، يعمل حلف شمال الأطلسي على عقيدة C - UAS، التي تمت الموافقة عليها بحلول نهاية عام 2023. من خلال الاختبارات والتقييمات والتمارين وتطوير الأفكار والمعايير الفنية، يسهل برنامج عمل الدفاع ضد الإرهاب (DAT POW) التطوير الكامل للقدرات في مجال C - UAS. قام برنامج عمل الدفاع ضد الإرهاب (DAT POW) بتمويل تحدي ابتكار في عام 2021 لإنشاء طرق التعلم الآلي والذكاء الاصطناعي لتتبع وتصنيف وتحديد الطائرات بدون طيار أثناء طيرانها داخل منطقة محددة سلفًا. تناولت مظاهرة تكنولوجية لرؤساء الدول والحكومات في قمة حلف شمال الأطلسي 2022 في مدريد بعضًا من أحدث القضايا المتعلقة بالأنظمة المضادة للطائرات بدون طيار وقدرات الاستغلال.



شكل 1. توغل طائرة بدون طيار في مطار جاتويك بالقرب من لندن، في ديسمبر/كانون الأول 2018.

إن أغلب الطائرات بدون طيار التي تستخدمها المنظمات الإرهابيَّة هي طائرات عسكرية متوسطة الحجم أو طائرات هواة؛ لأنها أرخص وأسهل في الوصول إليها. ويعتمد نوع الطائرات بدون طيار التي تستطيع الجماعات الوصول إليها على مقدار التمويل الخارجي الذي تتلقاه، ويمكن تصنيف استخدام الطائرات بدون طيار من قبل المسلحين إلى فئتين: الدفاع السلبي والهجوم النشط. ويشمل الاستخدام الهجومي النشط استخدام الطائرات بدون طيار في تنفيذ الهجمات. على سبيل المثال، هاجم الحوثيون مواقع حرجة في المملكة العربية السعودية وحلفائها باستخدام الطائرات بدون طيار؛ وكان آخر هجوم لهم على مصنع نفط في أبو ظبي في يناير 2022. قام تنظيم داعش بتحديث الطائرات بدون طيار الرباعية المراوح بين عامي 2015 و2017 حتى تتمكن من إسقاط المتفجرات على جنود التحالف على الأرض؛ ما أدَّى إلى 60 - 100 هجوم كل شهر.

كما يشمل الاستخدام السلبي للطائرات بدون طيار المراقبة والدعاية ونقل الأسلحة. وقد غير تنظيم داعش مؤخرًا إستراتيجيته الخاصة بالطائرات بدون طيار من الهجوم النشط إلى الدفاع السلبي. وقد أصبح هذا بارزًا جدًّا في إفريقيا. وفي يناير 2022، استخدم تنظيم داعش في غرب إفريقيا (ISWAP) طائرات بدون طيار رباعية المراوح لتصوير أجزاء من مقطع فيديو دعائي يسلط الضوء على معسكر تدريبي في نيجيريا. وفي يوليو 2022، شوهدت طائرات استطلاع تابعة لتنظيم داعش في غرب إفريقيا فوق مواقع قوات الحكومة النيجيرية، قبل وقت قصير من نصب التنظيم كمينًا لها. ووفقًا لتقارير حديثة، استخدمت حركة الشباب في الصومال طائرات بدون طيار ثابتة الجناح لإجراء المراقبة والهجمات. وقد استخدم المسلحون المتمركزون في باكستان طائرات بدون طيار رباعية المراوح لنقل الأسلحة عبر الحدود إلى جامو وكشمير.

بالإضافة إلى الطائرات بدون طيار التي يستخدمها بعض الإرهابيين مثل: طائرات DJI الرباعية المراوح، فإن القنابل الصغيرة مثل: Switchblade وPhoenix Ghost تستحق الاهتمام. هذه الطائرات بدون طيار الانتحارية المتطورة، مثل: أنظمة الهاون البسيطة، قادرة على تدمير الدبابات العسكرية والمركبات المدرعة. تأتي Switchblade في طرازين: Switchblade - 300 وSwitchblade - 600. يبلغ وزن Switchblade 300 - نحو 2.5 كجم فقط، ويمكن وضعه في حقيبة ظهر، ويمكن إعداده في دقائق. كما يبلغ مداه 10 كيلومترات وعمر البطارية 15 دقيقة، بالإضافة إلى نظام دقة موجه بنظام تحديد المواقع العالمي (GPS) يتم التحكم فيه بواسطة وحدة تحكم أرضية باستخدام جهاز لوحي بسيط. يعد Switchblade - 600 نظامًا أثقل بكثير؛ حيث يزن نحو 70 كجم، ويبلغ مداه 40 كيلومترًا ومدة 40 دقيقة. هناك القليل من التفاصيل حول Phoenix Ghost. ومع ذلك، مثل Switch-blade - 300، يُقال: إنه يمكن وضعه في حقيبة ظهر،

ولديه قدرة تحمل أطول بكثير تبلغ نحو ست ساعات.

لا يتم عرض هذه الأنظمة للبيع الآن؛ لأنها تخضع لقوانين مراقبة التصدير التي تنفذها وزارة الدفاع الأمريكية. من ناحية أخرى، تتوافر أنظمة Switch-blade للشراء على شبكة الويب المظلمة مقابل ما بين 4000 و7000 دولار.

ومن بين الاتجاهات التي ينبغي لنا أن نلاحظها في المستقبل استخدام الطائرات بدون طيار لتنفيذ هجمات كيميائية أو بيولوجية محدودة النطاق. ولا يتطلب تركيب صواريخ محملة بالمواد الكيميائية على طائرات بدون طيار انتحارية أو تركيب رشاشات مليئة بالسموم على طائرات رباعية المراوح الكثير من الخبرة أو الكفاءة [6].

4.2 الميتافيرس

لقد أحدثت تقنيات الميتافيرس تحولًا جذريًّا في الكثير من القطاعات من خلال توفير أدوات مبتكرة مثل: الواقع المعزز والواقع الافتراضي والواقع الممتد. في حين أوجدت هذه التقنيات فرصًا جديدة للمجرمين والإرهابيين لارتكاب أنواع جديدة من الجرائم، التي يمكن تسميتها "جرائم الميتا".

تتمتع هذه الأدوات بواجهة ثلاثية الأبعاد تستفيد من قدراتنا في التفكير؛ ممَّا يوفر إستراتيجيات جديدة وفعَّالة لمواجهة التحديات المعرفية المعقدة. إن هذا النهج المتطور يعد بإعادة تشكيل كيفية تعامل الجهات الأمنية مع القضايا المعقدة؛ ممَّا يؤدي إلى تقديم رؤى أكثر وضوحًا وفاعلية خلال عمليات التحقيق.

تُعتبر "جرائم الميتا" مصدر قلق متزايد، وقد تصبح قضية محورية مع تزايد اعتماد هذه التقنيات في حياتنا اليومية. لذلك، يصبح من الضروري لوكالات إنفاذ القانون أن تستعد لمواجهة التحديات المستقبلية من خلال إعداد قائمة بالتهديدات المحتملة وتحديد الفجوات، بما في ذلك تلك المرتبطة بالأطر القانونية اللازمة لتجريم هذه الأنشطة [7].

وقد لخصت الإنتربول أهم التحديات التي قد ترتكب من قبل الجماعات الإرهابيَّة في تقنية الميتافيرس وهي كالآتي:

1. الهجمات السيبرانية المادية (Cyber physical at-tack): يمكن أن تستغل الجهات الإرهابيَّة تقنية التوأم الرقمي للوصول غير القانوني، والتحكم في أنظمة البنية التحتية الحيوية؛ ممَّا يسهل تنفيذ الهجمات السيبرانية عليها.
2. تمويل الإرهاب: يمكن أن يُساء استخدام الميتافيرس من قبل الإرهابيين لجمع الدعم المالي لأنشطتهم، ممَّا قد يؤدي إلى تنفيذ هجمات إرهابية، وانتشار الأسلحة، وتعزيز الشبكات الإجرامية المنظمة.
3. التطرف والتلقين: قد تُستخدم الميتافيرس كمنصة لتجنيد الأفراد وتدريبهم وتلقينهم الأفكار المتطرفة. كما تمنح الإرهابيين القدرة على جمع الأموال بصورة مجهولة، ونشر المعلومات المضللة والدعاية بسرعة إلى الشرائح المستهدفة.
4. تنسيق الأنشطة الإرهابيَّة: يمكن للمستخدمين المشاركين في الإرهاب السيبراني استخدام تقنية

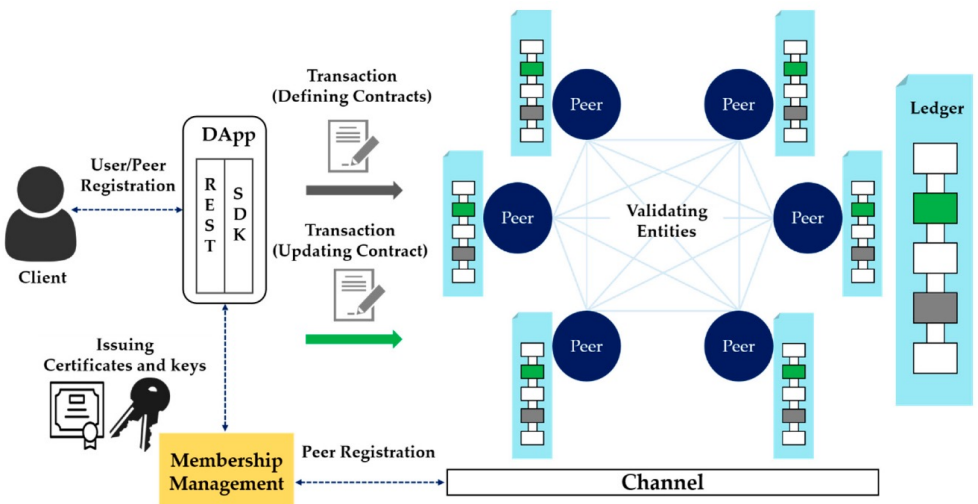
التوأم الرقمي لتعزيز التنسيق، وتنفيذ الهجمات في العالم الحقيقي المتعلقة بأنشطة الجماعات الإرهابيَّة.

5.2 تقنية البلوكشين

أصبحت تقنية البلوكشين تمثل تحولًا جذريًّا في عالم التجارة الرقمية وتبادل البيانات؛ حيث أثبتت نفسها كأداة فعَّالة تسهم في تعزيز الشفافية والأمان في مختلف القطاعات. ويعود الفضل في هذا التحول إلى هيكلها اللامركزي الذي يوفر منصة موثوقة وآمنة لتسجيل المعاملات المالية والأصول الرقمية، بالإضافة إلى البيانات الحساسة الأخرى. ويُمكن هذا الهيكل الشركات والمؤسسات من تحقيق أعلى مستويات الثقة مع عملائها؛ ممَّا يسهل العمليات التجارية ويعزز الابتكار.

تُعتبر البلوكشين دفتر أستاذ رقمي، يعمل بنظام تحكم لا مركزي؛ ممَّا يسمح لها بتجاوز الإجراءات التقليدية التي تعتمدها الجهات الأمنية في التحقيقات. وتعتمد هذه التقنية على تنظيم البيانات في شكل كتل، ويتم ربط كل منها بالكتلة السابقة لتكوين سلسلة متواصلة. كل كتلة تتضمن مجموعة من المعاملات، وطابعًا زمنيًّا، وتجزئة تشفير فريدة تُعزز من ارتباطها بالكتلة السابقة. هذه البنية التحتية تحافظ على سلامة البيانات وثباتها؛ ممَّا يجعل البلوكشين منصة مثالية للمعاملات الآمنة والشفافة.

ويُعدُّ البيتكوين من أشهر التطبيقات العملية لهذه التقنية؛ حيث يُستخدم في الكثير من المجالات المشروعة، ولكنه في الوقت ذاته يُستغل أيضًا لأغراض إجرامية ضمن الشبكة المظلمة؛ حيث يُسهم استخدام الرموز غير



شكل 2. سجل حسابات مبني على تقنية البلوكشين

القابلة للاستبدال (NFTs) في مخططات غسل الأموال والأنشطة الإجرامية الأخرى؛ ممَّا يزيد من تعقيد جهود مكافحة الجرائم السيبرانية. وهذه التطورات السريعة تتطلب من أجهزة إنفاذ القانون تطوير أدوات جديدة وتعديل القوانين القائمة لضمان قدرتها على مواجهة التحديات الناتجة عن هذا الاستخدام المتزايد لتقنية البلوكشين في الأنشطة غير المشروعة.

علاوة على ذلك، يسلط الاهتمام المتزايد على ضرورة تحسين التعاون الدولي بين أجهزة إنفاذ القانون؛ حيث إن الجرائم عبر البلوكشين غالبًا ما تتجاوز الحدود الوطنية. ويتطلب هذا التعاون تبادل المعلومات والخبرات، ممَّا يسهل التحقيقات، ويعزز من فاعلية الإجراءات القانونية. إن التكيف مع هذه التكنولوجيا الحديثة أصبح ضرورة ملحة لضمان سلامة المجتمع وحماية الحقوق المالية للأفراد [8].

3. التحديات الأمنية في عصر التقنيات الناشئة

تواجه الجهات الأمنية في جميع أنحاء العالم تحديات متعددة؛ نتيجة لتطور التقنيات الحديثة، وتشمل هذه التحديات:

1.3 تقنيات التلاعب الصوتي والمرئي

في السنوات الأخيرة، أصبحت الأخبار المزيفة تهديدًا حقيقيًّا للديمقراطية والحضارة الإنسانية، وكذلك للخطاب العام. تُعرف الأخبار المزيفة بأنها معلومات كاذبة تُنتج بغرض تضليل الجمهور، وقد انتشرت هذه المعلومات بسرعة عبر وسائل التواصل الاجتماعي؛ ممَّا يتيح لها التأثير على ملايين الأشخاص. حاليًّا، يُعتبر موقع يوتيوب ثاني أكثر المصادر شعبية للأخبار بين مستخدمي الإنترنت بعد فيسبوك؛ حيث يُستخدم من قبل واحد من كل خمسة أشخاص.

تسلط هذه الشعبية المتزايدة لمحتوى الفيديو الضوء على الحاجة الملحة لأدوات تحقق لضمان سلامة محتوى الوسائط والأخبار، خاصة في ظل التقنيات الجديدة التي تتيح إنتاج مقاطع فيديو يتم التلاعب بها بشكل مقنع. وأصبحت عملية التمييز بين المعلومات الصحيحة والمزيفة صعبة؛ ممَّا يؤثر سلبًا على اتخاذ القرارات المستنيرة.

كما سهلت التطورات التكنولوجية الحديثة إنشاء ما يُعرف بـ مقاطع فيديو، صوت أو صورة بعمق، وهي مقاطع فيديو حيوية تبدو حقيقية بشكل يثير الشك، مع وجود مؤشرات قليلة على التلاعب. يتم إنتاج محتوى التزييف العميق باستخدام خوارزميات الذكاء الاصطناعي التي تجمع بين الصور ومقاطع الفيديو وتعدلها لاستبدال الوجوه أو دمجها، ممَّا يتيح إنشاء أفلام مزيفة تبدو أصلية. يمكن لتقنية التزييف العميق على سبيل المثال، إنتاج محتوى فكاهي أو إباحي أو سياسي يظهر فيه أي شخص، وهو يقول أي شيء دون الحصول على موافقته.

إن مدى تعقيد التكنولوجيا المستخدمة في إنتاج التزييف العميق يجعلها ثورية؛ حيث يمكن لأي شخص يمتلك جهاز كمبيوتر إنشاء أفلام مزيفة تبدو مشابهة للوسائط الأصلي [9].

2.3 تصاعد الجرائم السيبرانية

يستغل المجرمون التحول نحو الفضاء السيبراني لاستغلال الثغرات الموجودة في الأنظمة والشبكات والبنية التحتية الرقمية. وللأسف، فإن لهذا التحول تأثيرات اقتصادية واجتماعية كبيرة على الحكومات والشركات والأفراد على مستوى العالم.

تشمل التهديدات السيبرانية الحالية تقنيات؛ مثل: التصيد الاحتيالي، وبرامج الفدية، واختراق البيانات؛ حيث تظهر أنواع جديدة من الجرائم السيبرانية بانتظام. وأصبح مجرمو الإنترنت أكثر مرونة وتنظيمًا، مستفيدين من التقدم التكنولوجي لتخصيص هجماتهم والتعاون بطرق جديدة ومبتكرة. لا تعرف الجرائم السيبرانية حدودًا جغرافية؛ حيث إن المجرمين والضحايا والبنية التحتية التكنولوجية موجودون في بلدان متعددة؛ ممَّا يعوق جهود التحقيق والملاحقة القضائية. هذه الطبيعة العابرة للحدود تسلط الضوء على الحاجة الملحة للتعاون الدولي في مواجهة هذه التحديات؛ حيث يتطلب الأمر تنسيقًا فعالًا بين السلطات القانونية المختلفة لمكافحة الجرائم السيبرانية بفاعلية [10].

3.3 انتشار المعلومات المضللة

تُعدُّ الشائعات والمعلومات الخبيثة موضوعًا حيويًّا يلقى اهتمامًا واسعًا في وسائل الإعلام المختلفة. وقد أدَّت الوسائط الرقمية، وبخاصة منصات التواصل الاجتماعي، إلى تفاقم هذه المشكلة؛ إذ يُعَدُّ التحكم في المعلومات غير المرغوب فيها أمرًا صعبًا؛ نظرًا لسهولة الوصول إليها، وسرعة انتشارها، وصعوبة تصحيح المعلومات الخاطئة بعد نشرها. ومع ظهور هذه المنصات، أصبحت المعلومات المضللة قضية بارزة تتطلب اهتمامًا علميًّا متزايدًا، خاصة بعد الانتخابات الرئاسية الأمريكية في عام 2016؛ حيث يُعتقد أن المعلومات المضللة أدَّت دورًا في التأثير على النتائج. وقد حدد المنتدى الاقتصادي العالمي «المعلومات المضللة» كإحدى القضايا العالمية الملحة التي تحتاج إلى معالجة [11].

4. إستراتيجيات فعَّالة لمكافحة الإرهاب باستخدام التقنيات الحديثة

يتعين على أجهزة إنفاذ القانون أن تأخذ التقنيات الجديدة في الاعتبار بطريقتين:

- التعرُّف إلى التكنولوجيا الناشئة التي يستخدمها الإرهابيون ومواجهتها.
- اقتناء التكنولوجيا الجديدة للاستعداد والاستجابة للمشكلات والإجراءات المتعلقة بالإرهاب.

على سبيل المثال، في الخيار الأول حول استخدام التكنولوجيا للحد من الإرهاب، هناك الكثير من الجهات التي حاولت الاستفادة من التقدم التكنولوجي لمواجهة التهديدات الإرهابيَّة. ومن أهم هذه الجهود:

أنشأت منظمة حلف شمال الأطلسي نموذجًا أوليًّا للتكنولوجيا يسمى DEXTER، يرمز إلى الكشف عن المتفجرات والأسلحة النارية لمكافحة الإرهاب؛ لمعالجة التهديد الذي تشكله الأسلحة والمتفجرات في المناطق المزدحمة. تم اختبار النموذج الأولي بنجاح لمدة شهر واحد في محطة مترو روما بإيطاليا بعد ثلاث سنوات

من الدراسة الممولة من برنامج العلوم من أجل السلام والأمن التابع لمنظمة حلف شمال الأطلسي.

ومن خلال استخدام التقنيات الثلاث التي ابتكرها نظام DEXTER، سيكون من الممكن تحديد المشاة الذين يحملون أسلحة نارية أو متفجرات عن بُعد، وفي الوقت الفعلي. وسيتجاوز النظام الضمانات الحالية، ويجعل من الممكن تحديد هذه المخاطر بشكل فردي دون الحاجة إلى عمليات تفتيش عشوائية للركاب أو نقاط التفتيش. ومن أجل مواكبة التهديدات المتغيرة، يدمج نظام DEXTER التقنيات بطريقة تسمح له بإضافة المزيد من أنظمة الكشف حسب الحاجة. ولا تنبع مثل هذه النتائج من البراعة العلمية والتكنولوجية فحسب، بل تنبع أيضًا من الشعور القوي بالوحدة بين الشركاء والرغبة المشتركة في تحسين أمن المواطنين ضد الهجمات العنيفة. وشارك في نظام DEXTER إحدى عشرة منظمة عامة وأكاديمية من أربع دول أعضاء في حلف شمال الأطلسي (فرنسا وألمانيا وإيطاليا وهولندا) وأربع دول شريكة (فنلندا وجمهورية كوريا وصربيا وأوكرانيا).

كما أكد حلف شمال الأطلسي أن الاستعداد الأفضل يتطلب فهمًا مشتركًا للتهديد ووعيًا شديدًا بالموقف. ويمكن تحقيق سياسات الاستعداد للمستقبل، وتعزيز مرونة التحالف، وتبسيط إجراءات التخطيط من خلال إجراء مسح للتهديدات واستشراف المستقبل الإستراتيجي. وعلاوة على ذلك، سيكون من الضروري زيادة التعاون على جميع المستويات لمكافحة التهديد الذي تشكله الطائرات بدون طيار.

كما زاد عدد الطائرات بدون طيار، وأصبح من السهل الوصول إليها واستخدامها بشكل كبير، وبذلك فإن تشجيع التحسينات المستمرة في الأداء التعاوني لأنظمة مكافحة الطائرات بدون طيار يُسهم في تعزيز الدفاع الجوي للحلفاء والردع والدفاع.

استضافت C - UAS Joint Nucleus، قسم من وزارة الدفاع الهولندية، الاجتماع الذي تم تنسيقه من قبل وكالة الاتصالات والمعلومات التابعة لحلف شمال الأطلسي (وكالة NCI)، حيث اجتمع أكثر من 300 مشارك من 15 حكومة من الحلفاء، وثلاث حكومات شريكة والاتحاد الأوروبي والقطاع التجاري في هولندا من 12 إلى 22 سبتمبر 2023، لتعزيز قدرتهم على معالجة المخاطر المحتملة التي يفرضها الاستخدام الخبيث للطائرات بدون طيار. جمع حلف شمال الأطلسي خبراء من الجيش والأوساط الأكاديمية والشركات لاختبار أنظمة الكشف عن الطائرات بدون طيار التجارية المتطورة وتحديدها وتحييدها خلال تمرين التشغيل البيني التقني لنظام مكافحة الطائرات بدون طيار (C - UAS TIE23). كان هناك نحو سبعين جهازًا وتقنية تم تقييمها في الوقت الفعلي، ومن ذلك المؤثرات وأجهزة الاستشعار وأجهزة التشويش. وكان الهدف هو التأكُّد من أن هذه الأنظمة المتطورة يمكنها التكامل والترابط بسلاسة في الوقت الفعلي.

إن الجمع بين التكنولوجيا والإستراتيجيات سيكون الطريقة العملية الوحيدة لمكافحة خطر الطائرات بدون طيار في المستقبل؛ حيث الطريقة الوحيدة للسيطرة على مشكلة الطائرات بدون طيار المضادة للطائرات هي أن يكون لدينا وعي كامل، ورؤية الأنماط، وتصور النتيجة المثالية والسعي نحوها. ويتبين أن "الحل السحري" عبارة عن خليط من الكثير من الإستراتيجيات التي تم

التخطيط لها بدقة: الفهم، والاستعداد، والإبداع، والتعاون، والقدرة على التكيف.

وعلى الرغم من أن الذكاء الاصطناعي يثير بعض المخاوف، كما ذكرنا سابقًا، فإنه يمتلك أيضًا القدرة على مساعدة جهود مكافحة الإرهاب بشكل كبير بعدة طرق. فقد يحلل الذكاء الاصطناعي مقاطع الفيديو الحية لتحديد الأشياء أو السلوك المشبوه في الأماكن العامة؛ ممَّا يساعد سلطات إنفاذ القانون على اتخاذ إجراءات سريعة في حالة وجود تهديد. وتتمتع أدوات الذكاء الاصطناعي بالقدرة على تحديد المحتوى المتطرف وإزالته تلقائيًّا من منصات الإنترنت، ومن ثم التخفيف من انتشار الدعاية الإرهابيَّة والمساعدة في عملية إزالة التطرف والدعاية المضادة. ومن خلال تحديد الأشخاص المعرضين للخطر وتحليل سلوكهم عبر الإنترنت، يمكن أن يساعد الذكاء الاصطناعي في مبادرات إزالة التطرف. كما يمكن للذكاء الاصطناعي أن يتنبأ بالأعمال الإرهابيَّة الوشيكة من خلال تحليل الأنماط في البيانات التاريخية، ونشاط وسائل التواصل الاجتماعي، ومصادر الاستخبارات الأخرى. ويمكنه فحص سلوك الأفراد أو الجماعات للكشف عن مؤشرات التطرف والتدخل قبل وقوع الحادث. كما يجمع الذكاء الاصطناعي مجموعة بيانات كبيرة من مصادر مختلفة؛ مثل: لقطات المراقبة، والمنصات الرقمية، والأنشطة المالية لتقديم رؤى شاملة. أيضًا يستخدم معالجة اللغة لتفسير وتحليل التهديدات المحتملة على شبكة الإنترنت.

إن الذكاء الاصطناعي قادر على زيادة الكفاءة التشغيلية في مكافحة الإرهاب. فهو قادر على تحسين تخصيص الموارد للعمليات، وضمان توزيع الموظفين والمعدات بشكل صحيح. كما يستطيع الذكاء الاصطناعي أن يزود صناع القرار بالبيانات والتوصيات في الوقت الحقيقي، ومن ثم تحسين فاعلية تكتيكات مكافحة الإرهاب. ومع ذلك، من الأهمية بمكان أن نلاحظ أن أي تدابير مضادة يتم اتخاذها لا بُدَّ أن تحقق توازنًا دقيقًا بين ضمان الرفاهة الاجتماعية وحماية التبادل المفتوح للأفكار والابتكار الذي يميز البلدان الديمقراطية.

في المملكة العربية السعودية، طوّرت جامعة نايف العربية للعلوم الأمنية برنامجًا متقدمًا يهدف إلى الكشف عن الأصوات المزيفة باللغة العربية. ويُعدُّ هذا التطبيق مشروعًا مميزًا يُظهر التزام الجامعة بتعزيز الحلول التكنولوجية الحديثة. حيث لا يقتصر دور هذا التطبيق على كونه أداة تقنية فحسب، بل يُعَدُّ خطوة إستراتيجية حيوية في جهود الجامعة المستمرة لتوطين هذه الحلول؛ استجابة للمخاطر الأمنية المتزايدة. كما يُسهم هذا التطبيق بشكل فعَّال في القدرة على إحباط العمليات الإرهابيَّة التي تستغل التكنولوجيا، خاصة في ظل التحديات الناتجة عن استخدام الذكاء الاصطناعي في إنشاء محتوى صوتي مزيف. بفضل قدرته على اكتشاف الأصوات المزيفة، يستطيع الجهاز الأمني تعزيز فاعلية تحقيقاته، وإجراء تحليل دقيق للأدلة؛ ممَّا يُعزِّز من قدرة السلطات على مواجهة التهديدات بشكل أكثر كفاءة.

كما قامت الجامعة بتطوير تطبيق ثانٍ يُعرف بتطبيق الكشف عن الأسلحة، يهدف إلى تعزيز إجراءات الأمن والسلامة في الأماكن العامة والمناسبات الكبرى. يستخدم هذا التطبيق تقنيات متقدمة لتحليل البيانات

والتقاط الصور، ممَّا يمكّنه من التعرف بدقة عالية على أشكال الأسلحة وتصنيفاتها. تم عرض هذا التطبيق في المعرض الدولي للدفاع؛ ممَّا يعكس التزام الجامعة بالتفاعل مع التطورات العالمية في مجال الأمن والدفاع.

بالتعاون مع مركز الأمم المتحدة لمكافحة الإرهاب، سيدعم الإنتربول الدول الأعضاء في وضع خطط مكافحة الإرهاب موضع التنفيذ بهدف منع الإرهابيين من الاستفادة من الابتكارات التكنولوجية المتطورة. وستعمل الأنشطة على تحسين القدرات التحقيقية والتحليلية والتشغيلية. وفي إطار برنامج CT TECH، تم تقديم ستة عناصر معرفية جديدة في يونيو 2023 خلال أسبوع الأمم المتحدة الثالث لمكافحة الإرهاب. وتشمل مبادرات مشروع CT - Tech:

1. تقييم احتياجات المخاطر الموجودة اليوم وكيفية ارتباطها بالتكنولوجيا الجديدة والمتطورة.
2. توسيع التعاون العالمي في تحقيقات مكافحة الإرهاب في المجالات ذات الصلة.
3. وضع إرشادات تؤكد الأساليب المناسبة للضبط والتعاون مع تكنولوجيا المعلومات والاتصالات.
4. إنشاء دورات التعلم الإلكتروني والندوات عبر الإنترنت وجلسات التعلم العملية حول التعرُّف إلى الوجوه والأصول الافتراضية/الشبكة المظلمة والاستخبارات مفتوحة المصدر (OSINT).
5. تنسيق مجموعات العمل الإقليمية وجلسات التدريب على تطبيق قدرات الإنتربول في مجال القياسات الحيوية.
6. توفير التعليمات بشأن جمع الأدلة الرقمية وحفظها وتطبيقها في القضايا القضائية.

5. التوصيات

1. تطوير الدعم لبناء القدرات للدول العربية لمواجهة تهديدات الإرهاب السيبراني.
2. إنشاء شراكات وطنية وإقليمية ودولية مع أصحاب المصلحة من القطاعين العام والخاص، بهدف تبادل المعلومات والخبرات لمنع الأضرار الناتجة عن الهجمات الإرهابيَّة على البنى التحتية الأساسية، وفرض الحماية اللازمة، والتخفيف من آثارها، والتحقيق فيها والاستجابة لها. وذلك من خلال تنفيذ تدريبات مشتركة وإنشاء شبكات مرتبطة بهدف التواصل والإنذار.
3. تطوير أدوات للوقاية والكشف عن الإرهاب السيبراني.
4. تطوير البرامج التدريبية في المجالات الأساسية؛ مثل: الأدلة الجنائية الرقمية، والأمن السيبراني، والجريمة السيبرانية، والاستخبارات السيبرانية، وعلم البيانات.
5. التركيز على مجالات بحثية أساسية، مثل: تمويل الإرهاب، والعملات المشفرة، ومنصات وسائل التواصل الاجتماعي المتاحة عبر الإنترنت، والتقنيات الناشئة.
6. تقارير متخصصة: الاستفادة من تقارير مركز الجرائم السيبرانية والأدلة الرقمية في جامعة نايف العربية للعلوم الأمنية.
7. تدريب سيبراني: الطلب من مركز الجرائم السيبرانية والأدلة الرقمية في جامعة نايف العربية للعلوم الأمنية تنفيذ برنامج تدريبي للدول العربية لقياس جاهزية الجهات في مواجهة الجرائم السيبرانية.

المراجع

1. Jackson، B.A.، 2001. Technology acquisition by terrorist groups: threat assessment informed by lessons from private sector technology adoption. Studies in Conflict & Terrorism، 24(3)، pp.183- 213.
2. NATO Review - Countering cognitive warfare: awareness and resilience، 20 - May، 2021.
3. Citaristi، I.، 2022. United Nations Office on Drugs and Crime—UNODC. In The Europa Directory of International Organizations 2022 (pp. 248 - 252). Routledge.
4. Chemical security experts call for multisector cooperation against terrorism (interpol.int)، Chemical security experts call for multisector cooperation against terrorism، November، 2022. Interpol
5. Ogun، M.N. ed.، 2015. Terrorist use of cyberspace and cyber terrorism: New challenges and responses (Vol. 42). IOS press.
6. Militants and Drones: A Trend That is Here to Stay | Royal United Services Institute (rusi.org)
7. https://www.interpolrednotice.com/news - 1/ metaverse - a - law - enforcement - perspective.
8. https://blog.merklescience.com/general/investigating - blockchain - crimes - using - blockchain - forensics.
9. https://timreview.ca/article/1282
10. https://www.interpol.int/en/Crimes/Cybercrime
11. Muhammed T، S.، & Mathew، S. K. (2022). The disaster of misinformation: a review of research in social media. International journal of data science and analytics، 13(4)، 271- 285.

يوليو 2026

July 2026

تقوى الحاج

عبد الرزاق بن عبد العزيز المرجان

مركز الجرائم السيبرانية والاقتصادية، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية.

Taqwa Al-Hajj

Abdul Razzaq bin Abdul Aziz Al-Marjan

Centre for Cybercrime and Economic Crime, Naif Arab University for Security Sciences, Riyadh, Saudi Arabia.

الكلمات المفتاحية: التقنيات الحديثة، الجرائم السيبرانية، الإرهاب، الذكاء الاصطناعي

Keywords: modern technologies, cybercrime, terrorism, artificial intelligence

Production and hosting by NAUSS

Email: TAlhaj@nauss.edu.sa
doi: 10.26735/QWDW3137