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

نحو سياسة فعَّالة لمكافحة الابتكار الخبيث للتنظيمات الإرهابيَّة

Towards an Effective Policy to Combat the Malicious Innovation of Terrorist Organizations

المخرجات الرئيسة

- بناء قدرات موظفي إنفاذ القانون ومكافحة الإرهاب بالمهارات اللازمة لمواجهة التحديات المتُطورة التي تشكلها التهديدات السيبرانية.
- وضع أطر تنظيمية ضد أنظمة الطائرات بدون الطيار، وذلك عبر الاستثمار في إنتاج تقنيات أنظمة مضادة للطائرات بدون طيار فعّالة للتعامل مع التهديد المستقبلي.
- تشجيع مراكز الفكر والأبحاث العربية على إنتاج دراسات نوعية تستهدف تحليل الاستراتيجيات التي تعتمد عليها التنظيمات الإرهابية.

المستخلص

تناولت الورقة آليات الابتكار الخبيث للتنظيمات الإرهابية، حيث اعتمدت تلك التنظيمات على وسائل التواصل الاجتماعي، والذكاء الاصطناعي، وألعاب الفيديو في عمليات الدعاية والتجنيد. كما وظفت العملات الافتراضية في جمع التبرعات، وتمويل الهجمات، والاتجار غير المشروع في ضوء المزايا التي تتمتع بها تلك العملات، حيث إخفاء الهوية، وسهولة الاستخدام، وسرية المعاملات. كذا استخدمت بشكل متزايد الطائرات بدون طيار في عملياتها نظرًا لانخفاض تكلفتها وسهولة استخدامها.

Abstract

The paper explores the mechanisms of malicious innovation employed by terrorist organizations, emphasizing their reliance on social media platforms, artificial intelligence, and video games for propaganda and recruitment purposes. These groups have also exploited virtual currencies to fundraise, finance attacks, and engage in illicit transactions; depending on the advantages, these currencies offer, especially anonymity, ease of use, and transactional secrecy. Furthermore, terrorist organizations exploit, in increasing pace, the unmanned aerial vehicles (drones) in its operations, attributed

وأخيرًا، أوصت الورقة بدمج الذكاء الاصطناعي في استراتيجيات مكافحة الإرهاب، حيث تساعد التحليلات التنبؤية المدعومة بالذكاء الاصطناعي على تعزيز الوقاية من التهديدات الإرهابية المحتملة. كما أوصت أيضًا بالعمل على تنظيم البنية التحتية للشبكة المظلمة، مع اتخاذ خطوات فاعلة من شأنها تشديد الرقابة على العملات الافتراضية. بجانب بناء قدرات موظفي إنفاذ القانون ومكافحة الإرهاب وتزويدهم بأحدث الأدوات التكنولوجية المتاحة.

to their affordability and user-friendliness.

The paper concludes by recommending the important integration of artificial intelligence into counter-terrorism strategies, highlighting the role of AI-driven predictive analytics in enhancing threat prevention. It also advocates for the regulation of dark web infrastructure and the implementation of effective measures to strengthen censorship over virtual currencies. Additionally, the paper underscores the importance of capacity building for law enforcement and counter-terrorism personnel, ensuring they are equipped with the most advanced technological tools available.

المقدمة

سعت التنظيمات الإرهابيَّة إلى استخدام سبل الابتكار المتاحة في نشر أفكارها، وتمويل أنشطتها، وتنفيذ هجماتها؛ حيث أثبتت قدرتها على استغلال التكنولوجيا الحديثة لتحقيق أهدافها وتعزيز نفوذها. فمنذ ظهور المواقع الإلكترونية في أواخر التسعينيات، وصولًا إلى منصات التواصل الاجتماعي الجديدة، سارعت تلك التنظيمات إلى توظيف التطورات الحديثة في الفضاء السيبراني في عمليات الدعاية والتجنيد، وقد تزامن ذلك مع تطويرها إستراتيجيات تمويلية جديدة قائمة على استخدام العملات الافتراضية في ضوء المزايا التي تتمتع بها؛ حيث إخفاء الهُوية، وسهولة الاستخدام، وسرية المعاملات، فضلًا عن استخدامها الطائرات بدون طيار في العديد من المهام كالمراقبة والدعاية وتنفيذ بعض العمليات. من ثمَّ أدى توظيف التطورات التكنولوجية الحديثة من قبل التنظيمات الإرهابيَّة إلى تهديد أمن الدول والمجتمعات؛ مما يقتضي ضرورة تحليل الكيفية التي تستغل بها تلك التنظيمات التكنولوجيا الجديدة لأغراض خبيثة.

أولًا: الإطار النظري والمنهجي

مفهوم الابتكار الخبيث

تعود الإرهاصات الأولى لتناول الجانب السلبي للابتكار الخبيث إلى حقل الاقتصاد؛ حيث أشار كل من «نيلسون» و«وينتر» في كتابهما الذي جاء بعنوان «نظرية تطورية للتغير الاقتصادي» إلى أن تطور سلوكيات الشركات في بيئة السوق ما هو إلا نتاج تراكمي للمعرفة المؤسسية والتجريب؛ التي تتداخل فيها عوامل عدة كالبنية المؤسسية والمنافسة، وقد أوضحا أن توظيف الشركات للابتكار في عملية المنافسة في بيئة السوق قد يحمل نتائج سلبية ويحقق أهدافًا أنانية، (Nelson& Winter,1982) ومن ثمَّ بدأ التأطير للجانب السلبي للابتكار.

وفي مرحلة لاحقة برز مفهوم «الاستخدام المزدوج للتكنولوجيا»، وتبلور نظريًّا في أعقاب الحرب الباردة؛ حيث عرفته دراسة جاءت بعنوان «التكنولوجيات ذات الاستخدام المزدوج ومراقبة الصادرات في حقبة ما بعد الحرب الباردة» بأنه التقنيات القابلة للتطبيق في الاستخدامات العسكرية والمدنية (أي التجارية) على

حد سواء، مستعرضةً التحديات التي تواجه سياسات مراقبة تصدير التكنولوجيا بعد انتهاء الحرب الباردة، لافتةً إلى احتمالية انتقال التكنولوجيا مزدوجة الاستخدامات إلى الجهات الفاعلة غير الحكومية بما في ذلك التنظيمات الإرهابيَّة (National Research Council, 1994).

وقد تصاعد استخدام التنظيمات الإرهابيَّة للتكنولوجيا، ولاسيما الإنترنت، ومن ثم بدأت بعض أدبيات الإرهاب تشير إلى هذا الطرح، حيث ركَّزت «دراسة التعلم التنظيمي والنشاط الإسلامي» على المرونة التي تتمتع بها التنظيمات الإرهابيَّة بجانب قدرتها على التعلم، لافتةً إلى دور الإنترنت في تطوير قدراتها (Kenney,2008).

ومع التطورات التي شهدتها البيئة الرقمية للتنظيمات الإرهابيَّة، ولا سيما «داعش»، برز مصطلح «الابتكار الخبيث» كمفهوم مستقل في دراسات الإرهاب؛ إذ بدأت الأدبيات تسلِّط الضوء عليه بصورة أكثر وضوحًا، فقد أشارت دراسة بعنوان «الابتكار الخبيث في التنظيمات الإرهابيَّة» إلى وجود عوامل داخلية وخارجية تؤدي دورًا في لجوء التنظيمات الإرهابيَّة إلى الابتكار؛ إذ إن توافر الموارد المادية والبشرية داخل التنظيمات يعزِّز من عملية الابتكار، كذلك يسهم الضغط الأمني من ناحية ورغبة التنظيمات الإرهابيَّة في التفوق بعضها على بعض في توجهها نحو الابتكار الخبيث (Gill& Cushenbery, 2013).

كذلك أوضحت دراسة بعنوان «الابتكار والتكيف في الإرهاب الجهادي: دراسة حالة القاعدة وداعش» أن هدف التنظيمات الإرهابيَّة من الابتكار الخبيث تأمين اتصالها وبنيتها التحتية والحفاظ على بقائها، ولا سيما مع توسع سياسات المكافحة وممارستها للضغوط الأمنية على هياكلها التنظيمية (Brantly, 2017). وفي السياق ذاته، تناول تقرير بعنوان «الخوارزميات والإرهاب: الاستخدام الخبيث للذكاء الاصطناعي لأغراض إرهابية» صادر عن الأمم المتحدة؛ المخاطر المحتملة لوقوع الذكاء الاصطناعي في أيدي التنظيمات الإرهابيَّة (United Nations Office of Counter-Terrorism, 2021).

وفي ضوء ما تقدم، تبنت الدراسة مفهوم «الابتكار الخبيث» كإطار نظري وتحليل أصيل، على الرغم من الندرة النسبية للأدبيات التي قدمت تأطيرًا مفاهيميًّا خاصًّا به، وبتطبيق المفهوم على الدراسة، يمكن القول: إن «الابتكار الخبيث» هو توظيف التنظيمات الإرهابيَّة للتكنولوجيا الحديثة من أجل تحقيق أهدافها؛ إذ يمثل تطورًا بارزًا في سلوك التنظيمات الإرهابيَّة؛ وذلك على خلفية دمجها مسارين رأسيين، أولهما: الاعتماد على التكنولوجيا المتاحة، بما يعني التوظيف المزدوج للتكنولوجيا، ثانيهما: استغلال اللامركزية التي يتميز بها الفضاء السيبراني، ومن ثمَّ يعزِّز هذا الدمج من التهديدات المرتبطة بالتنظيمات الإرهابيَّة على خلفية تجاوز الحدود المادية والجغرافية.

المنهج الوصفي التحليلي

اعتمدت الدراسة على المنهج الوصفي التحليلي؛ حيث يعنى بدراسة الظواهر كما هي في الواقع، ويدرس خصائصها، وأنماطها، والعوامل المؤثرة فيها، ولا يقتصر المنهج الوصفي على جمع البيانات حول الظاهرة، بل يمتد دوره إلى تحليل وربط وتفسير هذه البيانات واستخلاص نتائج منها (العسولي، 2020) وبتطبيق المنهج الوصفي التحليلي على الدراسة نجد أنه يقدم إطارًا منهجيًّا قائمًا على وصف الأدوات والنماذج

والأنماط التي تعتمد عليها التنظيمات الإرهابيَّة في توظيفها للابتكار الخبيث، كذلك يقدم إطارًا تحليليًّا حول نتائج وتداعيات هذا التوظيف.

مصادر جمع المعلومات

تستند هذه الدراسة إلى مصادر متنوعة؛ مثل: كتب، وأطروحات علمية، وأوراق بحثية، بجانب تقارير أممية صادرة عن الأمم المتحدة، فضلًا عن دراسات محكَّمة صادرة عن مراكز أبحاث عربية وأجنبية.

ثانيًا: الابتكار الخبيث في الدعاية والتجنيد

وظَّفت التنظيمات الإرهابيَّة الابتكار الخبيث في الدعاية والتجنيد؛ حيث اعتمدت على وسائل التواصل الاجتماعي، والتطبيقات المشفرة، وألعاب الفيديو، والذكاء الاصطناعي التوليدي من أجل إيجاد مساحات افتراضية لنشاطها، وهو ما سوف يتم إيضاحه على النحو التالي:

وسائل التواصل الاجتماعي وتطبيقات المراسلة

قديمًا، اعتمدت التنظيمات الإرهابيَّة على وسائل الإعلام التقليدية؛ مثل: المنشورات والمطبوعات والمحادثات الشخصية لتجنيد أفرادها. لكن في الوقت الحالي، أتاحت التكنولوجيا الحديثة أدوات أكثر تأثيرًا، يأتي على رأسها وسائل التواصل الاجتماعي، التي استغلتها تلك التنظيمات من أجل الترويج لأفكارها المتطرفة بجانب جذب مجندين جدد.

فقد أتاح الشيوع العالمي لهذه المنصات الإلكترونيَّة مساحةً أمام الشبكات الإرهابيَّة للاندماج والانتشار عبر الحدود الوطنية والثقافات المختلفة، ومن ثمَّ أصبح الإرهابيون قادرين الآن على نشر أفكارهم خارج دوائرهم الاجتماعية، ومن ثم الوصول إلى فئات لم تكن متاحة لهم سابقًا، وهو ما انعكس بشكل جلي على أعداد المقاتلين الأجانب الذين انضموا إلى تنظيم «داعش» إبان فترة خلافته المزعومة في العراق وسوريا؛ إذ أشار تقرير أممي صادر في يناير 2019 إلى أن أعدادهم تزيد على 40 ألف مقاتل، وينتمون إلى جنسيات مختلفة،(United Nations Security Council, 2019)؛ مما يؤكد الدور الذي أدَّته وسائل التواصل الاجتماعي في تجنيد هؤلاء.

بجانب وسائل التواصل الاجتماعي، تستخدم جميع التنظيمات الإرهابيَّة في الوقت الحالي تقنيات التشفير. فعلى سبيل المثال، أصبح تطبيق «تيليجرام»، التطبيق المفضل لمعظم التنظيمات الإرهابيَّة، ويرجع ذلك إلى أنه يوفر «محادثات سرية» بتشفير شامل؛ حيث لا يخزن في أي مكان آخر سوى هاتف المستخدم. وقد أثَّرت هذه الأشكال السهلة والمجانية غالبًا من التشفير وإخفاء الهوية بشكل كبير على عملية التجنيد، حيث سمحت للإرهابيين بإرسال الرسائل والملفات بشكل فوري، والبقاء مخفيين أثناء القيام بذلك (Bloom, 2018).

ومع الجهود المتُخذة من أجل تعطيل نشاط التنظيمات الإرهابيَّة على وسائل التواصل الاجتماعي والتطبيقات المشفرة؛ فإنها ما زالت متمسكةً بنشاطها؛ مثل: فيسبوك وإنستغرام وتيك توك وإكس (تويتر سابقًا)، بالإضافة إلى تطبيقات المراسلة؛ مثل: تيليجرام وواتساب وإليمنت.

وفي هذا السياق، أصدر «معهد الحوار الإستراتيجي» دراسة حديثة، أكَّدت أن منصات التواصل الاجتماعي وتطبيقات المراسلة لا تزال عُرضةً للاستغلال من قِبل تنظيم «داعش»، وأنه لا يزال

مؤثرًا عبر تلك المنصات، ويعمل في الوقت الحالي على توسيع نطاق وجوده؛ ليشمل تطبيقات جديدة ناشئة، تُمكنه من الصمود في وجه الجهود الرامية لتقويض نشاطه (Ayad, 2025).

ومن ثمَّ، يشكل استغلال تلك التنظيمات لوسائل التواصل الاجتماعي والتطبيقات المشفرة تحديات كبيرة أمام جهود الأجهزة المعنية بمكافحة الإرهاب؛ وذلك بسبب الحجم الهائل للمواد الإلكترونية المُشاركة، بالإضافة إلى برامج التشفير المتطورة التي يصعب تتبعها.

ألعاب الفيديو

تحوَّلت ألعاب الفيديو إلى شبكات رقمية واسعة تربط مليارات الأشخاص حول العالم؛ حيث يؤديها ما يقرب من 3 مليارات شخص في جميع أنحاء العالم (Hartgers& Leidig, 2023). إلا أن هذا التوسع السريع حمل معه واقعًا مقلقًا؛ إذ استغلت التنظيمات الإرهابيَّة منصات الألعاب لتجنيد ونشر التطرف متجاوزةً الحواجز الجغرافية لجذب الشباب حول العالم (Awasthi,2024).

وقد استغلت التنظيمات الإرهابيَّة ألعاب إطلاق النار العنيفة متعددة اللاعبين من منظور الشخص الأول لجذب الشباب. ففي عام 2014، عندما بدأ تنظيم «داعش» في السيطرة على الأراضي، أصدر لعبة فيديو خاصة به بعنوان «صليل الصوارم»: وهي لعبة إطلاق نار من منظور الشخص الأول، مستوحاة من سلسلة ألعاب «غراند ثفت أوتو» الشهيرة؛ إذ تولى اللاعبون دور مقاتلي «داعش» الذين يقاتلون في مناطق صراع حقيقية؛ مثل: العراق وسوريا. وقد نُشرت مقاطع دعائية للعبة على مواقع ومنصات متعددة عبر الإنترنت، أبرزها يوتيوب، الذي حقَّق عند إصدار اللعبة عام ٢٠١٤، ٣.٥ مليار مشاهدة شهريًّا على قنوات الألعاب الخاصة به فقط (AlRawi, 2018).

كما عمل التنظيم على إعادة تصميم ألعاب أخرى؛ مثل: «أرما3» وهي من الألعاب القتالية الأكثر شهرةً على مستوى العالم؛ حيث عمل على إضافة تعديلات برمجية عبر إضافة الصور والأصوات التي تروج للتنظيم، وتدعم أجندته (أيمن، 2023). وفي يناير 2019، استخدم التنظيم تطبيق «تيليجرام» لتزويد أنصاره بتعليمات محددة حول كيفية استخدام منصات الألعاب لتجنيد أعضاء جدد (Concentric, 2019).

ومن ثمَّ، وظَّف تنظيم «داعش» هذه الألعاب لتحقيق أهدافه المتمثلة في توسيع نطاق الدعاية الخاصة به في مساحات افتراضية، بجانب استقطاب الشباب؛ إذ تتمتع تلك الألعاب بشعبية كبيرة لدى اللاعبين الذكور، بالإضافة إلى محاولة تحقيق المحاكاة الافتراضية للعمل الميداني عبر التخطيط والتنفيذ لمعارك افتراضية داخل هذه الألعاب بعيدًا عن التعقب والمراقبة (أيمن، 2023).

الذكاء الاصطناعي

مع التطورات التي شهدها الذكاء الاصطناعي، وبروز نماذج أكثر تطورًا كأنظمة الذكاء الاصطناعي التوليدي، مثل: تشات جي بي تي ChatGPT، تصاعدت العديد من المخاوف الأمنية حول احتمالية سعي تلك التنظيمات إلى الاستفادة من هذه الأدوات من أجل تعزيز عملياتها وتوسيع نشاطها ونشر أفكارها (النجار، 2024).

وفي هذا السياق، أصدرت العديد من التنظيمات الإرهابيَّة إرشادات صريحة حول كيفية الاستفادة بشكل فعَّال من الذكاء الاصطناعي التوليدي لإنشاء المحتوى. إذ أعلنت جماعة تابعة لتنظيم «القاعدة» في فبراير2023، أنها ستبدأ بعقد ورش عمل في مجال الذكاء الاصطناعي عبر الإنترنت، وفي وقت لاحق، أصدرت الجماعة نفسها دليلًا حول استخدام روبوتات الدردشة القائمة على الذكاء الاصطناعي (Schaer,2024).

وفي الوقت الحالي، تستخدم التنظيمات الإرهابيَّة الذكاء الاصطناعي التوليدي في نشر الدعاية، سواء الصور أو مقاطع الفيديو أو مقاطع الصوت المزيفة. ففي شهر مارس 2023، وبعد أن قتل «داعش- خراسان» أكثر من 135 شخصًا في هجوم على مسرح في موسكو، قام أحد أتباع التنظيم بإنشاء بث إخباري مزيف حول الحدث، ونشره بعد أربعة أيام من الهجوم. وقد تبع هذا المقطع أربعة مقاطع مماثلة على الأقل، تتحدث عن أنشطة التنظيم في إفريقيا والشرق الأوسط.

كذلك استخدمت التنظيمات الإرهابيَّة الذكاء الاصطناعي التوليدي في التزييف العميق؛ حيث قامت بتزييفات صوتية للمشاهير والسياسيين، وهم يغنون الأناشيد الجهادية، وتمثل هذه التحركات من قبل التنظيمات، تطورًا مُعقَّدًا في الأساليب التي تستخدمها لتوسيع نطاق محتواها (Siegel, 2024).

وعلى صعيدٍ موازٍ، من المحتمل أن يؤدي الذكاء الاصطناعي في المستقبل أدوارًا مهمَّة في التجنيد؛ حيث يمكن لروبوتات الدردشة المدعومة بالذكاء الاصطناعي التفاعل مع الأفراد المستهدفين عبر تزويدهم بمعلومات تقع في نطاق اهتماماتهم؛ إذ تُمكِن نماذج اللغة الكبيرة التنظيمات الإرهابيَّة من توفير تجربة مشابهة بالبشر دون تدخلات بشرية، ومن ثمَّ الوصول إلى المجندين المحتملين الذين يتعاطفون مع قضيتهم (البهي، 2024).

كما يمكن للتنظيمات الإرهابيَّة استخدام الذكاء الاصطناعي التوليدي لتجاوز سياسات تعديل المحتوى على وسائل التواصل الاجتماعي أيضًا. على سبيل المثال، تستخدم شركات وسائل التواصل الاجتماعي عادةً تقنية تسمى «البصمة الرقمية» أو تتبع «البصمة الرقمية» للمحتوى المتطرف، لإزالة المحتوى الإرهابي عبر المنصات. ومع ذلك، من خلال التلاعب بدعاياتهم باستخدام الذكاء الاصطناعي التوليدي، يمكن للتنظيمات الإرهابيَّة تغيير البصمة الرقمية للمحتوى (Mathur, Broekaert& Clarke,2024).

وفي ضوء ما تقدم، يمكن القول: إن التنظيمات الإرهابيَّة وظَّفت الابتكار الخبيث في مجال الدعاية والتجنيد عبر استغلال وسائل التواصل الاجتماعي، وتطبيقات المراسلة وألعاب الفيديو، بما يعزِّز من جاذبيتها الدعائية، ويساعدها في الوصول إلى مساحات جغرافية، وشرائح عمرية، لم تتمكن من الوصول إليها من قبل، وفي الوقت الحالي بدأت تتخذ خطوات لاستغلال الذكاء الاصطناعي التوليدي في عمليات الدعاية والتجنيد، إلا أن مدى هذا التوظيف لا يرتبط فقط بالقدرات التي يوفرها، لكنه يرتهن في الوقت ذاته بجملة من العوامل؛ يتعلق أولها بأيديولوجية تلك التنظيمات ومدى ملاءمة أدوات الذكاء الاصطناعي للقناعات الفكرية الخاصة بها، وينصرف ثانيها إلى القدرات البشرية واللوجستية المالية المتوافرة لديها، ويتصل ثالثها بالسياق الذي تعمل فيه.

ثالثًا: الابتكار الخبيث في التمويل

تميَّزت التنظيمات الإرهابيَّة بالمرونة التمويلية؛ حيث تعمل على تعديل إستراتيجيتها التمويلية لتتماشى مع الضغوط الأمنية التي تُمارس عليها، وهو ما اتضح في توظيف تلك التنظيمات للعملات الافتراضية على الشبكة المظلمة؛ الأمر الذي سوف يتم إيضاحه على النحو التالي:

العملات الافتراضية

يزداد استخدام التنظيمات الإرهابيَّة للعملات الافتراضية بالنظر لما تقدمه هذه العملات من مزايا تتعلق بإخفاء الهُوية، وسهولة الاستخدام، وسرية المعاملات ودقتها، فضلًا عن إمكانية التحويل الفوري إلى جميع أنحاء العالم دون استخدام البنوك التي تتطلب مزيدًا من الشفافية والإبلاغ عن المعاملات المشبوهة (البهي، 2019).

وقد شجعت السمات سالفة الذكر التنظيمات الإرهابيَّة على استخدام تلك العملات؛ حيث تم استخدامها في عدد من الأنشطة المالية، مثل: جمع التبرعات، والاتجار غير المشروع، وتمويل الهجمات، ولا سيما أن الأولى تسعى إلى الحصول على تمويل مجهول المصدر وآمن وسهل التوافر. (Mappaselleng& others, 2025).

وقد بدأت شواهد توظيف التنظيمات الإرهابيَّة للعملات الافتراضية تتبلور مع إصدار أحد مؤيدي تنظيم «داعش» مقالًا على الإنترنت بعنوان «بيتكوين وصدقة الجهاد» في عام ٢٠١٤. إذ يروج المقال لاستخدام عملات «بيتكوين» كوسيلة لتسهيل الدعم الاقتصادي للجهاديين والالتفاف على النظام المصرفي الغربي، الذي يحد من التبرعات للجهاد من خلال القيود المفروضة على النظام المالي.

ويُعدُّ «بيتكوين» أول عملة افتراضية تُستخدم من قِبل تلك التنظيمات في حملات التمويل الجماعي، ولا تزال شائعة الاستخدام في تمويل الإرهاب وغسل الأموال على نطاق أوسع (Fatf, 2023)، وتزعم بعض التقارير أن تنظيم «داعش» استخدم تلك العملات لتمويل جزئي لهجمات باريس 2015 وبروكسل 2016، من خلال شراء أسلحة وبطاقات مسبقة الدفع عبر مدفوعات العملات الافتراضية. (Entenmann, Berg, 2018) كذا أشار تقرير أممي، صادر في 2023، إلى أن مكتب «الكرار» التابع للتنظيم يحوِّل ما يصل إلى 25000 دولار شهريًّا من العملات الافتراضية إلى أفرعه في العراق وسوريا وخراسان United Nations Security Council, February) (2023

كما أفاد جهاز مكافحة الجرائم المالية (FinCEN) التابع لوزارة الخزانة الأمريكية في إبريل 2025 بأن «داعش» والأفرع التابعة له أصبحوا يعتمدون بشكل متزايد على الأصول الرقمية، بما في ذلك العملات الافتراضية، كوسيلة لتخزين الأموال ونقلها (intelligence,2025).

وفي سياق متصل، أعلنت وزارة العدل الأمريكية في أغسطس 2020 عن تعطيل ثلاث حملات لتمويل الإرهاب عبر الإنترنت، مشيرة إلى أن هذا الجهد يمثل «أكبر عملية مصادرة على الإطلاق لحسابات العملات الافتراضية للتنظيمات الإرهابيَّة»، ووفقًا لوزارة العدل، أدارت «القاعدة» وبعض الأفرع التابعة لها في سوريا إحدى الحملات الثلاث، مستفيدةً من العملات الافتراضية لجمع الأموال ونقلها وإخفائها لتمويل الإرهاب . (Department of Justice, 2020)

وقد أصبحت العملات الافتراضية الناشئة أكثر جاذبيةً للتنظيمات الإرهابيَّة في ضوء الميزات التي تتمتع بها. فعلى سبيل المثال، كانت «البيتكوين» و«تثير» العملات الافتراضية المفضلة لدى تنظيم «داعش» قبل عام 2020، لكن في الوقت الحالي أصبحت عملة «مونرو» منتشرة داخل شبكات التنظيم؛ نتيجة تراجع جاذبية «البيتكوين» على خلفية زيادة الشفافية في المعاملات المالية والمحاسبة مع تقنيات تتبع blockchain المحسنة التي تبنتها وكالات الأمن في جميع أنحاء العالم؛ مما دفع «داعش» إلى التحول نحو «مونرو» التي تقدم ميزات خصوصية متقدمة؛ مثل: العناوين الخفية والمعاملات السرية، ومن ثمَّ صعوبة تتبع المعاملات المرتبطة بها (Roul,2024).

ومع مميزات العملات الافتراضية، لا يمكن إغفال أن ثمة تحديات تواجه التنظيمات الإرهابيَّة مرتبطة بإدارة الأموال من خلال تلك العملات؛ لكونها تتطلب بنية تحتية مالية قوية ومستويات متعددة من الإدارة والتخطيط المالي . (Ogele, 2024)

الشبكة المظلمة

يقتضي الحديث عن استخدام التنظيمات الإرهابيَّة للعملات الافتراضية الإشارة إلى استخدام تلك التنظيمات للشبكة المظلمة، والشبكة المظلمة هي جزء مجهول الهُوية ومشفر من شبكة الويب العالمية، ولا يمكن الوصول إليه عبر محركات البحث التقليدية. ويمكن تقسيم شبكة الويب إلى ثلاث فئات رئيسة؛ الفئة الأولى: هي الويب السطحي، وهو متاح للعامة دون الحاجة إلى مصادقة أو دفع، ويتم فهرسته بواسطة محركات البحث، مثل: جوجل؛ مما يسمح بتحديد هُوية أصحاب المصلحة، ويجعله عرضةً للمساءلة القانونية.

وتضم الفئة الثانية الويب العميق، الذي يشمل أقسامًا من الإنترنت غير متاحة للعامة، أو غير مفهرسة بواسطة محركات البحث. ويكون الوصول إلى هذا الجزء من الويب مقيدًا، إما بسبب متطلبات المصادقة، أو لأنه جزء من شبكة خاصة. ونتيجةً لإجراءات المصادقة هذه، هناك مستوى متزايد من المساءلة مقارنةً بالويب السطحي. والفئة الثالثة الويب المظلم، المعروف أيضًا باسم الشبكات المظلمة، ويشكل الجزء الخفي من الإنترنت الذي لا تُدرجه محركات البحث، ويتطلب برامج مخصصة للوصول إليه (Mappaselleng& others, 2025).

وقد بدأت التنظيمات الإرهابيَّة في تحويل نشاطها إلى الشبكة المظلمة، بسبب زيادة مراقبة الويب السطحي من قبل شركات وسائل التواصل الاجتماعي والسلطات؛ حيث تستخدمها لتنفيذ مجموعة من الأنشطة، بما في ذلك جمع التبرعات من خلال العملات الافتراضية، والحصول على الأسلحة، والتخطيط للهجمات، بجانب قيامها بنشر الأيديولوجيات المتطرفة وتجنيد أعضاء جدد. وتتيح الشبكة المظلمة ميزات رئيسة؛ مثل: إخفاء الهُوية، والرسائل المشفرة؛ مما يجعلها ذات قيمة عالية لتحقيق أهداف تلك التنظيمات بشكل أكثر فاعليةً وسريةً دون التعرض للاستهداف من قبل السلطات الأمنية.

وفي هذا السياق، أشار تقرير بعنوان «الإرهاب في الظلام: كيف يستخدم الإرهابيون التشفير والشبكة المظلمة والعملات الافتراضية»، صادر عن جمعية هنري جاكسون، إلى أن الشبكة المظلمة أصبحت «ملاذًا آمنًا» للتنظيمات الإرهابيَّة في أنشطتها، بما في ذلك التخطيط للهجمات القادمة (Malik, 2018).

ومن ثمَّ يتيح تواجد التنظيمات الإرهابيَّة على الشبكة المظلمة الفرصة لتعزيز مواردها المالية، وتحسين كفاءة عملياتها المادية.

ومن ثمَّ، يمكن القول: إن توظيف التنظيمات الإرهابيَّة للابتكار الخبيث في تمويل أهدافها يحمل العديد من التهديدات الأمنية على خلفية تجاوز العملات الافتراضية للأنظمة المصرفية التقليدية، فضلًا عن صعوبة تتبعها؛ مما يُعقد جهود المكافحة، وينعكس على نجاح التنظيمات الإرهابيَّة في الحفاظ على مواد تمويلها بعيدًا عن ساحات الرقابة والرصد.

رابعًا: الابتكار الخبيث في تنفيذ الهجمات

وظَّفت التنظيمات الإرهابيَّة الابتكار الخبيث في تنفيذ هجماتها؛ حيث اعتمدت في ذلك على الطائرات بدون طيار، بجانب الهجمات السيبرانية، وهو ما سوف يتم استعراضه على النحو التالي:

الطائرات بدون طيار

اعتمدت التنظيمات الإرهابيَّة بشكل متزايد على الطائرات بدون طيار في عملياتها؛ نظرًا لانخفاض تكلفتها وسهولة استخدامها، فضلًا عن توفيرها ميزة التشغيل عن بُعد؛ مما يقلِّل من المخاطر على أعضائها. فمن خلال التحكم بها عن بُعد، يمكن لتلك التنظيمات أن تظل مجهولة الهُوية ويصعب تتبعها (Aguilera, 2023).

ويساعد استخدام الطائرات بدون طيار من قِبَل الفواعل العنيفة من دون الدول على تحقيق أهدافها الإستراتيجية والأيديولوجية والنفسية، كما يُمكِّنها من اكتساب حضورٍ جويٍ مانحة إياها قوة جوية «مُصغرة» بتكلفة زهيدة. ويمكن تقسيم استخدام التنظيمات الإرهابيَّة للطائرات بدون طيار إلى فئتين؛ الأولى: استخدامات دفاعية سلبية، بمعنى توظيفها في جمع المعلومات الاستخباراتية، وإجراء عمليات المراقبة، وتصوير الدعاية. والثانية: استخدامات هجومية نشطة، بمعنى تنفيذ هجمات وتوصيل المتفجرات إلى هدف (Dass, 2023).

وقد استخدم «داعش» إبان فترة تمدده في العراق وسوريا الطيارات بدون طيار في كلا المسارين، سواء في تنفيذ مهام استخباراتية واستطلاعية، أو في تنفيذ عمليات إرهابية، ولا سيما في العراق وسوريا (Rasler, 2018)، في حين اقتصر استخدام كل من حركة «الشباب» الصومالية، و«بوكو حرام» على الاستخدامات الدفاعية؛ حيث تبنت الأولى استخدامها لأغراض المراقبة وجمع المعلومات الاستخباراتية في الصومال وكينيا، فيما وظَّفتها الثانية للمهمة ذاتها في نيجيريا (Haugstvedt, 2020).

وفي دراسة حول استخدام الطائرات بدون طيار من قبل الفواعل العنيفة من دون الدول أجرتها شركة «هافارد هاوستفيدت»، تم تسجيل عدد 1122 هجومًا في الفترة من 2006 إلى 2023. وقد وقع ما نسبته 91.3 % من مجموع هذه الهجمات في الشرق الأوسط وشمال إفريقيا، مع وقوع 1109 من أصل 1122 هجمة بعد عام 2016.

وتسلط الدراسة الضوء على زيادة كبيرة في هذه الهجمات منذ عام 2017، مع 252 هجومًا، معظمها من عمليات تنظيم «داعش» في معارك الموصل والرقة. ثم انخفض عدد الهجمات إلى 35 هجومًا في عام 2018، لكنه ارتفع بشكل مطَّرد في السنوات التالية: 129 هجومًا في عام 2019، و105 هجمات في عام 2020، و206 هجمات في عام 2021،

و116 هجومًا في عام 2022، وقد بلغت ذروة هذه الهجمات في عام 2023، مع شن هذه الفواعل لنحو 265 هجومًا، وهو أعلى عدد مسجل في الدراسة (Haugstvedt, 2024).

وقد يحمل المستقبل العديد من التحديات المرتبطة باستخدامات التنظيمات الإرهابيَّة لتلك الطائرات، في ضوء احتمالية توظيفها في هجمات بيولوجية أو كيميائية، (Barten& Others, 2022))، بجانب احتمالية توظيف الطباعة ثلاثية الأبعاد في إنتاج أجزاء منها، وفي هذا السياق، أفادت تقارير أممية بإجراء حركة «الشباب» الصومالية تجارب على الطباعة ثلاثية الأبعاد لتطوير متفجرات وأجزاء طائرات بدون طيار؛ مما يزيد من حجم المخاطر المرتبطة بها (United Nations Security Council, July 2024).

المركبات ذاتية القيادة

ثمة تهديد مرتبط باحتمالية توظيف التنظيمات الإرهابيَّة للمركبات ذاتية القيادة مستقبلًا؛ إذ حذر «كريستوفر راي» (مدير مكتب التحقيقات الفيدرالي سابقًا)، من خطر استخدام المركبات ذاتية القيادة كسلاح من قبل الجهات الخبيثة في عام 2023 في المنتدى الاقتصادي العالمي (Crider,2023). ويأتي هذا التحذير متسقًا مع التاريخ الطويل الذي يجمع بين الإرهاب والمركبات؛ حيث حرضت التنظيمات الإرهابيَّة على استخدامها في هجماتها.

فعلى سبيل المثال، دعا «أبو محمد العدناني» (المتحدث السابق باسم تنظيم داعش) في سبتمبر 2014، أنصاره إلى استخدام المركبات كأسلحة، قائلًا: «ابذل جهدك في قتل أي أميركي أو فرنسي، أو أي من حلفائهم، فإن عجزت عن العبوة أو الرصاصة، فاستفرد، واسحق رأسه بحجر، أو اذبحه بسكين، أو ادهسه بالسيارة».

وقد استخدمت المركبات في هجمات الدهس المتعمد من قبل التنظيمات الإرهابيَّة، كما حدث في هجوم سوق الكريسماس في برلين في ديسمبر 2016، وفي برشلونة في أغسطس 2017. كما استخدمت المركبات في هجمات السيارات المفخخة، مثل: تفجير سيارة الإسعاف في كابول في عام 2018 الذي أسفر عن مقتل 103 أشخاص وإصابة 235 آخرين.

ومن ثم، فإن زيادة الاستقلالية في السيارات قد تكون تطورًا يعزِّز من نشاط التنظيمات الإرهابيَّة؛ مما يسمح لها بتنفيذ هجماتها عن بعد دون تعريض عناصرها إلى الخطر، لكن في المقابل ثمة اتجاه آخر، يرى أن ميزات الأمان التي تتمتع بها تلك المركبات، وتمكنها من اكتشاف وتجنب موقف مثل: الاصطدام بالمشاة، أو تشغيل نظام المكابح أو ضبط السيارة على مسار بديل، من شأنها أن تحبط المخططات الإرهابيَّة لاستخدام مثل هذه المركبات بهذه الطريقة (United Nations Office of Counter-Terrorism, 2021).

الهجمات السيبرانية

تهدف الهجمات السيبرانية إلى تعطيل أنظمة الحاسوب أو تدميرها أو التحكم فيها، أو تغيير البيانات المخزنة داخلها أو حظرها أو حذفها أو التلاعب بها أو سرقتها. وتتنوع أنماط هذه الهجمات؛ إذ يتخذ بعضها نمط «حجب الخدمة» الذي يهدف إلى تعطيل الشبكة أو التدخل فيها عن طريق إرسال كميات هائلة من الحزم إلى الخادم المستهدف؛ مما يجعل من المستحيل عليه الاستجابة لطلبات الخدمة المنتظمة من المستخدمين المصرح لهم.

بينما يتخذ البعض الآخر نمط «البرمجيات الخبيثة»، ويشير إلى مجموعة كبيرة من البرمجيات تتسلل إلى نظام الخادم المستهدف وتتسبب في تعطيله، ويمكن توظيفها من أجل الحصول على المعلومات السرية أو إلحاق الضرر بالبنية التحتية السيبرانية للمؤسسات المختلفة، ومن أمثلتها: برامج التجسس، وبرامج الفدية، وأحصنة طروادة، والفيروسات، والديدان.

في حين أن هناك نمطًا آخر لتلك الهجمات وهو «تخمين كلمات المرور» أي الحصول على كلمة مرور للوصول إلى مواقع الويب المحمية؛ مما يُمكّن التنظيمات الإرهابيَّة من دخول الأنظمة أو الشبكات، ومن ثمَّ تسبب العديد من التهديدات؛ على سبيل المثال، تعطيل الخدمات الأساسية، أو إحداث الفوضى، أو سرقة بيانات أو معلومات قيِّمة، أو تثبيت برامج ضارة. (United Nations Office of Counter-Terrorism, 2021)

وقد نجح تنظيم «داعش» والجماعات المؤيدة له في تنفيذ بعض الهجمات السيبرانية المحدودة، ففي الفترة ما بين ديسمبر 2016 ويناير 2017، نفذت مجموعتان من مجموعات التهديد الإلكتروني المؤيدتان لتنظيم «داعش» هجمات الحرمان من الخدمة؛ إذ طور منتدى «داعش» على الشبكة المظلمة في ديسمبر 2016، أداةً خاصة بالحرمان من الخدمة أطلق عليها "مدفع الخلافة - Caliphate Cannon" وشنت هجمات ضد أهداف حكومية في منطقة الشرق الأوسط، وفي الوقت نفسه تقريبًا، أعلنت مجموعة أخرى مؤيدة لتنظيم «داعش» تُعرف باسم الخلافة السيبرانية المتحدة (UCC) مسؤوليتها عن سبع هجمات مماثلة في بعض دول الشرق الأوسط (Flashpoint,2017).

كذلك استطاعت عناصر متعاطفة مع التنظيم اختراق مواقع الويب وحسابات التواصل الاجتماعي لأغراض التشويه ونشر المواد الدعائية. فعلى سبيل المثال، أعلن مركز شكاوى جرائم الإنترنت التابع لمكتب التحقيقات الفيدرالي (FBI) في منتصف إبريل لعام 2015 أن أفرادًا متعاطفين مع «داعش» يُعطلون عمليات مواقع WordPress (نظام نشر ويب مجاني ومفتوح المصدر) (TrendMicro,2015).

يضاف إلى ما تقدم نجاح «أرديت فيريزي» (قرصان إلكتروني) في عام 2015 من الوصول إلى خوادم في الولايات المتحدة، واستخرج معلومات تعريف شخصية لما يقرب من 1300 فرد من الجيش والحكومة الأمريكية، وتواصل مع عناصر تنظيم «داعش» عبر تويتر وسكايب، من أجل تسليم هذه المعلومات إلى قسم القرصنة في التنظيم، الذي بدوره قام بنشر هذه البيانات لاحقًا (U.S. Department of Justice, 2016).

وفي هذا السياق، أفادت مؤسسة البيانات الدولية IDC، في أحدث تقاريرها الصادر عام 2025 أنه من المتوقع أن يرتفع الإنفاق العالمي على الأمن بنسبة 12.2% في عام 2025، وذلك مع تزايد التهديدات السيبرانية العالمية، التي تعززها تقنيات الذكاء الاصطناعي التوليدي والذكاء الاصطناعي عامةً (IDC,2025)، الأمر الذي يقتضي تجنب التعامل مع الأمن السيبراني وفق إستراتيجية ضيقة تركز على الأبعاد المادية والفنية فقط، وإنما يجب تبني إستراتيجية واسعة تشمل القوة الناعمة بأبعادها المختلفة (علام، 2024).

وارتباطًا بما تقدم، يمكن القول: إن توظيف الابتكار الخبيث من قبل التنظيمات الإرهابيَّة في تنفيذ الهجمات المادية أو السيبرانية، يُعدُّ تقويضًا لسيادة

الدولة من ناحية، ويضعف احتكارها للعنف المشروع من ناحية أخرى، لكن في الوقت ذاته، تعتبر قدرات التنظيمات الإرهابيَّة على شن الهجمات الإلكترونية ذات مستوى معقول، وليس متطورًا، فليس هناك أدلة دامغة على أنها قادرة على شن هجوم إلكتروني واسع النطاق من النوع الذي يسبب الموت أو الدمار.

وفي حين تزايد القلق بشأن الهجمات الإلكترونية المحتملة في السنوات الأخيرة، بما يتناسب مع النمو في البنية الأساسية الرقمية والسيبرانية، فإن الغالبية العظمى من الهجمات السيبرانية الخطيرة التي تسببت في أضرار جسيمة أو تعطيل، يمكن إرجاعها إلى الدول؛ إذ إن الدول، في الأغلب الأعم، حتى الوقت الحالي هي التي تملك القدرات السيبرانية القادرة على التسبب في الدمار من خلال الوسائل الإلكترونية الرقمية، لكن هذا الطرح لا يعني ضرورة متابعة تطور القدرات السيبرانية للتنظيمات الإرهابيَّة.

خامسًا: سياسة فعَّالة لمكافحة الابتكار الخبيث للتنظيمات الإرهابيَّة

ثمة حاجة مُلحَّة إلى تطوير سياسات واضحة عملية من أجل التعاطي مع توظيف التنظيمات الإرهابيَّة للابتكار الخبيث في آليات وإستراتيجيات عملها؛ وذلك لضمان اتخاذ تدابير استجابة مناسبة لمثل هذه التهديدات، ومن ثم هناك محددات أساسية ينبغي أن تتم صياغة تلك السياسات في ضوئها، ويمكن تناولها على النحو التالي:

- إدراك طبيعة التهديد: يقتضي وضع سياسات فاعلة لمكافحة الابتكار الخبيث للتنظيمات الإرهابيَّة الفهم الدقيق لطبيعة التهديد المرتبط بالكيفية التي تلجأ لها التنظيمات الإرهابيَّة لتوظيف التكنولوجيا الحديثة لتحقيق أهدافها. وهذا الفهم يتطلب توسيع نطاق جمع البيانات والأدلة حول استخدام تلك التنظيمات للتقنيات الناشئة، بجانب إجراء المزيد من الأبحاث حول طبيعة التهديد وأنماطه المختلفة.

إذ يضمن إدراك وفهم التهديد أن تكون السياسات استباقيةً ووقائيةً، وليست قائمة على رد الفعل فقط، ومن ثم يساعد بناء معرفة حقيقية للجهات المعنية بمكافحة الإرهاب على اتخاذ سياسات فاعلة مستدامة، وبدون إدراك شامل لطبيعة التهديد ستظل جهود المكافحة متراجعة أمام تطور توظيف التنظيمات الإرهابيَّة للتكنولوجيا الحديثة.

- التوازن بين الأمن القومي وحقوق الإنسان: تتطلب تلك السياسات تحقيق التوازن بين مفهومي الأمن القومي وحقوق الإنسان؛ حيث يحتل كلا المفهومين أهمية قصوى في سياسات الدول؛ وذلك لأن صيانة الأمن القومي جزء أساسي من الحفاظ على حقوق الإنسان.

ويمكن القول: إن الجهود التي تبذلها أجهزة إنفاذ القانون ومكافحة الإرهاب لجمع المعلومات الاستخباراتية، وجمع البيانات، ومراقبة استخدام الإرهابيين للشبكة المظلمة، قد تنتهك عددًا من الحقوق، بما في ذلك، على سبيل المثال، الحق في الخصوصية، وحماية البيانات، أو الحق في حرية التعبير. ومن ثمَّ من الضروري أن تكون الأطر التشريعية التي تحكم سياسات مكافحة الإرهاب واضحة، وأن توفر ضمانات كافية ضد الانتهاكات بما يحافظ على التوازن بين اعتبارات الأمن القومي

وحقوق الإنسان الذي من شأن تحققه أن يؤدي إلى رفع فاعلية جهود مكافحة الإرهاب واستدامتها.

- تطوير الأطر القانونية: تستلزم سياسات مكافحة الابتكار الخبيث للتنظيمات الإرهابيَّة تطوير الأطر القانونية وتحديثها، فمع تصاعد التهديدات الناشئة المرتبطة باستخدام التنظيمات الإرهابيَّة للتكنولوجيا، أصبح من الضروري تحديث التشريعات من أجل توفير أطر قانونية مصممة للعصر الرقمي، تعالج التهديدات المرتبِطة بالأنشطة الإرهابيَّة المتطورة. فعلى سبيل المثال، هناك حاجة مُلِحَّة لتطوير قوانين الأمن السيبراني، بجانب سن تشريعات تستهدف تنظيم استخدام العملات الافتراضية، وتنظيم استخدام الذكاء الاصطناعي أيضًا، وما إلى ذلك من تحديات تكنولوجية صاعدة تتطلب منظومة قانونية حديثة ومتطورة.
- تعزيز الشراكات الفاعلة: تقتضي سياسات مكافحة الابتكار الخبيث للتنظيمات الإرهابيَّة ضرورة تعزيز الشراكات بين القطاعين العام والخاص، وبين جميع أصحاب المصلحة، بما في ذلك منظمات المجتمع المدني، وخبراء حقوق الإنسان. وتأتي تلك الشراكات عبر إستراتيجيات متنوعة؛ مثل: ورش العمل الإستراتيجية، ومنصات تبادل المعلومات، ومبادرات التعاون بين مختلف أصحاب المصلحة، بما يضمن الاستفادة من نقاط قوة كل الأطراف. ومن ثمَّ، يساعد التواصل المفتوح وتبادل الأفكار على سد فجوات المعرفة، وتعزيز تبادل المعلومات، والتحديد الاستباقي للتهديدات الناشئة، بما يعزِّز من الاستجابة بفاعلية للمشهد الديناميكي المرتبط بتصاعد تهديدات الابتكار الخبيث للتنظيمات الإرهابيَّة (United Nations Office of Counter-Terrorism,2024).
- تبادل الخبرات: يتطلب التصدي الفعَّال للتهديدات التقنية اتباع نهج متعدد الجوانب؛ لذلك ثمة حاجة مُلحَّة لوضع أطر عمل تعزِّز تبادل الخبرات والتعاون الوثيق بين كل من وحدات مكافحة الإرهاب، ووكالات إنفاذ القانون، والمتخصصين التقنيين، والخبراء الثقافيين واللغويين. الأمر الذي يعزِّز من دقة الكشف عن التهديدات من ناحية، ويساعد على فهم الفروق الدقيقة في الاتصالات الإرهابيَّة في مختلف السياقات الثقافية والاجتماعية من ناحية أخرى، ومن ثمَّ يضمن تبادل الخبرات فهمًا شاملًا للتحديات متعددة الجوانب التي تفرضها التهديدات التقنية المتطورة؛ مما يُسهل استجابةً أكثر شمولًا وتنسيقًا (United Nations Office of CounterTerrorism,2024).

التوصيات

ارتباطًا بهذا التوجه الإستراتيجي لمواجهة تلك التهديدات، تقترح الورقة جملة من التوصيات يمكن استعراضها على النحو التالي:

اتخاذ خطوات من شأنها تقويض نشاط التنظيمات الإرهابيَّة على وسائل التواصل الاجتماعي؛ وذلك عبر الآليات الآتية:

- التوسع في تدشين وحدات متخصصة لرصد المحتوى الرقمي المتطرف بلغات متعددة، وفي هذا الصدد ثمة تجارب عربية ناجحة؛ مثل: «مرصد الأزهر لمكافحة التطرف»، و«المركز العالمي لمكافحة الفكر المتطرف (اعتدال)».
- تتخذ بعض الجهات الفاعلة كالحكومات وشركات التكنولوجيا إجراءات من شأنها إزالة المحتوى الإرهابي عبر المنصات المختلفة، لكن ثمة حاجه مُلحَّة إلى أرشفة هذا المحتوى من أجل تعزيز فهم سلطات إنفاذ القانون لأنماط سلوك المتطرفين عبر الإنترنت.
- تلجأ المنافذ الإعلامية التابعة للتنظيمات الإرهابيَّة إلى حلول بديلة؛ مثل: نشر «النصوص المكسورة» كوسيلة لتجاوز الإشراف على المحتوى المتطرف؛ مما يتطلب تعزيز الأساليب الآلية للتعرف على تلك الحلول . (Ayad, 2025)
- تطبيق إجراءات مبتكرة لمواجهة استغلال التنظيمات الإرهابيَّة لألعاب الفيديو، وذلك عبر الآليات الآتية:
- تفعيل أدوار سلطات الأمن الداخلي في مراقبة منصات ألعاب الفيديو. على سبيل المثال، أنشأت الشرطة الدنماركية وحدة دورية عبر الإنترنت؛ حيث يتم تكليف الضباط بمراقبة شبكات الألعاب أثناء تأدية هذه الألعاب للبحث عن أي نشاط إرهابي وإجرامي (Danylov,2022)، ويمكن اللجوء لمثل هذه الإجراءات من أجل الحيلولة دون استغلال التنظيمات الإرهابيَّة لألعاب الفيديو.
- إيجاد بدائل تعزِّز المفاهيم الإيجابية؛ وذلك عبر تصميم ألعاب فيديو تركِّز على تعزيز قيم التسامح وقبول الآخر ونبذ العنف.
- رفع الوعي المجتمعي بمخاطر ألعاب الفيديو؛ بهدف تعزيز دور الأسر في متابعة سلوك أبنائها على تلك المنصات.
- العمل على دمج الذكاء الاصطناعي في إستراتيجيات مكافحة الإرهاب؛ إذ يدمج الذكاء الاصطناعي كميات ضخمة من البيانات من مصادر مختلفة لتوفير رؤى شاملة تساعد على الإنذار المبكر، إذ تساعد التحليلات التنبئية المدعومة بالذكاء الاصطناعي على تعزيز الوقاية من التهديدات الإرهابيَّة (النجار، 2024). وفي هذا الصدد، تجدر الإشارة إلى تجربة «Moonshot CVE» (وهي شركة تعمل على تطوير تقنيات ومنهجيات تكنولوجية جديدة لتحديد التهديدات عبر الإنترنت) إذ أطلقت مشروعًا قائمًا على إستراتيجية إعادة توجيه الأفراد الذين يبحثون عن محتوى متطرف إلى رسائل بديلة معتدلة؛ وذلك عبر تحليل سلوك المستخدمين باستخدام تقنيات التعلم الآلي.
- بناء قدرات موظفي إنفاذ القانون ومكافحة الإرهاب بالمهارات اللازمة لمواجهة التحديات المُتطورة التي تشكلها التهديدات السيبرانية، وذلك عبر الآليات التالية:
- رفع الكفاءة في مجالات رئيسة؛ مثل: الجرائم الإلكترونية، والتحليل الجنائي الرقمي، والويب المُظلم، وتحقيقات العملات الافتراضية، لتزويدهم بفهم شامل للمشهد السيبراني.

- تزويد هيئات إنفاذ القانون بأحدث الأدوات التكنولوجية المتاحة لمكافحة أنشطة التنظيمات الإرهابيَّة المعتمدة على توظيف التكنولوجيا.
- تبادل الخبرات بين أجهزة الأمن المعنية بالدول المختلفة، بما يشكل تصورًا شاملًا عن التهديدات المحتملة المرتبطة بالابتكار الخبيث للتنظيمات الإرهابيَّة، ومن ثمَّ بناء رؤية مشتركة فاعلة من شأنها مواجهة هذا النمط من التهديدات.
- العمل على تنظيم البنية التحتية للشبكة المظلمة، وذلك عبر الآليات الآتية:
- وضع سياسات أكثر صرامة لمراقبة خدمات الشبكات الافتراضية الخاصة (VPN)، وشبكات تور (Tor)، ومنصات الرسائل المشفرة التي تستخدمها التنظيمات الإرهابيَّة بشكل متكرر.
- تطوير برامج استخباراتية تستهدف تتبع نشاط التنظيمات الإرهابيَّة على الشبكات المظلمة، على أن تأتي تلك الإجراءات بالتوازي مع الحفاظ على حقوق الخصوصية على الإنترنت للمستخدمين الشرعيين.
- اتخاذ خطوات من شأنها تشديد الرقابة على العملات الافتراضية؛ وذلك عبر الآليات الآتية:
- تفعيل أنظمة تتبع المعاملات المالية لرصد حركة انتقال الأموال المشبوهة؛ مما يتطلب التغلب على بعض التحديات التي تواجه الرقابة الفعَّالة على تلك المعاملات في عدد من الدول العربية، ويأتي على رأسها: قصور الأطر التشريعية، وضعف البنية التحتية الرقمية، بجانب غياب التنسيق الفعَّال بين المؤسسات ذات الصلة، فضلًا عن تصاعد حدة الاضطرابات السياسية؛ مما يحول دون فرض رقابة فعَّالة.
- تطوير الأطر الرقابية والقانونية لضمان تحديد هُوية مستخدمي هذه العملات.
- زيادة التنسيق بين الدول في مجالات مكافحة تمويل الإرهاب.
- وضع أطر تنظيمية ضد أنظمة الطائرات بدون طيار، وذلك عبر الآليات الآتية:
- تفعيل أطر رقابية تستهدف تسجيل جميع الطائرات بدون طيار وربطها ببطاقات هُوية مشغليها.
- الاستثمار في إنتاج تقنيات أنظمة مضادة للطائرات بدون طيار فعَّالة للتعامل مع التهديد المستقبلي. وفي هذا الصدد، قدمت فرنسا نموذجًا غير تقليدي للتعامل مع تلك الطائرات؛ إذ دربت النسور على اصطيادها وإسقاطها (France24,2017).
- تشجيع مراكز الفكر والأبحاث العربية على التعاطي مع تطورات الظاهرة الإرهابيَّة، وذلك عبر الآليات الآتية:
- العمل على إنتاج دراسات نوعية تستهدف تحليل الإستراتيجيات الجديدة التي تعتمد عليها التنظيمات الإرهابيَّة.
- عقد ورش عمل ومؤتمرات من أجل تقديم أطر غير تقليدية للتعامل مع الظاهرة الإرهابيَّة.

المراجع

المراجع باللغة العربية

أيمن، هاجر. (2023). ماذا تغير في الخطاب الإعلامي لداعش؟ المركز المصري للفكر والدراسات الإستراتيجية .متاح على: https://ecss.com.eg/35568/

البهي، رغدة (2019). العملات الافتراضية وسيلة جديدة لتمويل الإرهاب.. أفكار مقترحة للمواجهة. المركز المصري للفكر والدراسات الإستراتيجية. متاح على: https:// ecss.com.eg/6484/

البهي، رغدة. (2024). حدود التوظيف: الإرهاب والذكاء الاصطناعي التوليدي. المركز المصري للفكر والدراسات، متاح على: https://ecss.com.eg/47950/

العسولي، عبد الصمد. (2020). المنهج الوصفي التحليلي في مجال البحث العلمي، مجلة المنارة للدراسات القانونية والإدارية، متاح على: https://drasah.com/Ar-chiving/website/1135202410081371.pdf

علام، مها. (2024). الفضاء السيبراني وسيادة الدولة في العلاقات الدولية.. دراسة نظرية بالتطبيق على حالة الولايات المتحدة الأمريكية، رسالة دكتوراه، كلية الاقتصاد والعلوم السياسية، جامعة القاهرة.

النجار، تقى. (2024). الذكاء الاصطناعي والإرهاب: ازدواجية الأدوار، الديمقراطية، العدد 96. 101-96.

مراجع باللغة الإنجليزية

Aguilera, A. (2023).Drone Use by Violent Extremist Organizations in Africa: The Case of Al-Shabaab. Global Network on Extremism & Technology. Available at:https://gnet-research.org/2023/07/05/drone-use-by-violent-extremist-organisations-in-africa-a-case-study-of-al-shabaab/

AlRawi, A. (2018) .Video Games, Terrorism, and ISIS's Jihad 3.0. Terrorism and Political Violence. 30(4).740-760. Available at:https://www.tandfonline.com/doi/full/10.1080/09546553.2016.1207633

Am intelligence.(2025).NEWS: ISIS using crypto to launder $25k per month, says US. Available at:https://www.amlintelligence.com/2025/04/news-isis-using-crypto-to-launder-25k-per-month-says-us/

Awasthi, S. (2024).Gaming platforms: A new frontier for extremist recruitment and radicalization. Observer Research. Available at: Foundation. Available at:https://www.orfonline.org/expert-speak/gaming-platforms-a-new-frontier-for-extremist-recruitment-and-radicalisation

Ayad, M. (2025). A decade after the Caliphate: The state of the Islamic State online. Institute for Strategic Dialogue. Available at:https://www.isdglobal.org/digital_dispatches/a-decade-after-the-caliphate-the-state-of-the-islamic-state-online/

Barten, D, Tin, D, De Cauwer, H, Ciottone, R & Ciottone, G. (2022). A Counter-Terrorism Medicine Analysis of Drone Attacks. Prehospital and Disaster Medicine, 37(2), 192–196. Available at:https://www.cambridge.org/core/journals/prehospital-and-disaster-medicine/article/abs/counterterrorism-medicine-analysis-of-drone-attacks/214B62C89F0D7F57FC7BAF16F1434E7F

Bloom, M.(2018).Assessing the Future Threat: ISIS's Virtual Caliphate. Orbis. Available at:https://www.sciencedirect.com/science/article/abs/pii/S0030438718300437

Brantly, A. (2017). Innovation and Adaptation in Jihadist Digital Security. Survival, 59(1), 79–

ist-financing-and-virtual-currencies-different-sides-same-bitcoin

Fatf. (2023). Crowdfunding for Terrorism Financing. Available at:https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Crowdfunding-Terrorism-Financing.pdf.coredownload.inline.pdf

Flash point. (2017).Cyber Jihadists Dabble in DDoS: Assessing the Threat. Available at: https://flashpoint.io/blog/cyber-jihadists-ddos/

France24.(2017).France deploys new force to combat drones - and it has claws. . Available at:https://www.france24.com/en/20170214-french-air-force-deploys-eagles-intercept-rogue-drones-military

Gill, P, Horgan, J., Hunter, S. T., & Cushenbery, L. D. (2013). Malevolent creativity in terrorist organizations. The Journal of Creative Behavior, 47(2), 125-151. Available at:https://doi.org/10.1002/jocb.28

Hartgers, M& Leidig, E. (2023). Fighting extremism in gaming platforms: a set of design principles to develop comprehensive P/CVE strategies. The International Centre for Counter-Terrorism. Available at:https://icct.nl/publication/fighting-extremism-gaming-platforms-set-design-principles-develop-comprehensive-pcve

Haugstvedt, H. (2020).A Flying Threat Coming to Sahel and East Africa? A Brief Review. Journal of Strategic Security. 14(1). 92-105.Available at:https://www.jstor.org/stable/26999979

Haugstvedt, H. (2024).Still aiming at the Harder Targets: An Update on Violent Non-State Actors' Use of Armed UAVs. Perspectives on Terrorism. 102. Available at: https://doi.org/10.1080/00396338.2017.1282678

Concentric. (2019).E-Recruits: How Gaming is Helping Terrorist Groups Radicalize and Recruit a Generation of Online Gamers. Available at:https://www.concentric.io/blog/e-recruits-how-gaming-is-helping-terrorist-groups-radicalize-and-recruit-a-generation-of-online-gamers

Crider, J.(2023). FBI Director Says Self-Driving Cars Could Era in New Terror Attack Opportunities. Teslarati .Available at: https://www.teslarati.com/fbi-director-self-driving-terrorism/

Danylov, O. (2022) The Danish police created the Police Online Patrol, which plays games with young people. Mezha. Available at:https://mezha.media/en/2022/12/19/the-danish-police-created-the-police-online-patrol-which-plays-games-with-young-people/

Dass, R. (2023). The Evolving Threat from Terrorist Drones in Africa. The Lawfare Institute. .Available at:https://www.lawfaremedia.org/article/the-evolving-threat-from-terrorist-drones-in-africa

Department of Justice.)2020(.Global Disruption of Three Terror Finance Cyber-Enabled Campaigns. Available at:https://www.justice.gov/archives/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns

Entenmann,E, Berg,W.(2018). Terrorist Financing and Virtual Currencies: Different Sides of the Same Bitcoin?. The International Centre for Counter-Terrorism (ICCT). Available at: https://icct.nl/publication/terror-

Nelson, R. R., & Winter, S. G. (1982). An Evolutionary Theory of Economic Change. Harvard University Press, 99-112,341-348. Available at: https://inctpped.ie.ufrj.br/spiderweb/pdf_2/Dosi_1_An_evolutionary-theory-of_economic_change..pdf

Ogele, E. (2024) .Terrorist financing in the digital Age: An Analysis of Crypto Currencies and online Crowd Funding. Journal of Terrorism Studies. 6(2). Available at:https://scholarhub.ui.ac.id/cgi/viewcontent.cgi?article=1121&context=jts

Rasler,D.(2018).The Islamic State and Drones: Supply, Scale, and Future Treats. Combating Terrorism Center at West Point .Available at:https://ctc.westpoint.edu/wp-content/uploads/2018/07/Islamic-State-and-Drones-Release-Version.pdf

Roul, A. (2024).The Rise of Monero: ISKP's Preferred Cryptocurrency for Terror Financing. The Global Network on Extremism and Technology. Available at:https://gnet-research.org/2024/10/04/the-rise-of-monero-iskps-preferred-cryptocurrency-for-terror-financing/

Schaer, C.(2024). How extremist groups like 'Islamic State' are using AI.Dw. Available at:https://www.dw.com/en/how-extremist-groups-like-islamic-state-are-using-ai/a-69609398

Siegel, D. (2024).AI Jihad: Deciphering Hamas, Al-Qaeda and Islamic State's Generative AI Digital Arsenal. Global Network on Extremism & Technology. Available at:https://gnet-research.org/2024/02/19/ai-jihad-deciphering-hamas-al-qaeda-and-islamic-states-generative-ai-digital-arsenal/

18 (1). 132-143. Available at:https://www.jstor.org/stable/27301123

IDC. (2025).Worldwide Security Spending to Increase by 12.2% in 2025 as Global Cyber threats Rise, Says IDC. Available at:https://www.idc.com/getdoc.jsp?containerId=prEUR253264525

Kenney, M. (2008). Organizational Learning and Islamic Militancy. American Journal of Sociology .Available at: https://www.researchgate.net/publication/279886521_Organizational_Learning_and_Islamic_Militancy

Malik, N. (2018). Terror in the Dark: How Terrorists use Encryption, the Darknet and Cryptocurrencies. Henry Jackson Society. Available at:http://henryjacksonsociety.org/wp-content/uploads/2018/04/Terror-in-the-Dark.pdf

Mappaselleng, N, Kadir, N, Ahmad& A, Kadir, Z. (2025) .Beyond the Surface: Exploring the Next Level of Terrorism on the Dark Web. Jambura Law Review, 7)1(. 309-335. Available at:https://ejurnal.ung.ac.id/index.php/jalrev/article/viewFile/26150/10332

Mathur, P, Broekaert, C & Clarke, C.(2024).The Radicalization (and Counter-radicalization) Potential of Artificial Intelligence, The International Centre for Counter Terrorism. Available at:https://www.icct.nl/publication/radicalization-and-counter-radicalization-potential-artificial-intelligence

National Research Council. (1994) .Dual-Use Technologies and Export Control in the Post-Cold War Era. The National Academies Press, 1-2, 111-114. Available at:https://nap.nationalacademies.org/download/2270#

rorism/sites/www.un.org.counterterrorism/files/dw_beneath_the_surface_update.pdf

United Nations Security Council. (February 2023). Thirty-first report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to resolution 2610 (2021) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities. Paragraphs 21. Available at: https://docs.un.org/en/S/2023/95

United Nations Security Council. (January 2019). Twenty-third report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to resolution 2368 (2017) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities, .Paragraph 91. Available at:https://docs.un.org/en/S/2019/50

United Nations Security Council. (July 2024). Thirty-fourth report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to resolution 2734 (2024) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities. Paragraph 116. Available at: https://docs.un.org/en/S/2024/556

TrendMicro. (2015). ISIS Sympathizers Defacing and Exploiting WordPress Sites, FBI Warns .Available at:https://www.trendmicro.com/vinfo/tr/security/news/cyber-attacks/isis-sympathizers-defacing-and-exploiting-wordpress-sites-fbi-warns

U.S. Department of Justice (2016).ISIL-Linked Kosovo Hacker sentenced to 20 Years in Prison. .Available at:https://www.justice.gov/archives/opa/pr/isil-linked-kosovo-hacker-sentenced-20-years-prison

United Nations Office of Counter-Terrorism. (2021).Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes. 27-31, 33. Available at:https://unicri.org/sites/default/files/2021-06/Malicious%20Use%20of%20AI%20-%20UNCCT-UNICRI%20ReportWeb.pdf

United Nations Office of Counter-Terrorism. (2024). Beneath the surface: terrorist and violent extremist use of the dark web and cybercrime-as-a-service for cyber-attacks.33-39. Available at: https://www.un.org/counterter-

Received 06 Apr. 2025; Accepted 15 May 2025; Available online 24 Sep. 2025

Security Research Center
Naif Arab University for Security Sciences
Riyadh, Saudi Arabia

مركز البحوث الأمنية
جامعة نايف العربية للعلوم الأمنية
الرياض، المملكة العربية السعودية

Keywords:
security studies, malicious innovation, artificial intelligence, virtual currencies, dark web

الكلمات المفتاحية:
الدراسات الأمنية، الابتكار الخبيث، الذكاء الاصطناعي، العملات الافتراضية، الشبكة مظلمة.

Production and hosting by NAUSS

Email: srcenter@nauss.edu.sa
doi: 10.26735/WMOT9791