On Research Center
for Scientific Research
& Consultations

مركز أون ريسيرش
للبحوث العلمية
والاستشارات

تحولات الإرهاب المعاصر: تقييم الأداء الاستراتيجي للتنظيمات الإرهابية في ظل السيولة الدولية والثورة الرقمية

إعداد فريق عمل المركز

كراسات استراتيجية

أبريل ٢٠٢٦

مركز أون ريسيرش للبحوث العلمية والاستشارات

القاهرة – جمهورية مصر العربية

On Research Center for Scientific Research & Consultations

Cairo, Arab Republic of Egypt

Web: https://onresearch.org/

Email: info@onresearch.org

أبريل ٢٠٢٦

كراسات استراتيجية

مركز أون ريسيرش للبحوث العلمية والاستشارات

تحولات الإرهاب المعاصر: تقييم الأداء الاستراتيجي للتنظيمات الإرهابية في ظل السيولة الدولية والثورة الرقمية

إعداد

فريق عمل المركز

تصميم فنى - د – فاطمة مصطفى

تدقيق لغوي : أ- أحمد شعبان

الفهرس

ملخص الدراسة

تبحث هذه الدراسة في ديناميكيات التحول الهيكلي والوظيفي للتنظيمات الإرهابية في العقد الحالي، مع التركيز على تقييم كفاءتها في استغلال البيئة الدولية المضطربة. تستخدم الدراسة منهجاً تحليلياً لرصد كيفية انتقال التنظيمات من السيطرة الجغرافية إلى الانتشار الشبكي والافتراضي. وتوصلت النتائج إلى أن انشغال القوى الكبرى بالصراعات الجيوسياسية المباشرة قد أضعف جهة مكافحة الإرهاب الدولية، مما سمح لهذه التنظيمات بتطوير تكتيكات "هجينة" تدمج بين العنف المسلح والتوظيف التقني المتقدم.

الكلمات المفتاحية : التنظيمات الإرهابية - الصراع الجيوسياسي - التكتيكات الهجينة - السيولة الدولية - الإرهاب السيبراني- التقييم الاستراتيجي.

Abstract

This study explores the dynamics of structural and functional transformation within terrorist organizations over the current decade, focusing on evaluating their efficiency in exploiting the turbulent international environment. The study employs an analytical approach to monitor how these organizations have transitioned from territorial control to networked and virtual proliferation. The findings indicate that the preoccupation of great powers with direct geopolitical conflicts has weakened the international counter-terrorism front, thereby allowing these organizations to develop "hybrid" tactics that integrate armed violence with advanced technical applications.

Keywords

Terrorist Organization - Structural Transformation - Geopolitical Conflict - Hybrid Tactics - International Liquidity - Cyber-Terrorism - Strategic Evaluation .

المقدمة

لم تعد ظاهرة الإرهاب الدولي المعاصر مجرد انفعال عنيف أو فعل عشوائي عابر للحدود، بل تطورت لتصبح **استراتيجية جيوسياسية معقدة** تدار بعقلية مؤسسية تتقاطع فيها الحسابات السياسية الدولية بالقدرات التقنية الفائقة. إن المشهد العالمي الراهن يشهد حالة من **"السيولة الاستراتيجية"** الناتجة عن احتدام التنافس بين الأقطاب الكبرى على قيادة النظام الدولي، وهو ما أدى بدوره إلى تراجع التنسيق الأمني العالمي وتهميش ملف مكافحة الإرهاب لصالح صراعات القوى العظمى. هذا الارتباك في أولويات الأمن الدولي خلق "فجوات سيادية" مكنت التنظيمات الإرهابية من إعادة إنتاج ذاتها داخل بيئات حاضنة جديدة، مستغلةً تآكل سلطة الدولة الوطنية في مناطق التماس الملتهبة.

وعلاوة على ذلك، فإن هذه التنظيمات لم تكتفِ باستغلال الهشاشة السياسية، بل انخرطت في **"ثورة تكتيكية"** موازية للثورة الرقمية؛ حيث انتقلت من أساليب المواجهة التقليدية إلى نمط **"الإرهاب الهجين"** الذي يمزج بين العنف المادي المسلح والعمليات السيبرانية الممنهجة. إن قدرة هذه التنظيمات على تطويع تقنيات الذكاء الاصطناعي، والعملات المشفرة، والدرونات، قد منحتها "أدوات سيادية" كانت في السابق حكراً على الجيوش النظامية، مما أدى إلى تآكل احتكار الدول للقوة وتصاعد وتيرة التهديدات غير المتماثلة.

بناءً على هذا الواقع، تسعى هذه الدراسة إلى تقديم تقييم شامل ومعمق للأداء الاستراتيجي لهذه التنظيمات، عبر تشريح قدرتها الفائقة على **التكيف الهيكلي** من النماذج الهرمية إلى الشبكات العنقودية الافتراضية، وتحليل آليات استغلالها للثغرات القانونية والأمنية في النظام الدولي الراهن. كما تركز الدراسة على تتبع مسارات التطور في تكتيكاتها العملياتية التي باتت تعتمد على "عولمة التهديد" و"لامركزية التنفيذ"، مستهدفةً بذلك تقويض الاستقرار القومي للدول من خلال ضرب مرافقها الحيوية وشل قدراتها الإدراكية عبر الفضاء السيبراني. إن الهدف الأسمى لهذا البحث هو رسم خارطة طريق منهجية تفكك شيفرات الأداء الإرهابي الحديث، بما يساهم في صياغة استراتيجيات مواجهة استباقية قادرة على تحييد مخاطر هذا "العدو الرقمي" في ظل عالم يموج بالتحولات الكبرى.

أولاً: إشكالية الدراسة

تكمن إشكالية الدراسة في الفجوة المتزايدة بين آليات مكافحة الإرهاب التقليدية التي تتبعها الدول، وبين التطور النوعي والسيولة الهيكلية التي أظهرتها التنظيمات الإرهابية في العقد الحالي. فبينما يركز النظام الدولي على صراعات القوى العظمى(Great Power Competition) ، نجحت التنظيمات في إعادة تموضعها استراتيجياً مستغلةً "الفراغات الأمنية" والتحول الرقمي الهائل.

وتتبلور المشكلة في تساؤل رئيسي حول :**مدى كفاءة الأداء الاستراتيجي للتنظيمات الإرهابية في تحويل التحديات الجيوسياسية والتقنية الراهنة إلى فرص لتعزيز بقائها وتأثيرها العملياتي؟**

ثانياً: تساؤلات الدراسة

تسعى الدراسة للإجابة على التساؤلات الفرعية التالية:

1. كيف ساهمت حالة الاستقطاب الدولي الراهنة وانشغال القوى الكبرى في خلق بيئة محفزة لنمو التنظيمات الإرهابية؟
2. ما هي طبيعة التحول في الهيكل التنظيمي من "المركزية الجغرافية" إلى "اللامركزية الشبكية والافتراضية"؟
3. إلى أي مدى نجحت التنظيمات الإرهابية في دمج تقنيات الثورة الرقمية (الذكاء الاصطناعي، والعملات المشفرة، والدرونات) ضمن عقيدتها القتالية؟
4. ما هي الملامح المستقبلية لتهديدات "الإرهاب الهجين" في ظل استمرار السيولة الدولية؟

ثالثاً: منهجية الدراسة

اعتمدت الدراسة على تكامل منهجي يجمع بين:

- **منهج تحليل النظم** :لفهم التنظيمات الإرهابية كمدخلات مثل (موارد، تكنولوجيا) وعمليات (تكتيكات) ومخرجات مثل (عمليات ميدانية) ضمن بيئة دولية مضطربة.

- **المنهج المقارن: وذلك** للمقارنة بين أداء التنظيمات في مرحلة "التمكين المكاني" داخل (الدولة) ومرحلة "الانتشار الشبكي" فيما عرف ب (ما بعد الخلافة الجغرافية).(Clarke, 2019)
- **أداة الاستشراف المستقبلي :** لتحليل مسارات التهديد القادمة بناءً على المعطيات التقنية والجيوسياسية الراهنة.

رابعاً: الإطار المفاهيمي

1- مفهوم الأداء الاستراتيجي : ويُقصد به قدرة التنظيم على المواءمة بين وسائله المحدودة وأهدافه الكبرى عبر الابتكار التكتيكي، وضمان ديمومة التدفقات المالية والبشرية رغم الضغوط الأمنية (Hoffman, 2017).

2- مفهوم السيولة الدولية : ويُشير هنا إلى حالة عدم الاستقرار في التحالفات الدولية وتراجع التوافق حول معايير الأمن العالمي، مما يؤدي إلى نشوء "مناطق رمادية" تفتقر للسيادة الأمنية الفعالة (Zimmerman, 2022).

3- مفهوم الإرهاب الهجين : ويُعرف بأنه النمط الذي يدمج بين العنف المسلح التقليدي، والعمليات السيبرانية، والحروب النفسية المعتمدة على الذكاء الاصطناعي، لخلق حالة من الارتباك الشامل لدى الدولة المستهدفة.(UNCCT, 2023)

خامساً: الإطار النظري (نظرية التكيف التنظيمي):

تستند الدراسة إلى "نظرية التكيف التنظيمي(Organizational Adaptation Theory) "، التي تفسر كيف تغير الجماعات العنيفة من سلوكها وبنيتها استجابةً للضغوط الخارجية. فالتنظيمات الإرهابية تعمل ك "كائنات حية سياسية" تمارس "الانتخاب الطبيعي التقني"؛ حيث تبقى التنظيمات الأكثر قدرة على دمج التكنولوجيا الرقمية في هيكلها.(Cronin, 2020)

سادساً - تقسيم الدراسة : تقسم الدراسة إلى ثلاثة مباحث :

المبحث الأول بعنوان : **الكفاءة العملياتية والتكيف الهيكلي في بيئة دولية مضطربة**

المبحث الثانى بعنوان : **التطور التقني والسيبراني وتكتيكات "الحروب الهجينة"**

المبحث الثالث بعنوان : **الاقتصاد الرقمي والتمويل غير التقليدي (آليات استدامة الإرهاب)**

المبحث الأول

الكفاءة العملياتية والتكيف الهيكلي في بيئة دولية مضطربة

يُمثل الأداء العملياتي للتنظيمات الإرهابية في الوقت الراهن انعكاساً مباشراً لقدرتها على قراءة التحولات الجيوسياسية العالمية. فلم يعد النشاط الإرهابي مجرد رد فعل عشوائي، بل اتبع استراتيجية تعتمد على "المرونة الهيكلية" و"الانتشار الشبكي" لتجاوز آليات المكافحة الدولية التي أصابها الارتباك نتيجة صراع القوى الكبرى.

أولاً-استغلال السيولة الجيوسياسية وصراع القوى العظمى

تعتمد التنظيمات الإرهابية في بقائها وتمددها على استغلال ما يُسمى "المناطق الرمادية" في العلاقات الدولية.حيث إن تطور الأوضاع الراهنة أدى إلى تحول جذري في أولويات الأمن العالمي، وهو ما يمكن تفصيله في النقاط التالية:

1- تراجع التعاون الأمني الدولي وفجوة المعلومات :تاريخياً، كان التنسيق الاستخباراتي بين القوى العظمى (خاصة الولايات المتحدة وروسيا) يمثل حجر الزاوية في محاصرة التنظيمات العابرة للحدود. إلا أن احتدام الصراع في أوكرانيا وتصاعد التوترات في شرق آسيا أدى إلى تجميد قنوات تبادل المعلومات (Hoffman, 2017). هذا "العمى الاستخباراتي" المتبادل منح التنظيمات فرصة ذهبية للتحرك في المساحات غير المراقبة، حيث تراجعت عمليات الرصد المشتركة للتمويل والتحركات البشرية عبر القارات (Zimmerman, 2022).

2-استراتيجية "الاستثمار في الفوضى" ونشوء الملاذات الجيوسياسية :لم تعد الملاذات الآمنة مجرد جغرافيا وعرة، بل أصبحت "سياسية" بامتياز. في مناطق مثل الساحل الأفريقي وسوريا واليمن، تداخلت أنشطة الجماعات الإرهابية مع حروب الوكالة بين القوى الإقليمية والدولية. فالتقييم العملياتي يشير إلى أن التنظيمات باتت توظف "عدم الاستقرار" لترسيخ نفوذها، حيث تستفيد من غياب سيادة الدولة

لتقديم نفسها كبديل إداري وأمني محلي، مستغلةً تضارب مصالح الدول الكبرى التي باتت تضع مكافحة الإرهاب في مرتبة ثانوية بعد صراع النفوذ.(Clarke, 2019)

ثانيًا - التحول الهيكلي نحو "اللامركزية الشبكية"

أدركت التنظيمات الإرهابية أن الهياكل التنظيمية المركزية (Hierarchical Structures) تجعلها صيداً سهلاً للضربات الجوية وعمليات الاغتيال الممنهجة، مما دفعها نحو تبني نماذج أكثر مرونةعلى النحو التالي:

1- نموذج "الشبكة العنقودية (Cluster Network): "انتقل الأداء التنظيمي من "القيادة والسيطرة المركزية" إلى نظام الفروع المستقلة أو ما يعرف بـ "اللامركزية الاستراتيجية". في هذا النموذج، تعمل الفروع الإقليمية (مثل تنظيم داعش في غرب أفريقيا أو ولاية خراسان) كمؤسسات شبه مستقلة تمتلك مواردها المالية الخاصة وخططها الميدانية بمعزل عن "المركز .(Crenshaw, 2011) "هذا التحول يضمن أن القضاء على القيادة العليا لا يعني انهيار التنظيم، بل تتحول الفروع إلى مراكز قوة جديدة قادرة على المبادرة (UN Security Council, 2022).

2- تصاعد ظاهرة "الإرهاب بلا قيادة :(Leaderless Terrorism) "يمثل هذا التكتيك الذروة في التكيف الهيكلي؛ حيث يتم تحويل الأيديولوجيا إلى "منتج استهلاكي" عبر الفضاء السيبراني. يعتمد الأداء هنا على "الذئاب المنفردة" الذين يتلقون الإلهام والتدريب عبر المنصات المشفرة دون وجود ارتباط تنظيمي مادي. هذا النمط من العمليات يتميز بـ "البصمة الأمنية المنخفضة(Low Signature) "، مما يجعل من المستحيل على أجهزة الاستخبارات التنبؤ بها عبر تتبع الهياكل التنظيمية التقليدية.(Simon, 2016)

ثالثًا-"الخلافة الرقمية" وإدارة السيادة الافتراضية

مع فقدان السيطرة المكانية على الأرض (كما حدث لداعش في العراق وسوريا)، برز تحول نحو "التمكين الافتراضي" كآلية للتعويض عن الهزيمة العسكريةكانت ملامحه على النحو التالي:

1-تشييد الملاذات الآمنة في الويب المظلم :(Dark Web) نجحت التنظيمات في نقل "أرشيفها" وقواعد بياناتها ومنصات تدريبها إلى فضاءات رقمية لامركزية. وفي التقييم الحديث يثبت أن هذه التنظيمات تدير الآن "مجتمعات افتراضية" متكاملة توفر التعليمات اللوجستية، وصناعة المتفجرات، وتنسيق الهجمات عبر قنوات مشفرة تتجاوز قدرات الرقابة التقنية للدول.(Weimann, 2015)

2-احترافية "الجيوش التقنية" وتوظيف الكوادر النوعية :شهد أداء التنظيمات تحولاً من استقطاب "المقاتلين التقليديين" إلى التركيز على "المقاتلين الرقميين"،حيث يتم تقييم أداء التنظيم اليوم بناءً على قدرته على تجنيد مهندسي البرمجيات، وخبراء الأمن السيبراني، ومنتجي المحتوى الإعلامي المحترفين. هؤلاء الكوادر لا يشاركون في القتال الميداني، بل يديرون "جبهة الوعي" ويوفرون الحماية التقنية لاتصالات التنظيم، مما يمنحه تفوقاً في حرب المعلومات.(Cronin, 2020) .

رابعًا : المرونة الجغرافية والقدرة على إعادة التموضع

تتميز التنظيمات الإرهابية المعاصرة بـ "سرعة التكيف الجغرافي"؛ فبمجرد زيادة الضغط العسكري في إقليم ما، تبدأ عمليات "النزوح الاستراتيجي" نحو أقاليم أخرى تعاني من هشاشة أمنية:

- **الهجرة نحو القارة الأفريقية :**يوضح تحليل المسار العملياتي أن الثقل الاستراتيجي للتنظيمات قد انتقل بشكل ملحوظ نحو منطقة الساحل وجنوب الصحراء. هذا الانتقال لم يكن عشوائياً، بل جاء نتيجة تقييم دقيق لضعف الجيوش الوطنية في تلك المناطق وتصاعد النزاعات العرقية والمجتمعية التي توفر بيئة تجنيد مثالية.(International Crisis Group, 2021)
- **تكتيك "الكمون والظهور :"**تتبنى التنظيمات تكتيكات تسمح لخلاياها بالذوبان في المجتمعات المحلية عند اشتداد الحملات الأمنية، مع الحفاظ على "جاهزية الاستدعاء" للقيام بعمليات خاطفة عند حدوث أي ثغرة أمنية أو سياسية.(Clarke, 2019) .

المبحث الثاني

التطور التقني والسيبراني وتكتيكات "الحروب الهجينة"

يُمثل التطور التقني المتسارع في العقد الثالث من القرن الحادي والعشرين "مضاعف قوة (Force Multiplier) " غير مسبوق للتنظيمات الإرهابية، حيث أدى اندماج التكنولوجيا الرقمية بالعمل العسكري التقليدي إلى ظهور ما يُعرف بـ "الإرهاب الهجين". هذا النمط من العمليات يتجاوز القيود الجغرافية والزمنية، ويسمح لتنظيمات محدودة الموارد بشن هجمات ذات أثر استراتيجي واسع النطاق، مستغلةً العولمة الرقمية وسهولة الوصول إلى التقنيات المزدوجة الاستخدام التي كانت في السابق حكراً على الجيوش النظامية والمؤسسات الاستخباراتية للدول الكبرى.

أولاً: توظيف الذكاء الاصطناعي وتقنيات التزييف العميق في هندسة الإدراك : لم يعد استخدام الذكاء الاصطناعي (AI) مجرد أداة ثانوية، بل اعتبرت "العقل المدبر" للآلة الدعائية والتجنيدية للتنظيمات الإرهابية،حيث يتم تقييم أداء هذه التنظيمات اليوم من خلال قدرتها على توظيف خوارزميات تعلم الآلة لتحليل كميات ضخمة من البيانات السلوكي لمستخدمي الإنترنت؛ حيث تتيح هذه التقنيات للتنظيم تحديد "الفئات الهشة" والشباب الأكثر عرضة للراديكالية بناءً على اهتماماتهم، ومواقعهم الجغرافية، وتفاعلاتهم الرقمية. وهذا الاستهداف المجهري يرفع من كفاءة التجنيد بشكل غير مسبوق (UNCCT, 2023).

علاوة على ذلك، برز خطر "التزييف العميق" كأخطر أداة في "الحروب الإدراكية"؛ إذ يمكن للتنظيمات الآن إنتاج مقاطع فيديو وصور مزيفة بجودة سينمائية لقادة سياسيين أو عسكريين، بهدف بث الرعب، أو التحريض على انقلابات عسكرية، أو تضليل الرأي العام في أوقات الأزمات الراهنة. لذلك إن القدرة على تزييف "الحقيقة" تؤدي إلى تقويض شرعية الدول وهدم "العقد الاجتماعي" من خلال نشر معلومات مضللة لا يمكن للمواطن العادي تمييزها، مما يمهد الطريق لفوضى اجتماعية تسهل تنفيذ العمليات الإرهابية الميدانية.(Cronin, 2020)

ثانياً: سلاح الطائرات بدون طيار (الدرونات) وتحطيم احتكار القوة الجوية: شهد الأداء الميداني للتنظيمات الإرهابية ثورة تكتيكية من خلال الاستخدام المكثف للطائرات المسيرة(UAVs) ، والتي أصبحت تُعرف بـ "القوة الجوية للفقراء". حيث نجحت هذه التنظيمات في تحويل الدرونات التجارية البسيطة إلى أسلحة هجومية فتاكة عبر تزويدها بآليات لإسقاط القنابل أو تحويلها إلى طائرات "كاميكازي" انتحارية. فهذا التطور كسر التفوق الجوي التقليدي للدول؛ إذ لم تعد الجيوش النظامية بمأمن داخل قواعدها المحصنة.(Rassler, 2018)

إن تقييم الأداء في صراعات الشرق الأوسط وأفريقيا يظهر أن الدرونات لم تعد تُستخدم للاستطلاع فقط، بل لشن هجمات منسقة تهدف لإغراق أنظمة الدفاع الجوي وتدمير البنى التحتية النفطية، والمطارات، ومحطات الكهرباء. فانخفاض تكلفة هذه التقنية وسهولة الحصول على قطع غيارها عبر الأسواق الإلكترونية العالمية جعل من الصعب السيطرة على انتشارها، مما وضع الأمن القومي للدول أمام تحدٍ وجودي يتمثل في مواجهة "عدو طائر" رخيص التكلفة ولكنه عالي الأثر التدميري.(Don Rassler, 2018)

ثالثاً: الهجمات السيبرانية الاستراتيجية وشلل المرافق الوطنية الحيوية: انتقلت الجريمة الإرهابية في الفضاء الرقمي من مجرد "اختراق المواقع" إلى "الإرهاب السيبراني الصلب" الذي يستهدف تدمير المكونات

المادية للدولة، حيث تشير التقارير الأمنية إلى سعي التنظيمات لامتلاك أو شراء برمجيات خبيثة متطورة قادرة على اختراق أنظمة التحكم الصناعي (SCADA) التي تدير سدود المياه، والمفاعلات النووية، وشبكات توزيع الغاز.(Weimann, 2015) ، حيث أن خطر "التخريب الرقمي" يكمن في قدرته على إحداث انفجارات مادية أو تسميم مصادر المياه أو شل حركة الملاحة الجوية دون ترك بصمة مادية واضحة للمهاجم.

كما برز تكتيك "برمجيات الفدية كخدمة(RaaS) "، حيث تقوم التنظيمات باحتجاز السجلات الطبية للمستشفيات أو البيانات المالية للبنوك المركزية، ليس فقط لتحصيل الأموال بالعملات المشفرة، بل لإثارة السخط الشعبي ضد الحكومات وإظهارها بمظهر العاجز عن حماية الخصوصية والأمن القومي.و هذا النوع من الهجمات يمثل "حرب استنزاف رقمية" تهدف لنشر الذعر وشل عجلة الاقتصاد الوطني (Liska & Gallo, 2016).

رابعاً: التمويل الرقمي اللامركزي وتجاوز المنظومات الرقابية الدولية :أحدثت تكنولوجيا "البلوكشين " (Blockchain)تحولاً راديكالياً في البنية المالية للإرهاب، حيث وفرت العملات المشفرة (Cryptocurrencies)مثل (Monero) و (Zcash)التي تتميز بخصوصية مطلقة، قنوات تمويل دولية عصية على التتبع من قبل مؤسسات مثل: (FATF) هذا الانتقال نحو "التمويل السيبراني" سمح للتنظيمات بتجاوز نظام (SWIFT) والعقوبات المصرفية الدولية، مما منحها تدفقات مالية مستدامة لدعم العمليات في قارات مختلفة في آن واحد.(FATF, 2020)

إن استخدام "العملات المستقرة (Stablecoins) "مثل (USDT) المربوطة بالدولار قلل من مخاطر تذبذب القيمة، مما سمح للتنظيمات بتخزين ثرواتها في محافظ رقمية مشفرة واستخدامها لشراء الأسلحة والمعدات التقنية من "الويب المظلم .(Dark Web) "كما برزت ظاهرة "التبرعات المجتمعية الرقمية" عبر منصات التمويل الجماعي غير المراقبة، مما حول تمويل الإرهاب إلى نشاط لامركزي يصعب تجفيف منابعه بالوسائل التقليدية.(Clarke, 2019)

خامساً: الإعلام السيبراني والعمليات النفسية عبر الشبكات المشفرة: تطور الأداء الإعلامي للتنظيمات نحو بناء "جيوش إلكترونية" محترفة تدير منصات تواصل لامركزية (Decentralized Platforms) لا تخضع لرقابة الشركات التقنية الكبرى. كذلك استخدام تطبيقات مثل (Telegram) و (Element) و (Signal)وفر غطاءً آمناً لنقل التعليمات العملياتية وتدريب العناصر على "صناعة المتفجرات" عبر غرف دردشة مغلقة.(Singer & Brooking, 2018)

إن استراتيجية "الانتشار الفيروسي" للمحتوى تضمن وصول الفكر المتطرف إلى الملايين في ثوانٍ معدودة عبر شبكات "البوتات (Bots) "التي تعيد نشر الرسائل الدعائية بشكل آلي. هذا الأداء الإعلامي يهدف لكسر الروح المعنوية للخصوم وتجنيد "الذئاب المنفردة" الذين يتم تزويدهم بـ "أدلة تشغيلية" رقمية تتيح لهم تنفيذ هجمات معقدة بجهد فردي، مما يحول الفضاء الرقمي إلى ساحة معركة مفتوحة تتفوق فيها الرسالة الإرهابية أحياناً على الرواية الرسمية للدولة.(Simon, 2016)

المبحث الثالث

الاقتصاد الرقمي والتمويل غير التقليدي (آليات استدامة الإرهاب)

يُمثل التمويل "شريان الحياة" لأي تنظيم إرهابي، وبدونه تتحول الأيديولوجيا إلى مجرد شعارات عاجزة عن التنفيذ الميداني. ففي ظل التطورات الدولية الراهنة، شهدت الهياكل المالية للتنظيمات الإرهابية تحولاً جذرياً انتقل بها من الاعتماد على التبرعات التقليدية ونظام الحوالة الورقية إلى الانخراط الكامل في "الاقتصاد الرقمي الموازي". هذا التحول لم يكن مجرد استجابة لضغوط الرقابة المالية الدولية، بل كان سعياً نحو امتلاك منظومات مالية لامركزية تمنح التنظيمات استقلالية سيادية بعيداً عن سيطرة الدول والنظام المصرفي العالمي الموحد.

أولاً: الانتقال الاستراتيجي نحو العملات المشفرة(Cryptocurrencies) : أحدثت تكنولوجيا السجلات الموزعة (Blockchain) ثورة في الأداء المالي للتنظيمات الإرهابية، حيث وفرت العملات الرقمية بيئة مثالية لنقل الثروات العابرة للحدود في ثوانٍ معدودة وبخصوصية شبه مطلقة. يتم تقييم الأداء المالي الحديث للتنظيمات من خلال قدرتها على توظيف "عملات الخصوصية (Privacy Coins) "مثل (Monero) و(Zcash)، والتي تختلف عن البتكوين في كونها تستخدم تقنيات إخفاء الهوية التي تجعل من المستحيل على المحللين الماليين تتبع مسار المعاملات أو تحديد هوية المرسل والمستقبل.(FATF, 2020)

إن هذا النزوح نحو "التشفير المالي" سمح للتنظيمات بتجاوز نظام (SWIFT) والعقوبات التي تفرضها وزارة الخزانة الأمريكية ومجلس الأمن الدولي. فلم يعد التمويل يتطلب حقائب من النقود السائلة، بل أصبح يُدار عبر "محافظ رقمية" يمكن حملها على شريحة ذاكرة صغيرة أو تخزينها في السحابة الإلكترونية. هذا التطور أدى إلى فشل الاستراتيجيات التقليدية لمكافحة غسل الأموال(AML) ، حيث باتت التنظيمات

تمتلك قنوات تمويل مستدامة تتدفق من المتبرعين في مختلف القارات مباشرة إلى الميدان دون المرور بأي وسيط مصرفي خاضع للرقابة.(Clarke, 2019)

ثانياً: العملات المستقرة (Stablecoins) وإدارة الأصول القومية للتنظيم :لعل أبرز التحولات في أداء التنظيمات هو الاعتماد المتزايد على "العملات الرقمية المستقرة" مثل :(Tether - USDT) تاريخياً، كانت التنظيمات تخشى تقلبات أسعار البتكوين، لكن العملات المستقرة المربوطة بالدولار وفرت لها أداة لتخزين القيمة وإدارة ميزانياتها الضخمة دون مخاطر الانهيار السعري. فالتقييم الميداني يشير إلى أن التنظيمات الإقليمية (خاصة في الساحل الأفريقي والشرق الأوسط) باتت تستخدم هذه العملات لدفع رواتب المقاتلين، وشراء المعدات العسكرية من تجار السلاح في الويب المظلم، وتمويل الخدمات الاجتماعية لكسب الحواضن الشعبية.(UN Security Council, 2022)

إن استخدام (USDT) تحديداً وفر للتنظيمات "دولاراً رقمياً" يمكن تداوله في الأسواق السوداء العالمية بيسر وسهولة. هذا الأداء المالي الاحترافي مكن التنظيمات من بناء "اقتصاد سيادي" موازٍ، حيث يتم تحويل عائدات الأنشطة الإجرامية (مثل التهريب والضرائب غير القانونية) إلى أصول رقمية مستقرة يصعب تجميدها أو مصادرتها، مما يمنح التنظيم قدرة عالية على الصمود الطويل الأمد حتى في ظل الحصار الاقتصادي الخانق.(Clarke, 2019)

ثالثاً: الويب المظلم (Dark Web) كمنصة للتجارة غير المشروعة :تحول "الويب المظلم" إلى المركز التجاري الرئيسي للتنظيمات الإرهابية، حيث يتم توظيفه لربط العرض بطلب العمليات الإرهابية. في هذه الأسواق الخفية، يتم تقييم الأداء اللوجستي للتنظيم بناءً على قدرته على تأمين الأسلحة المتطورة، والوثائق المزورة (جوازات سفر وهويات)، والمواد الكيميائية اللازمة لصناعة المتفجرات، حيث أن "التشفير المزدوج" والمواقع التي تنتهي بلاحقة (onion.) توفر غطاءً يحمي المتعاملين من الاختراق الاستخباراتي (Weimann, 2015).

علاوة على ذلك، برز تكتيك "غسيل الأموال السيبراني" عبر منصات الألعاب الإلكترونية وتجارة .(NFTs) فتقوم التنظيمات بشراء أصول رقمية داخل الألعاب أو رموز غير قابلة للاستبدال بأموال غير مشروعة، ثم إعادة بيعها لتحويلها إلى "أموال نظيفة" يمكن سحبها في أي مكان في العالم. هذا الابتكار في غسيل

الأموال يعكس مدى تطور "العقلية المالية" للتنظيمات الإرهابية التي باتت تسبق التشريعات القانونية الدولية بخطوات عديدة، مما يجعل من الفضاء الرقمي "جنة مالية" للفاعلين من غير الدول (Cronin, 2020).

رابعاً: استغلال منصات التمويل الجماعي (Crowdfunding) والعمل الخيري الرقمي: تطورت آليات جمع التبرعات من "صناديق المساجد" إلى "حملات التمويل الجماعي" الرقمية واسعة النطاق، حيث تستغل التنظيمات منصات التواصل الاجتماعي لإطلاق حملات تحت غطاء "إنساني" أو "إغاثي"، كذلك يتم استقبال التبرعات عبر روابط دفع إلكترونية أو عناوين محافظ رقمية. هذا الأداء الدعائي المالي يعتمد على "التضليل العاطفي" لجذب المتبرعين من مختلف أنحاء العالم، مما يصعب على الأجهزة الأمنية التمييز بين العمل الخيري الحقيقي والتمويل المستتر للإرهاب.(Singer & Brooking, 2018)

إن هذه الحملات لا تهدف فقط لجمع المال، بل لـ "تسييس المانحين" وخلق ارتباط معنوي بين المتبرع والتنظيم. فيتم استخدام تقنيات "الخلاطات المخططة (Mixing Services) "لتشتيت مسار التبرعات الصغيرة ودمجها في مبالغ كبيرة يصعب تعقب مصدرها الأصلي،هذا النمط من التمويل اللامركزي (Decentralized Finance)حول كل فرد يمتلك هاتفاً ذكياً إلى "مانح محتمل"، مما يوسع قاعدة التمويل لتشمل آلاف الأفراد بدلاً من الاعتماد على ممولين كبار يسهل رصدهم.(FATF, 2020)

خامساً: اقتصاد الموارد المحلية والاندماج في شبكات الجريمة المنظمة :لا ينفصل الأداء المالي الرقمي عن الواقع المادي على الأرض، حيث نجحت التنظيمات في دمج مواردها المحلية في الاقتصاد العالمي عبر "شبكات الجريمة المنظمة العابرة للحدود"، فيتم تقييم الأداء المالي من خلال قدرة التنظيم على السيطرة على موارد طبيعية (مثل الذهب في الساحل الأفريقي أو النفط سابقاً في العراق) وبيعها عبر وسطاء في الأسواق الدولية، ثم تحويل العوائد فوراً إلى عملات مشفرة لإخفاء منشئها.(Zimmerman, 2022)

إن هذا "التحالف الهجين" بين الإرهاب والجريمة المنظمة (مثل تجارة المخدرات والبشر) وفر للتنظيمات سيولة مالية ضخمة بعيداً عن أي رقابة دولية. فالتنظيم يعمل كـ "قوة حماية" لخطوط التهريب مقابل نسب مئوية من الأرباح، مما يخلق تداخلاً وظيفياً يجعل من الصعب مكافحة أحدهما دون الآخر.

هذا الاندماج في اقتصاد الظل يضمن استمرارية تدفق الأموال حتى في حال انقطاع التبرعات الخارجية، مما يجعل التنظيم الإرهابي "كياناً اقتصادياً" قادراً على تمويل حربه الطويلة ضد الدولة (Hoffman, 2017).

الخاتمة:

تُمثل هذه الدراسة محاولة لتفكيك الديناميكيات المعقدة التي تحكم أداء التنظيمات الإرهابية في ظل التحولات الجيوسياسية والتقنية الراهنة. إن الحقيقة الاستراتيجية التي تفرض نفسها اليوم هي أن الإرهاب لم يعد مجرد "عدو عابر للحدود"، بل استحال "منظومة هجينة" قادرة على التكيف مع أكثر البيئات ضغطاً. ومن خلال استعراض المباحث السابقة، يمكن بلورة النتائج والتوصيات النهائية على النحو التالي:

نتائج الدراسة :

أولاً-انتقال السيادة من "الجغرافيا" إلى "الفضاء السيبراني":

أثبتت النتائج أن فقدان التنظيمات الإرهابية لمناطق سيطرتها المادية لم يؤدِ إلى تلاشيها، بل دفعها نحو "النزوح الرقمي"، فلقد نجحت هذه التنظيمات في بناء "مجتمعات افتراضية" بديلة توفر كافة وظائف الدولة (تجنيد، تدريب، تمويل، إعلام) بعيداً عن الاستهداف العسكري التقليدي، هذا التحول جعل من الفضاء السيبراني "الملاذ الآمن المستدام" الذي يوفر حصانة تقنية ضد أدوات الردع التقليدية (Weimann, 2015).

ثانياً- الاستفادة من "فراغ القوة" في النظام الدولي :

كشف التقييم عن علاقة طردية بين احتدام الصراع بين القوى العظمى (الولايات المتحدة، وروسيا، والصين) وتنامي قدرات التنظيمات الإرهابية. حيث أن تراجع التنسيق الأمني الدولي نتيجة الاستقطاب الجيوسياسي الراهن قد منح الإرهاب انتعاش، حيث استغلت التنظيمات انشغال الجيوش النظامية بالحروب الكبرى لإعادة تموضعها في مناطق الهشاشة الأمنية، لا سيما في القارة الأفريقية ووسط آسيا (Zimmerman, 2022).

ثالثًا- ديمقراطية التكنولوجيا وتآكل احتكار القوة :

أدت "الثورة التقنية الرابعة" إلى نقل أسلحة استراتيجية (مثل الدرونات، والذكاء الاصطناعي، والتشفير المالي) من أيدي الدول إلى أيدي الفاعلين من غير الدول. إن استخدام التنظيمات للدرونات الرخيصة والعملات المشفرة قد كسر احتكار الدول للقوة الجوية والمالية، مما خلق حالة من "اللا تماثل الاستراتيجي" التي تسمح لمجموعات صغيرة بتهديد أمن دول عظمى بتكلفة لا تُذكر (Cronin, 2020).

التوصيات :

بناءً على ما تقدم، توصي الدراسة بتبني مقاربات أمنية وسياسية مبتكرة تتجاوز الأطر التقليدية على النحو التالي:

1. **صياغة "بروتوكول سيبراني دولي" موحد** :يجب على المجتمع الدولي تجاوز خلافاته الجيوسياسية الراهنة للاتفاق على معايير صارمة لتنظيم العملات المشفرة ومنع استخدامها في التمويل الإرهابي. التوصية هنا تذهب نحو تفعيل أنظمة رصد تعتمد على "البلوكشين التحليلي" لتتبع التدفقات المالية بالتعاون مع شركات التقنية الكبرى ومؤسسة(FATF) ، مع ضرورة تجريم "خلاطات العملات" التي تُستخدم لغسيل الأموال الإرهابية.
2. **تطوير أنظمة "الدفاع الجوي المصغر" والتصدي للدرونات** :نظراً لتصاعد خطر الطائرات بدون طيار، يتعين على الدول الاستثمار في تقنيات التشويش السيبراني والأسلحة الليزرية منخفضة التكلفة لحماية المنشآت الحيوية والتجمعات المدنية. لم يعد كافياً الاعتماد على صواريخ الدفاع الجوي التقليدية لمواجهة "أسراب الدرونات" الرخيصة، بل لا بد من حلول تكنولوجية موازية تعتمد على الذكاء الاصطناعي لرصد وتحييد الأهداف الصغيرة.
3. **تعزيز "الأمن الإدراكي" ومكافحة التزييف العميق** :يجب على الحكومات بناء استراتيجيات لـ "المناعة الرقمية" لدى المواطنين، تتضمن برامج وطنية لكشف المحتوى المزيف (Deepfakes) وتفنيد الدعاية الإرهابية في وقتها الحقيقي. إن المواجهة في الفضاء الرقمي تتطلب "رواية مضادة"

قوية تعتمد على الحقائق والشفافية لسد الفجوة التي تستغلها التنظيمات لنشر الإحباط وفقدان الثقة في مؤسسات الدولة.

4. **المقاربة التنموية في "مناطق التماس** :"تؤكد الدراسة أن المواجهة الأمنية وحدها لن تجتث الإرهاب ما لم يتم معالجة "الجذور الجيوسياسية" والهشاشة الاقتصادية في مناطق النزاع. فيجب تفعيل مشروعات تنموية حقيقية في مناطق مثل الساحل الأفريقي لسحب البساط من تحت أقدام التنظيمات التي تستغل الفقر والتهميش لتجنيد المقاتلين وبناء حواضن شعبية .

قائمة المراجع :

- **Clarke, C. P. (2019).** *After the Caliphate: The Islamic State and the Future Terrorist Diaspora*. Cambridge: Polity Press.
- **Crenshaw, M. (2011).** *Explaining Terrorism: Causes, Processes, and Consequences*. London: Routledge.
- **Cronin, A. K. (2020).** *Power to the People: How Open Technological Innovation is Arming Tomorrow's Terrorists*. Oxford: Oxford University Press.
- **FATF. (2020).** *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*. Financial Action Task Force.
- **Hoffman, B. (2017).** *Inside Terrorism* (3rd ed.). New York: Columbia University Press.
- **Hoffman, B., & Ware, J. (2024).** *God, Guns, and Sedition: Far-Right Terrorism in America*. New York: Columbia University Press.
- **International Crisis Group. (2021).** *The Sahel: What's at Stake?*, Africa Report No. 301.
- **Liska, A., & Gallo, T. (2016).** *Ransomware: Defending Against Digital Extortion*. Sebastopol, CA: O'Reilly Media.
- **Lynn III, W. J. (2010).** "Defending a New Domain: The Pentagon's Cyber Strategy," *Foreign Affairs*, Vol. 89, No. 5.
- **Rassler, D. (2018).** *The Islamic State and Drones: Global Capacities and Future Trajectories*. West Point: Combating Terrorism Center.
- **Schmitt, M. N. (Ed.). (2017).** *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press.
- **Simon, J. D. (2016).** *Lone Wolf Terrorism: Understanding the Growing Threat*. New York: Prometheus Books.
- **Singer, P. W., & Brooking, E. T. (2018).** *LikeWar: The Weaponization of Social Media*. New York: Eamon Dolan/Houghton Mifflin Harcourt.
- **Singer, P. W., & Friedman, A. (2014).** *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford: Oxford University Press.
- **UNCCT. (2023).** *The Use of Artificial Intelligence for Counter-Terrorism Purposes*. United Nations Counter-Terrorism Centre Publication.

- **UN Security Council. (2022).** *Thirtieth Report of the Analytical Support and Sanctions Monitoring Team*. UN Document S/2022/547.

- **Weimann, G. (2015).** *Terrorism in Cyberspace: The Next Generation*. New York: Columbia University Press.

- **Zetter, K. (2014).** *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown Publishing Group.

- **Zimmerman, K. (2022).** *Terrorism After the 2022 Invasion of Ukraine*. Washington, D.C.: American Enterprise Institute.