

CRIPTO ASSET E TERRORISMO

Il nuovo mezzo finanziario delle organizzazioni terroristiche

Sara Osimani



International Institute for Global Analyses

Vision & Global Trends. International Institute for Global Analyses
Piazza dei Navigatori 22, 00147 – Rome (Italy)

The views and opinions expressed in this publication are those of the authors and do not represent the views of the Vision & Global Trends. International Institute for Global Analyses unless explicitly stated otherwise.

© 2025 Vision & Global Trends - International Institute for Global Analyses
© 2025 Sara Osimani

First Edition: February 2025

Analytical Dossier 07/2025 - ISSN 2704-6419

www.vision-gt.eu
info@vision-gt.eu

CRIPTO ASSET E TERRORISMO

Il nuovo mezzo finanziario delle organizzazioni terroristiche

Sara Osimani



Vision & Global Trends - International Institute for Global Analyse

CRIPTO ASSET E TERRORISMO

Il nuovo mezzo finanziario delle organizzazioni terroristiche

Sara Osimani

Introduzione

Il denaro è sempre stato la pista principale da seguire nelle indagini sulle attività criminali, poiché queste, come qualsiasi altra attività, richiedono finanziamenti costanti.

Dalle valigette di soldi consegnate di mano in mano, al riciclaggio di denaro internazionale effettuato da membri della criminalità organizzata, ogni transazione lascia una traccia.

La tracciabilità dei finanziamenti è quindi uno dei modi più efficaci per riuscire a contrastare le vecchie e nuove minacce alla sicurezza nazionale.

Nel corso del tempo, sono stati sviluppati diversi stratagemmi per finanziare gli attori coinvolti in azioni criminali da parte di Stati sponsor o entità private, ma il cambiamento più importante degli ultimi anni e allo stesso tempo quello che rappresenta la sfida più grande per le forze dell'ordine è l'uso di cripto asset come metodo di finanziamento.

Come tutte le organizzazioni, anche quelle terroristiche necessitano di ingenti finanziamenti per raggiungere i propri obiettivi, sia che si tratti di attività operative sia che si tratti di diffondere la propria narrativa all'interno delle varie piattaforme disponibili.

L'obiettivo di questo articolo è fornire una panoramica di come il metodo di finanziamento attraverso il cripto asset abbia cambiato il fenomeno del terrorismo transazionale e quali strategie siano state messe in atto dalla comunità internazionale per contrastarlo.

Cripto asset

Lo sviluppo tecnologico ha influenzato ogni aspetto del mondo contemporaneo, compreso il sistema finanziario ed economico.

Nel 2008 una nuova forma di moneta digitale è stata creata da un programmatore anonimo con l'obiettivo di migliorare la sicurezza degli scambi monetari (Gregersen, 2024).

Di fatto, la *cripto asset* è una moneta virtuale utilizzata nel cyberspazio la cui sicurezza si basa sulla crittografia, un processo di cifratura e decifrazione dei dati che circolano su internet che impedisce a terzi di comprendere i dati che vengono trasferiti.

Il termine *crypto* deriva effettivamente dalla tecnica crittografica (*cryptography*) su cui si basa l'intero sistema.

La moneta tradizionale è regolata e controllata da autorità pubbliche statali e internazionali che sono vulnerabili a una serie di minacce interne ed esterne, mentre gli asset virtuali sono protetti da un sistema di crittografia a chiave pubblica.

Questo sistema si basa su due chiavi, una pubblica e una privata che è univocamente a disposizione dell'utente destinatario e che è responsabile della decifrazione dei dati.

Le due chiavi sono generate da algoritmi specifici sulla base di una relazione matematica.

Il trasferimento di criptovalute viene registrato in un registro strutturato in blocchi in ordine cronologico, comunemente noto come blockchain.

La blockchain è registro pubblico peer-to-peer che raccoglie tutte le transazioni digitali monetarie e mantiene la cronologia di quelle verificate, archiviate in una rete di computer (nodi). È proprio il fatto che il registro sia pubblico che permette al sistema di funzionare senza un'autorità centrale.

Anche se la blockchain è disponibile pubblicamente, l'identità degli utenti è protetta da pseudonimi che utilizzano per completare le transazioni monetarie.

Per utilizzare e conservare le criptovalute gli utenti creano portafogli digitali che sono software collegati a un indirizzo di portafoglio che conferisce loro uno pseudo-anonimato (Alfieri, 2022).

La prima criptovaluta a essere sviluppata è stata il Bitcoin nel 2009, ma da allora l'uso delle criptovalute è aumentato in modo esponenziale grazie all'estrema discrezione che garantisce alle transazioni finanziarie (Gregersen, 2024).

Nel tempo, come alternativa al Bitcoin sono emerse una serie di nuove monete virtuali, con diversi livelli di garanzia della privacy.

Infatti, con il Bitcoin, anche se le identità reali non sono registrate nella blockchain, se il proprietario del portafoglio viene identificato le autorità possono risalire alle transazioni.

Mentre altri tipi di asset virtuale, come Monero o Zcash (C. Dion-Schwarz, 2019), sono caratterizzati da un livello di privacy ancora più elevato e inoltre Zcash permette di utilizzare e trasferire le monete virtuali in modalità offline, rendendo quasi impossibile il tracciamento (Alfieri, 2022).

Infatti, l'identità degli utenti è mantenuta anonima e il sistema blockchain è molto difficile da attaccare, a differenza dei sistemi bancari che hanno ripetutamente mostrato le loro vulnerabilità.

Inoltre, ciò consente di trasferire denaro senza dover passare attraverso un'autorità centrale.

Nel 2024 il valore di mercato degli asset virtuali è stato attestato a 3.000 miliardi di dollari circa (Gregersen, 2024).

Ovviamente anche il sistema dei cripto asset ha dimostrato delle vulnerabilità, essendo diventati un obiettivo principale per gli hacker che hanno visto in questo settore un nuovo mercato fruttuoso e, proprio per la mancanza di un'autorità centrale e di una regolamentazione, il valore della moneta digitale è estremamente volatile.

In ogni caso, l'elemento più controverso che circonda gli asset virtuali è che hanno attirato l'attenzione solo degli utenti comuni e degli uomini d'affari, ma anche di soggetti impegnati in attività illegali e criminali come il riciclaggio di denaro e il finanziamento di organizzazioni terroristiche, poiché garantiscono la possibilità di trasferire grandi quantità di denaro senza essere monitorati e rimanendo anonimi.

Ciò ha portato diversi Stati a vietare completamente o parzialmente l'uso di cripto asset (Gregersen, 2024) poiché sono emersi come fattore di rischio per la sicurezza interna.

La rivoluzione informatica

Come già detto lo sviluppo tecnologico e la globalizzazione hanno completamente rivoluzionato ogni aspetto del mondo contemporaneo, compreso il terrorismo.

Infatti, se da un lato Internet ha dato la possibilità di sviluppare piattaforme in cui persone con gli stessi interessi o le stesse esigenze potevano entrare in contatto indipendentemente dalla loro posizione geografica, dall'altro ha rappresentato una nuova risorsa per le organizzazioni criminali e terroristiche.

In seguito allo sviluppo delle nuove tecnologie, le piattaforme online sono state utilizzate per vari scopi, dalla pianificazione di attentati terroristiche, alla diffusione dell'ideologia, al reclutamento e al finanziamento.

Le attività dei gruppi terroristiche si sono spostate dal mondo reale a quello virtuale, dato il gran numero di vantaggi che il cyber spazio può garantire ai membri delle organizzazioni nel raggiungimento dei loro obiettivi.

Infatti, la diffusione di Internet, che ha rafforzato ed è stata a sua volta rafforzata dalla globalizzazione, ha dato il via a una nuova fase in cui le organizzazioni terroristiche sono caratterizzate da una dimensione transnazionale.

I confini statali e il sistema nazionale non vengono quindi presi in considerazione, in quanto la minaccia viene in qualche modo considerata “liquida”, trascendendo quindi i confini fisici.

Il regno cibernetico ha dato, e dà tuttora, la possibilità di diffondere materiali radicalizzanti raggiungendo un numero potenzialmente infinito di utenti e garantendo il mantenimento dell’anonimato grazie al sistema di crittografia end-to-end su cui si basano le piattaforme (es. Telegram) che vengono utilizzate a scopo di radicalizzazione, reclutamento, pianificazione o addirittura attacco.

L’organizzazione terroristica ha immediatamente riconosciuto il potenziale di Internet come risorsa e ha iniziato il passaggio alla piattaforma online.

Ad esempio, nel 2015 un gruppo di terroristi affiliati ad al-Qaeda, Al-Aqsa IT Team, ha distribuito tra i suoi membri “*The Browser Security Guidelines*”, un manuale contenente le istruzioni per una navigazione sicura e anonima attraverso il software Tor. Il manuale elencava i dettagli su ogni passo e misura da adottare per utilizzarlo evitando di essere geolocalizzati, tracciati e identificati dalle autorità (Surace, 2020).

Tor è un software che reindirizza il traffico web attraverso un elevato numero di server informatici al fine di oscurare l’indirizzo di emissione e di ricezione, rendendo quasi impossibile per le forze dell’ordine tracciare e identificare l’utente che naviga utilizzando Tor.

La combinazione di Tor e cripto asset è una risorsa importante per mantenere l’anonimato dei criminali che si dedicano ad azioni illecite, di cui una parte avviene nel cyberspazio.

Attività tradizionali, nuovi strumenti

Concentrandosi sul settore finanziamento, i gruppi terroristici o gli individui, utilizzano Internet per facilitare le transazioni illecite e il finanziamento delle loro attività.

È ora necessario delineare le principali fonti di reddito dei gruppi terroristici e come l’emergere delle monete virtuali abbia influito su queste attività di finanziamento.

Tra le principali attività finanziarie che i gruppi terroristici hanno utilizzato per finanziare le loro attività ci sono (C. Dion-Scwarz, 2019):

- Contrabbando. Le organizzazioni hanno creato una rete di traffico di droga, armi e risorse naturali, anche in associazione con gruppi di criminalità organizzata, in cui si impegnano direttamente o proteggono chi trasporta illegalmente queste risorse.
- Raccolta fondi. Provengono da donatori privati o anche da sponsor statali, di solito in contanti.

Ovviamente, entrambe queste strategie di finanziamento sono state influenzate dall’emergere delle criptovalute, che hanno il vantaggio di garantire l’anonimato, la rapidità e la sicurezza dei dati.

Il commercio di beni illeciti ha sempre rappresentato una parte importante delle entrate delle organizzazioni terroristiche, in particolare il contrabbando di armi e droga.

Questo tipo di mercato illegale ha visto una rivoluzione con l’evoluzione di Internet e dei cosiddetti *dark net marketplace*, o *criptomercati*, che sono siti situati nel dark web in cui le persone possono vendere o acquistare qualsiasi tipo di merce.

L’introduzione dei cripto asset e del già citato software Tor ha reso il mercato ancora più redditizio, in quanto gli utenti possono contare sull’estrema privacy garantita dai due asset (Alfieri, 2022).

La Silk Road è stato il primo famoso *criptomercato*, creato nel 2011 da Ross Ulbricht, in cui si vendeva e si comprava qualsiasi bene illecito immaginabile, soprattutto droga.

Il mercato si basava sull'uso di criptovalute e su Tor, che garantivano l'anonimato degli utenti e la riservatezza della loro posizione fisica.

In ogni caso, il sito è stato sequestrato dall'FBI nel 2013 e Ulbricht arrestato e condannato all'ergastolo, ma dopo Silk Road sono stati creati altri mercati dark net e ancora le forze dell'ordine devono interfacciarsi con un sistema di contrasto inefficace (Alfieri, 2022).

Per quanto riguarda il sistema della raccolta fondi, essa è stata tradizionalmente effettuata attraverso vari metodi, come rimesse fisiche, trasferimenti a familiari o amici o attraverso organizzazioni professionali che utilizzano sistemi di trasferimento informali.

Uno dei sistemi informali più utilizzati è l'*hawala*, che si basa sul coinvolgimento di due attori esterni, chiamati *hawaldar*:

- Il soggetto emittente che deve trasferire la donazione da un Paese all'altro si rivolge a un primo *hawaldar* e gli consegna l'importo scelto;
- Il primo *hawaldar* contatta un secondo *hawaldar* residente nel Paese di destinazione, incaricandolo di pagare l'importo al destinatario finale (Surace, 2020).

In questo modo non c'è contatto diretto tra il soggetto emittente e quello ricevente.

Ad esempio, nel 2017 l'organizzazione terroristica sciita libanese Hezbollah ha lanciato una campagna di raccolta fondi online chiamata "*Equipaggia un Mujahid*" per sollecitare donazioni al fine di finanziare le proprie azioni ed equipaggiare i propri membri (T. Johnston, 2023).

La campagna di raccolta fondi è stata lanciata attraverso il loro account Twitter e il loro sito web, in cui hanno usato strumentalmente il pilastro islamico delle donazioni di beneficenza obbligatorie per incoraggiare le persone a donare (MEMRI, 2017).

La Banca Centrale libanese ha avuto un ruolo fondamentale nel reprimere e contrastare la campagna di Hezbollah in quanto autorità centrale attraverso la quale venivano effettuati i pagamenti.

Per questo motivo il sistema delle cripto monete è emerso come un asset alternativo fondamentale per le campagne di raccolta fondi, poiché, come già detto, non dipende dal controllo di un'autorità centrale ed è più veloce dei trasferimenti in contanti.

Da qualche anno, infatti, le raccolte fondi hanno registrato un significativo spostamento verso l'uso delle cripto monete.

Le piattaforme online legate alle organizzazioni terroristiche hanno iniziato a richiedere il pagamento delle donazioni tramite cripto asset. Le piattaforme forniscono persino le istruzioni su come donare e su come preservare l'anonimato.

Ad esempio, dal 2019 l'organizzazione terroristica operante nella Striscia di Gaza, Hamas, e altri gruppi ad essa collegati come l'ala militare *Izz ad-Din Al-Qassam Brigades* (IQB), hanno lanciato pubblicamente campagne di raccolta fondi con pagamento tramite cripto monete (L. Marchese, 2023).

L'IQB ha lanciato la prima vera campagna basata su Bitcoin nel 2019 attraverso il proprio sito web, chiedendo ai sostenitori di utilizzare un codice QR che reindirizzava l'utente all'indirizzo Bitcoin. Poi l'utente doveva inviare il denaro virtuale all'indirizzo Bitcoin. Quando le autorità sono riuscite a scoprire l'indirizzo, il gruppo aveva già raccolto circa 2.000,00 USD (Surace, 2020).

In seguito, per continuare a ricevere donazioni hanno cambiato il sistema lanciando la creazione di un nuovo portafoglio virtuale per ogni transazione del sostenitore (T. Wilson, 2019) e in un video hanno anche spiegato i due modi possibili per inviare la criptovaluta:

- Il già citato metodo *hawala*, riadattato al trasferimento di Bitcoin.
- La creazione di un portafoglio Bitcoin privato.

Quando la campagna è stata chiusa dalle autorità nel 2020, IQB aveva già guadagnato 10.000 USD.

Le cripto monete sono quindi estremamente rilevanti nel contesto delle campagne di raccolta fondi a sostegno delle organizzazioni terroristiche, in quanto garantiscono l'anonimato, la rapidità e la decentralizzazione che il sistema tradizionale non offre.

Hamas non è l'unica organizzazione che si affida sempre di più alle criptovalute per finanziare la propria struttura e le proprie azioni.

Da quando l'IS ha fondato il Califfato nel 2014 stabilendo un controllo territoriale su parti della Siria e dell'Iraq, ha rappresentato una rivoluzione nel sistema di finanziamento in quanto i membri dell'organizzazione potevano contare sulla proiezione di un'autorità effettiva sul territorio (T. Johnston, 2023).

Quindi le entrate dell'IS derivavano principalmente dal commercio illecito di petrolio e dal controllo delle autorità finanziarie che permetteva loro di raccogliere tasse e donazioni dalla popolazione locale ma anche da sostenitori esterni, offrendo loro un accesso alle istituzioni finanziarie internazionali lecite (T. Johnston, 2023).

È infatti con l'IS che la comunità di ricerca ha notato un passaggio al terrorismo transnazionale, poiché il suo obiettivo, le strategie messe in atto per raggiungerlo e la portata del suo messaggio non solo erano internazionali, ma trascendevano le barriere fisiche.

Questo è il motivo per cui IS fin dall'inizio ha visto le nuove tecnologie e Internet come un asset fondamentale, le cripto monete sono uno di questi.

Anche dopo aver perso il controllo del territorio, l'ISIS ha potuto contare sulle riserve monetarie e dispone di una sofisticata rete globale che gli garantisce un accesso continuo alle risorse finanziarie. L'ISIS ha istituito due uffici principali che monitorano e garantiscono la stabilità finanziaria dell'organizzazione, l'ufficio *al-Siddiq* e l'ufficio *al-Karrar*, il primo responsabile dei flussi monetari nella regione dell'Asia centrale e meridionale, mentre il secondo per i Paesi africani.

Attraverso le campagne di raccolta fondi lanciate tramite i social media o la letteratura di propaganda, l'IS ha raccolto una quantità significativa di valuta virtuale che è stata poi collegata direttamente agli operatori affiliati all'IS (Roul, 2024).

Se all'inizio utilizzavano in modo preponderante il Bitcoin, la crescente trasparenza del flusso monetario virtuale ha spinto l'organizzazione e i suoi affiliati a passare ad altre cripto monete caratterizzate da indirizzi stealth, estrema privacy e anonimato che le hanno trasformate in un nuovo asset virtuale per la stabilità finanziaria dell'organizzazione terroristica.

Uno dei più utilizzati è Monero, in quanto nasconde i dettagli delle transazioni garantendo una protezione maggiore dal monitoraggio e dal tracciamento delle autorità.

Un ultimo caso di interesse che vede l'implicazione del finanziamento virtuale è l'attentato alla Crocus Hall di Mosca, perpetrato il 22 marzo 2024 da membri dell'ISKP (*Stato Islamico-Provincia del Khurasan*), che è risultato nell'uccisione di 130 persone.

L'organizzazione, affiliata all'IS in Afghanistan, aveva visto in precedenza un trasferimento di almeno 2.000 dollari in criptovaluta e secondo le Nazioni Unite aveva ricevuto migliaia di dollari al mese dall'ufficio di *al-Karrar* (Insight, 2024).

Dal 2021 l'ISKP ha iniziato a lanciare campagne e messaggi di propaganda per le donazioni monetarie da effettuare tramite Monero e ha anche pubblicato una guida all'acquisto di Monero (Roul, 2024).

Quindi, anche se le cripto monete sono solo una parte del complesso sistema di finanziamento delle organizzazioni terroristiche, la loro struttura decentralizzata e la garanzia di anonimato hanno messo in allarme le autorità che hanno iniziato a studiare a fondo nuove strategie per contrastare questo specifico elemento dell'intero quadro.

Segui il denaro

Quadro internazionale

Il rischio posto dalle criptovalute è consistente anche a causa della mancanza di una normativa che ne regoli l'uso e il trasferimento attraverso la rete mondiale.

Dalla fine dello scorso millennio la comunità internazionale ha riconosciuto la necessità di strutturare un quadro normativo in materia di finanziamento del terrorismo.

Nel 1999 la Convenzione di New York ha posto le basi per un approccio comune internazionale al riconoscimento del finanziamento delle organizzazioni terroristiche come condotta criminale autonoma.

Nello stesso anno il Consiglio di Sicurezza delle Nazioni Unite ha approvato la Risoluzione 1267/1999 che ha introdotto la pratica del “congelamento dei fondi e delle altre risorse finanziarie” legate ai Talebani, ad eccezione di alcuni importi che possono essere “autorizzati da Comitato per i bisogni umanitari” nell'articolo 4.b (S/RES/1267, 1999).

All'articolo 6 la Risoluzione istituiva inoltre un Comitato del Consiglio di Sicurezza che doveva osservare, analizzare e riferire ogni azione in violazione delle misure elencate nella Risoluzione e ogni Stato membro era tenuto a inviare rapporti periodici al Consiglio.

La Risoluzione è stata creata nel contesto delle azioni del gruppo talebano in Afghanistan che, guidato da Osama bin Laden, nel 1998 ha bombardato le ambasciate statunitensi in Kenya e Tanzania e ha continuato a proteggere e addestrare i terroristi internazionali (S/RES/1267, 1999).

Il Comitato aveva il compito di stilare una lista nera con le entità e i soggetti riconosciuti come membri di organizzazioni terroristiche o legati ad al Qaeda.

Poi, all'indomani dell'attacco sul territorio nazionale statunitense da parte di terroristi jihadisti membri di al Qaeda l'11 settembre 2001, la lista è stata estesa anche ad altre organizzazioni terroristiche.

La Risoluzione 1373/2001, all'articolo 1.a, obbliga tutti gli Stati membri a “prevenire e reprimere il finanziamento di atti terroristici” e, di conseguenza, a criminalizzare qualsiasi finanziamento diretto o indiretto di un atto terroristico e a congelare qualsiasi fondo o attività finanziaria o risorsa economica o di soggetti o entità coinvolte o collegate a organizzazioni terroristiche (S/RES/1373, 2001).

Con l'emergere dell'ISIS nel 2014, il Consiglio di Sicurezza delle Nazioni Unite ha adottato due nuove risoluzioni.

Si estende ai membri dell'ISIS e del *Fronte al-Nusra* le misure applicate ad al Qaeda e ai Talebani (S/RES/2170, 2014) e si impone agli Stati membri la messa in campo di strategie specifiche per colpire il fenomeno dei *foreign fighters* che costituivano una nuova e fondamentale risorsa per il finanziamento dell'organizzazione.

Negli anni successivi il quadro normativo internazionale implementato dalle Nazioni Unite si è concentrato principalmente sulla lotta all'ISIS.

Una delle misure riguardava specificatamente il congelamento dei fondi dell'organizzazione e l'arresto dei flussi monetari derivanti dal commercio del petrolio estratto dal territorio controllato, o dal commercio illecito di antichità o ancora dai riscatti (Banca d'Italia, s.d.).

Ovviamente, per attuare queste norme, gli Stati e le Nazioni Unite si sono affidati al controllo dei flussi di denaro da parte delle autorità centrali o, in caso di trasferimenti di denaro contante, al monitoraggio fisico delle frontiere.

Ciò rende le cripto monete una minaccia dirompente per l'attuazione di strategie internazionali di controllo contro il finanziamento del terrorismo, poiché i beni virtuali non possono essere congelati da un'autorità centrale finanziaria eludendo i controlli tradizionali.

Gruppo di azione finanziaria internazionale (GAFI)

Poiché il finanziamento del terrorismo è un crimine finanziario che può destabilizzare non solo la stabilità finanziaria di un paese, ma anche la stabilità interna generale, le organizzazioni internazionali hanno iniziato ad implementare una serie di misure per contrastarlo.

Infatti, poiché il mondo è sempre più interconnesso e le minacce che i Paesi si trovano ad affrontare riguardano l'intera stabilità internazionale, le politiche per mitigarle e contrastarle devono basarsi sulla cooperazione e sulla collaborazione che passa necessariamente attraverso le organizzazioni internazionali.

L'organo di controllo globale per il riciclaggio di denaro e i crimini finanziari, noto come GAFI, è stato istituito nel 1989 durante un vertice del G7 a Parigi.

Poiché l'11 settembre è stato un evento spartiacque per l'ordine globale, la comunità internazionale ha iniziato ad applicare la politica del “*segui i soldi*” anche per prevenire attacchi terroristici.

Così, il GAFI ha esteso il suo mandato anche al monitoraggio e alla riduzione del finanziamento del terrorismo.

L'atto principale del GAFI nel contrastare questo fenomeno è stato quello di pubblicare una lista di Otto Raccomandazioni Speciali sul finanziamento del terrorismo che nel corso degli anni sono state ripetutamente riviste e rafforzate per tenere il passo con l'evoluzione delle strategie di finanziamento dei gruppi terroristici (FATF, n.d.).

Come obiettivo principale del presente documento, è necessario sottolineare la revisione attuata nel 2019, quando la task force ha incluso nelle Raccomandazioni una parte di strategie obbligatorie che i membri dovevano adottare per regolamentare e monitorare la minaccia emergente delle cripto monete come strumento di finanziamento del terrorismo.

Il problema principale è il fatto che le criptovalute non sono regolamentate a livello internazionale in quanto non devono passare attraverso un'autorità centrale o l'autorizzazione di uno Stato; questo ha portato a un approccio globale frammentato rispetto ai cripto asset con alcuni Stati che hanno regolamentato gli scambi di valuta virtuale, come il Giappone, e altri che li hanno vietati, come la Cina.

Il GAFI rappresenta lo strumento di risposta alla necessità di un'armonizzazione internazionale delle misure di contrasto ai crimini internazionali di oggi, poiché questo è l'unico modo in cui queste minacce nazionali possono essere mitigate.

Le attuali 40 Raccomandazioni includono un quadro normativo, regolamenti e strategie operative specifiche per ogni settore che rientra nel mandato dell'Agenzia, una delle quali è il “Finanziamento del terrorismo e finanziamento della proliferazione” (FATF, n.d.).

- L'attuazione su base nazionale della Convenzione sul finanziamento del terrorismo per criminalizzare il finanziamento del terrorismo, anche se la donazione non è direttamente collegata a un atto terroristico.
- L'attuazione di sanzioni economiche in conformità alle risoluzioni 1267 e 1373 del Consiglio di Sicurezza delle Nazioni Unite.
- L'attuazione di sanzioni economiche legate al contrasto del commercio e alla prevenzione dell'uso di armi di distruzione di massa.

Per quanto riguarda il rischio che emerge dall'uso delle cripto monete, la Raccomandazione del GAFI indica che i promotori di tali attività devono conformarsi agli standard antiriciclaggio e di

lotta al finanziamento al terrorismo (AML/CTF) e alle Raccomandazioni del GAFI, nonché essere registrati o autorizzati.

Le autorità internazionali e nazionali stanno lavorando per implementare lo Standard GAFI nel contesto del finanziamento del terrorismo.

Ad esempio, il Fondo Monetario Internazionale (FMI) ha contribuito all'attuazione delle misure antiriciclaggio e di assistenza ai Paesi membri nel settore finanziario.

Il FMI, in quanto principale organizzazione internazionale in materia di finanza, ha la possibilità di svolgere un ruolo fondamentale nel monitoraggio, nel contenimento e nella prevenzione del flusso di fondi illeciti, lavorando in collaborazione con il GAFI (IMF, s.d.).

Regolamentazione internazionale delle cripto monete: UE

L'uso di cripto monete è ancora associato a un vulnus legislativo nel sistema nazionale e internazionale, che consente l'uso di beni virtuali per il finanziamento del terrorismo. In ogni caso, le cose in questo ambito stanno rapidamente evolvendo, ad esempio l'Autorità europea degli strumenti finanziari e dei mercati (ESMA), l'agenzia dell'UE responsabile della regolamentazione e della vigilanza dei mercati finanziari, nel maggio del 2023 ha stabilito una normativa completa senza precedenti sulle criptovalute, la *Markets in Crypto-Assets Regulation* (MiCA), che introduce una serie di norme restrittive sull'uso degli asset virtuali e una maggiore trasparenza e stabilità nel relativo mercato (MiCA, n.d.).

Il Regolamento è entrato in vigore nel giugno 2023 e si trova ora nella fase di consultazione che consiste nel dialogo con altre organizzazioni e con il pubblico con l'obiettivo di delineare una serie di misure e standard completi che potrebbero regolare la materia e che saranno attuati nel dicembre 2024 dopo l'adozione da parte della Commissione Europea.

Questo rappresenta un primo tentativo di allineare il quadro normativo a livello internazionale e gli Stati membri e la comunità internazionale dovrebbero considerarlo un'opportunità fondamentale.

Conclusioni

In conclusione, è possibile affermare che l'approccio di "segui il denaro" è necessario per affrontare le attuali minacce alla sicurezza nazionale, soprattutto nel contesto del finanziamento del terrorismo, indipendentemente dall'evoluzione degli strumenti utilizzati.

Anche se i beni virtuali sono solo una parte del sistema di finanziamento delle organizzazioni terroristiche, stanno acquisendo sempre più importanza, soprattutto perché le cripto monete come Monero e Zcash danno la possibilità di oscurare i dettagli delle transazioni e dei soggetti coinvolti. Inoltre, le organizzazioni terroristiche hanno dimostrato una grande capacità di resistenza e di adattamento alle forze dell'ordine, come nel caso del cambiamento di strategia applicato dalle *Brigate Izz ad-Din Al-Qassam* nel contesto della loro campagna di finanziamento online.

Ciò evidenzia la necessità per i governi e le autorità di tenersi costantemente aggiornati all'evoluzione della tecnologia utilizzata dalle organizzazioni terroristiche, al fine di comprendere meglio come si muovono e, di conseguenza, come arginare il crescente utilizzo di questa risorsa virtuale.

Vale la pena ricordare che tra le ragioni che hanno impedito alle criptovalute di diventare lo strumento preferito di finanziamento c'era un motivo religioso relativo al fatto che la loro elevata volatilità le faceva avvicinare alla categoria del gioco d'azzardo, che nella religione islamica è vietato (*haram*).

Il loro utilizzo rischiava quindi di minare anche la credibilità religiosa e l'autorità dell'organizzazione che lanciava le campagne di finanziamento.

La situazione sta cambiando da quando alcune agenzie hanno raggiunto la standardizzazione del valore dei loro cripto asset, aprendo la strada a un'evoluzione che potrebbe rendere gli asset virtuali più stabili sul mercato e di conseguenza più conformi ai precetti islamici.

Tutti questi elementi supportano la tesi per cui gli asset virtuali, se non adeguatamente regolamentati, rappresenteranno uno strumento fondamentale per il finanziamento del terrorismo e quindi una seria minaccia per la sicurezza interna.

Bibliografia

Alfieri, C. (2022). Criptovalute e sicurezza nazionale. *International Journal on Criminology*.

Banca d'Italia. (s.d.). *Contrasto al finanziamento del terrorismo*. Tratto da Unità di Informazione Finanziaria per l'Italia (UIF), Banca d'Italia: <https://uif.bancaditalia.it/normativa/norm-contr-terr/index.html?com.dotmarketing.htmlpage.language=102&dotcache=refresh>

C. Dion-Schwarz, D. M. (2019). Uso terroristico delle criptovalute, barriere tecniche e organizzative e minacce future. *RAND Corporation*.

GAFI. (n.d.). *Le raccomandazioni del GAFI*. Recuperato dal GAFI: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html>

Gregersen, E. (2024). *criptovalute*. Tratto da Encyclopaedia Britannica: <https://www.britannica.com/money/cryptocurrency>

FMI. (s.d.). *Antiriciclaggio e lotta al finanziamento del terrorismo (AML/CTF)*. Tratto dal Fondo Monetario Internazionale: <https://www.imf.org/en/Topics/Financial-Integrity/amlcft#>

Insight, T. (2024). *Dopo l'attacco di Mosca, l'uso delle criptovalute da parte dell'ISIS*. Tratto da TRM: <https://www.trmlabs.com/post/in-wake-of-moscow-attack-understanding-isis-use-of-cryptocurrencies>

L. Marchese, G. D. (2023). *Criptovalute a sostegno della macchina bellica di Hamas: così adesso si finanzia il terrorismo*. Tratto da Cybersecurity360: <https://www.cybersecurity360.it/cybersecurity-nazionale/criptovalute-a-sostegno-della-macchina-bellica-di-hamas-cosi-adesso-si-finanzia-il-terrorismo/>

MiCA. (n.d.). *Regolamento sui mercati dei cripto-asset (MiCA)*. Recuperato dall'Autorità europea per la sicurezza e i mercati: <https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica>

Roul, A. (2024). *L'ascesa del Monero: la criptovaluta preferita dall'ISKP per il finanziamento del terrorismo*. Tratto da Global Network on Extremism & Technology : <https://gnet-research.org/2024/10/04/the-rise-of-monero-iskps-preferred-cryptocurrency-for-terror-financing/>

S/RES/1267, S. (1999). *S/RES/1267*. Tratto dal Consiglio di Sicurezza delle Nazioni Unite: <http://unscr.com/en/resolutions/doc/1267>

S/RES/1373. (2001). *Risoluzione 1373*. Tratto dal Consiglio di Sicurezza delle Nazioni Unite: <http://unscr.com/en/resolutions/doc/1373> [Ultimo visto: 19.11.2024].

Surace, V. (2020). Il ruolo delle criptovalute nel sistema di finanziamento delle organizzazioni terroristiche. *Analytica for intelligence and security studies*.

T. Johnston, E. E. (2023). Convertire il finanziamento di attori non statali violenti. *RAND Corporation*.

T. Wilson, D. W. (2019). *Il cambio di tattica di Hamas nella raccolta di fondi in bitcoin evidenzia i rischi della criptovaluta: ricerca*. Tratto da Euronews: <https://www.euronews.com/2019/04/26/hamas-shifts-tactics-in-bitcoin-fundraising-highlighting-crypto-risks-research>

Sara Osimani – *Dottoressa in Scienze della Mediazione Linguistica presso la Scuola Superiore per Mediatori Linguistici di Pisa, Master in Relazione Internazionale e Protezione Internazionale dei Diritti Umani presso SIOI (Società Italiana per l'Organizzazione Internazionale), attualmente studente magistrale in Investigazione, Criminalità e Sicurezza Internazionale, presso l'Università degli Studi Internazionali di Roma. Stagista presso Vision & Global Trends International Institute for Global Analyses, nell'ambito del progetto [Società Italiana di Geopolitica](#).*



Vision & Global Trends - International Institute for Global Analyses

www.vision-gt.eu

info@vision-gt.eu