FINANCING TERRORISM THROUGH CRYPTOCURRENCIES

Alina Georgiana HOLT
Lect.univ.dr.
Universitatea „Constantin Brâncuși" din Târgu Jiu

Ing. Cătălin UDROIU
Stefanini Romania

ABSTRACT

TODAY'S SECURITY ENVIRONMENT IS INCREASINGLY COMPLEX. THE TIMES WHEN PEACE, CRISIS AND CONFLICT WERE THREE DISTINCT PHASES, WHEN CONFLICTS WERE MOSTLY FOUGHT BY MILITARY MEANS AND WHEN THE ADVERSARIES WERE WELL KNOWN, ARE OVER. TODAY, CYBER ATTACKS HIT NATIONS BEFORE A MILITARY ATTACK. SOCIAL MEDIA CAMPAIGNS CREATE ALTERNATE REALITIES THAT SEEK TO DESTABILIZE POLITICAL COMMUNITIES WITHOUT A SINGLE SOLDIER CROSSING A SINGLE BORDER. AND THE "HYBRID" COMBINATION OF MILITARY AND NON-MILITARY TOOLS CREATES AMBIGUITIES THAT MAKE NATO'S SITUATIONAL AWARENESS AND, CONSEQUENTLY, CONSENSUAL AND RAPID DECISION-MAKING MUCH MORE DIFFICULT. HYBRID THREATS ARE A GROWING CONCERN FOR SOCIAL COHESION AND THE CONTINUITY OF GOVERNMENTS. IN RECENT YEARS, THIS NEW FORM OF THREAT HAS COME TO BE INCREASINGLY PRESENT AMONG THOSE RESPONSIBLE FOR MANAGING CRISIS CELLS AND SECURITY POLICY. THEY CAN THREATEN TO WEAKEN A STATE AND MAJOR STATE INSTITUTIONS OR INDUSTRIES BY EXPLOITING THEIR VULNERABILITIES. THESE THREATS REQUIRE MINIMAL RESOURCES AND REDUCED COSTS THROUGH THE MAJOR INFLUENCE OF TODAY'S SOCIAL MEDIA. FROM CYBER ATTACKS ON CRITICAL SYSTEMS, TO DISINFORMATION THROUGH SOCIAL MEDIA AND BROADCAST CAMPAIGNS, RECENT EXAMPLES DEMONSTRATE THE POWER OF HYBRID THREATS TO ERODE SOCIAL COHESION, CITIZENS' TRUST IN PUBLIC INSTITUTIONS, ELECTORAL PROCESSES AND GOVERNMENT CONTINUITY.

THE ROLE OF THIS ARTICLE IS TO PRESENT A NEW TYPE OF FINANCING OF TERRORIST GROUPS WITH THE HELP OF A PAYMENT METHOD THAT IS INCREASINGLY DIFFICULT TO TRACE.

KEYWORDS: *TERRORISM, ECONOMIC CRIME, CRYPTOCURRENCY, NATIONAL SECURITY, HYBRID THREATS*

Finanțarea terorismului este baza economică a activităților teroriste și colacul de salvare al acestor organizații. În ultimii ani, organizațiile teroriste au ajuns treptat să folosească criptomoneda pentru a-și finanța activitățile pe baza modalităților tradiționale de strângere de fonduri. Anonimitatea criptomonedei este atractivă pentru organizațiile teroriste, dar utilizarea sa rămâne la un nivel scăzut.

Încă nu s-au manifestat îngrijorările cu privire la utilizarea criptomonedei pentru a permite activități teroriste[1], dar îmbunătățirile actuale și viitoare ale tehnologiilor folosite

[1] Ina Raluca Tomescu, „CITIZENS' RIGHTS AND LIBERTIES vs. ANTITERRORIST LEGISLATION", în Annals of the „Constantin Brâncuși" University of Târgu Jiu, Letter and Social Science Series, Issue 3/2013, pp. 48-52

pentru creareacriptomonedei vor avea, probabil, un efect semnificativ pe termen lung asupra finanțării terorismului.

Viteza cu care aceste tehnologii sunt adoptate și cum sunt implementate, sunt incertitudini critice care au impact operațional important.

Reglementarea și supravegherea criptomonedelor, împreună cu cooperarea internațională dintre forțele de ordine și serviciile de informații, ar fi pași importanți pentru a preveni organizațiile teroriste să folosească criptomonede pentru a-și susține activitățile.

Criptomoneda, ca instrument de finanțare a terorismului, prezintă probleme dificile pentru serviciile secrete de informații. Spre deosebire de profilurile de pe rețelele sociale și conturilebancare, agenții, de multe ori, nu pot închide o adresă prin intermediul căreia se tranzacționează criptomonedă, din cauza naturii descentralizate a blockchain-urilor.

În timp ce schimbul de cunoștințe este esențial pentru a contracara sau a identifica o astfel de amenințarepericuloasă, finanțarea terorismului în criptomonede este, de asemenea, dificil de raportat public, deoarece majoritatea cazurilor implică informații sensibile sau sunt clasificate din motive de securitate națională[1].

Izz ad-Din al-Qassam Brigades (AQB) - Cea mai mare campanie de finanțare a terorismului

La începutul anului 2019, Brigăzile Izz ad-Din al-Qassam (AQB)[2], aripa militară a Hamas și o altă organizație teroristă desemnată – au început să solicite donații în Bitcoin într-una dintre cele mai mari și mai sofisticate campanii de finanțare a terorismului bazate pe criptomonede văzută vreodată. AQB a folosit mai multe tipuri de infrastructuri cu portofel electronic pentru aprimi donații, înainte a se implementa un sistem care a generat o nouă adresă pentru fiecare donator ce urma să trimită fonduri, și, totodată, primul exemplu verificat de o astfel de tehnologie utilizată de o grupare teroristă.

Până în prezent, campania a generat sute de mii saupoate chiar milioane de dolari în Bitcoin pentru AQB. Și în prezent, anchetatorii și analiștii folosesc aceste tranzacții, ceea ce le-ar putea permite să identifice originea donațiilor și destinația fondurilor primite de AQB în timpul campaniei sau deoricare organizație teroristă. În cele din urmă, acest lucru i-ar putea ajuta să identifice donatoriișisi beneficiarii financiari de la AQB care au condus campania[3].

Cum a solicitat AQB donații prin intermediul criptomonedelor

Cel mai simplu mod de a înțelege evoluția campaniei 2019 a AQB este împărțirea acesteia în treisubcampanii, în funcție de tipul de portofel pe care organizația l-a folosit pentru a primi donații.

Prima subcampanie a început în ianuarie 2019, când site-ul web AQB a început să afișeze un mesaj care invita utilizatorii să „doneze jihadului", pe baza unui cod QR aflat in partea de jos aafișului care ducea la o singură adresă Bitcoin. Acea adresa Bitcoin a fost asociată cu un cont la o bursă reglementată din SUA. Oamenii legii au reușit să alerteze rapid bursa, să înghețe contul și să investigheze persoana care a creat acel cont precum și tranzacțiile efectuate prin intermediul acestuia. A doua subcampanie a început când AQB a înlocuit adresa tranzacționare

[1] V. Neagoe, I. R. Tomescu, Geopolitică și strategii de securitate, Ed. Universității Naționale de Apărare "Carol I", București, 2005

[2] New Hamas Fundraising Campaign - https://www.terrorism-info.org.il/en/new-hamas- fundraising-campaign-hamas-military-wing-began-a-new-fundraising-campaign-about-a-month- after-the-united-states-thwarted-digital-coin-campaigns-of-hamas-al-qaeda-and-isis/

[3] Global Disruption of Three Terror Finance Cyber-Enabled Campaigns - https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled- campaigns

cu una nouă legată deun portofel privat, fără custodie, invocând necesitatea unui anonimat sporit.

Cu toate acestea, analiștii si serviciile abilitate au reușit să urmărească donațiile și retragerile de pe adresa respectivă. Ulterior, AQB a lansat cea de-a treia subcampanie mult mai avansată, cu un portofel Bitcoin integrat în site-ul lor, care a generat o adresă Bitcoin unică pentru fiecare donator la care puteau trimite contribuții. AQB a publicat și un videoclip despre el pe site-ul web
care le arată utilizatorilor cum să doneze cât mai anonim posibil.

Figura 1. QR Code si Adresa Bitcoin pentru donații

Videoclipul cu instrucțiuni al AQB a oferit donatorilor două metode de a trimite în Bitcoin. În prima metodă, donatorii au fost instruiți să meargă la o hawala, un tip de afacere de servicii monetare care este populară în Orientul Mijlociu.

Donatorii puteau pur și simplu să meargă la un hawala, să predea oricât de mulți bani doreau să doneze și să furnizeze adresa de donație pe care AQB le-a dat-o. De acolo, hawala trimitea cantitate echivalentă de Bitcoin.

Pentru a doua metodă, donatorii au fost instruiți despre cum să-și creeze propriul portofel privat prin care să poată trimite donația - videoclipul AQB afișează chiar și o listă de portofele recomandate și, de asemenea, platforme de tranzacționare de unde pot obține Bitcoin.

Figura 2. Crearea unui portofel electronic pe un site web de încredere

Instrucțiunile AQB au fost destul de amănunțite, spunându-le donatorilor chiar să folosească wifi-ul public atunci când își creează portofelul privat pentru a evita compromiterea adresei IP.

Analizând cele 3 campanii, subcampania 3 este cea mai avansată din punct de vedere al tehnologiei folosite pe care care o grupare a folosit-o până în prezent pentru finanțarea terorismului cu ajutorul criptomonedelor.

În timp ce majoritatea donatorilor au oferit sume relativ mici, au existat încă destui donatorimari pentru Subcampania 3 pentru a aduce criptomonede în valoare de zeci de mii de dolaripentru AQB.

Având în vedere succesul campaniei de donații a AQB, este posibil să vedem alte organizații teroriste lansând campanii similare cu aceasta în 2020 și mai departe.

În timp ce majoritatea donatorilor au oferit sume relativ mici, au existat însă și donatori care prin intermediul subcampaniei 3 au donat sume mari care au dus la strângeri substanțiale defonduri prin intermediul criptomonedelor pentru gruparea teroristă AQB.

Având în vedere succesul campaniei de donații a AQB, este posibil să vedem și alte organizații teroriste lansând campanii similare cu aceasta în viitor.

În concluzie, ce urmează în ceea ce privește criptocrima și rolul ei în zona de terorism ?

Cripto-crima va continua probabil să evolueze atât în domeniul de aplicare, cât și în ceea ce privește avansarea tehnologică. Pe măsură ce organele de aplicare a legii, autoritățile de reglementare și profesioniștii în criptomonede își îmbunătățesc capacitatea de a preveni și de a răspunde la diferite forme de criminalitate cripto, criminalii înșiși vor deveni, de asemenea, maisofisticați, aceasta fiind singura constantă pe care am văzut-o ca investigator în zona de blockchain.

Pe scurt, acestea sunt câteva idei despre cum ar putea evolua terorismului prin aceasta modalitate de finanțare[1].

1. Mai multe platforme de tranzacționare fără custodie

După închiderea Bestmixer, credem că utilizatorii – infractori și nu numai, vor căuta alternative,cum ar fi portofelele care oferă funcționalitate în care custodia portofelului este 100% controlată de utilizator, similară portofelelor CoinJoin precum Wasabi[2].

Este probabil ca maimulte monede, în afară de Bitcoin, să primească analogi cu CoinJoin, așa cum am văzut cu CoinShuffle[3] pentru Bitcoin.

Retrageri sau tranzacții fără tracking prin contracte inteligente pentru criptomoneda Ethereum.

2. Sărituri (Hopping) în lanț ca o altă alternativă la serviciile de tranzactionare în custodie(mixing)

Pe lângă mixul de tranzacții în portofel, cred, de asemenea, că unii criminali pot începe să favorizeze saltul în lanț ca alternativă la mixarea terților. Hopping-ul în lanț este procesul de schimbare a unui tip de criptomonedă cu altul, adesea de mai multe ori în succesiune rapidă, de obicei de pe piețe care au un KYC (Know-Your-Customer) scăzut, astfel încât să ascundă și mai mult sursa fondurilor.

3. Monede cu un anonimat suplimentar încorporat

Pe piețelor darknet, monedele cu un anonimat suplimentar încorporat, precum Monero, câștigă popularitate și ar putea deveni criptomoneda preferată de mai mulți teroriști/criminali.

Aceste monede le sporesc anonimatul utilizatorilor prin utilizarea unui registru public mai greu de urmărit, mai degrabă decât unul complet public, precum cel al Bitcoin.

Pe măsură ce tot mai multe platforme de tranzacționare accepta monede de confidențialitate, acestea ar trebui, de asemenea, să colaboreze cu autoritățile de reglementare, cu serviciile secrete și între ele pentru a stabili cadre pentru investigarea infractorilor care folosesc monede cu un anonimat suplimentar încorporat.

4. Mai multe opțiuni anonime de schimb P2P (de la persoană la persoană)

Schimburile descentralizate fără custodie, cum ar fi rețeaua Bisq, vor continua să câștige popularitate în rândul criminalilor în 2022. Schimburile descentralizate permit tranzacții peer-to-peer fără ca platforma de tranzacționare să acționeze ca o terță parte mediatoare.

De asemenea, s-ar putea să vedem infractori care folosesc schimburile P2P beneficiind de schimbările viitoare ale protocolului Bitcoin, cum ar fi Taproot și Schnorr Signatures[taproot], care fac ca tranzacțiile complicate bazate pe contracte inteligente efectuate pe platformele detranzacționare să pară identice cu tranzacțiile standard din blockchain.

Toate aceste schimbări le-ar oferi criminalilor mai multe modalități de a-și ascunde activitățile cu criptomonede și ar face tranzacțiile mai dificil de urmărit.

[1] Mărcău, Flavius Cristian; Peptan, Cătălin; Gorun, Tiberiu Horațiu: Băleanu, Vlad Dumitru; Gheorman; Victor (2022b), Analysis of the impact of the armed conflict in Ukraine on the population of Romania, Frontiers in Public Health, 10:964576, iulie 2022, https://doi.org/10.3389/fpubh.2022.96457

[2] WASABI] Wasabi Wallet - Bitcoin privacy wallet with built-in CoinJoin -https://wasabiwallet.io/ [coinsufle] CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin - https://petsymposium.org/2014/papers/Ruffing.pdf

[3] https://www.numbrs.com/schnorr-signatures-and-taproot-coming-to-bitcoin-soon/

Cu toate acestea, suntem încrezători că, odată cu o strânsă colaborarea dintre companiile de criptomonede, serviciilor secrete și autoritățile de reglementare, acest domeniu va fi mult mai ușor de gestionat din punct de vedere ar confidențialității și al transparenței.

CONCLUZII

Interconectarea dintre domeniile fizic, digital și social – ca efect al dezvoltărilor generate de cea de-a patra revoluție industrială pe care o experimentăm în prezent – face ca formele hibride de manifestare a agresiunii să devină mult mai accesibile actorilor statali și non-statali, care le utilizează pentru susținerea propriilor interese strategice în relațiile internaționale.

Noua eră a amenințărilor hibride pune în discuție rolul statului-națiune și, în egală măsură, pe cel al formatelor de cooperare regională și al alianțelor din care acestea fac parte, precum și normelor de drept internațional existente care fie limitează, fie nu asigură un cadru adecvat de răspuns la acest gen de acțiuni.

În noul context de securitate definit de manifestări hibride în conduita actorilor internaționali, reziliența și securitatea nu sunt concepte incompatibile. În acest cadru de analiză, reziliența nu trebuie considerată o alternativă la securitatea națională, ci, dimpotrivă, un mod inovativ de asigurare a acesteia. Această posibilă nouă perspectivă asupra securității ar trebui să fie mult mai flexibilă și să permită descurajarea și contracararea adversarilor hibrizi cu o gamă largă de instrumente, rezultat al interconectării dintre sectoarele civile (publice și private) și sectorul militar.

Formele deosebit de complexe în care se pot manifesta amenințările hibride conduc atât la testarea capacității de răspuns a instituțiilor publice, cât și la testarea legăturii existente între societate și autorități. Acesta este și argumentul care face ca, în faza de pre manifestare a amenințării, conștientizarea pericolului și întărirea parteneriatului dintre instituțiile publice și societatea civilă să fie primordiale pentru creșterea rezilienței sociale. Considerăm că intensificarea efortului pentru identificarea unor soluții inteligente pe dimensiunea culturii de securitate poate susține dezvoltarea rezilienței sociale / comunitare pe termen mediu și lung.

Relația dintre guvern şi populație în context hibrid este esențială. Reziliența națională la amenințări hibride nu implică doar măsurile specifice de răspuns proiectate la nivel instituțional (cum se pregătesc autoritățile să răspundă în cazul unei agresiuni?) ci este un proces înglobat care include toate elementele componente ale unei națiuni, inclusiv participarea societății. Dezvoltarea culturii de securitate la nivelul societății nu trebuie să vizeze exclusiv palierul consolidării încrederii în instituțiile cu atribuții în domeniul securității naționale ci și măsuri concrete destinate creșterii gradului de cunoaștere/conștientizare a formelor emergente/revoluționare de manifestare a amenințărilor de securitate, precum și politici concrete de combatere a noilor acțiuni din sfera războiului informațional – cum sunt, de exemplu, acțiunile de minimizare a efectelor generate de propagarea la scară globală a fenomenului „știrilor false" – și din domeniul cibernetic.