AZ NKE HHK TUDOMÁNYOS FOLYÓIRATA ÁLTALÁNOS

HADTUDOMÁNYI SZEMLE

Budapest, 2014.
7. évfolyam 2. szám

KATONA László

HAGYOMÁNYOS PÉNZTOVÁBBÍTÁSI RENDSZEREK ÉS MODERN TECHNOLÓGIÁK ALKALMAZÁSA A PÉNZMOSÁS ÉS A TERRORFINANSZÍROZÁS TERÜLETÉN

A 2001 szeptemberi terrortámadás-sorozat nemcsak azt jelentette, hogy a terrorizmus történetében új fejezet kezdődött, hanem azt is, hogy az ellene való fellépésnek is új eszközöket kell csatasorba állítani, illetve a meglevőket is hatékonyabban kell alkalmazni.

Kiemelt hangsúlyt kapott a terrorizmus pénzügyi-anyagi hátterének a felderítése, a finanszírozás ellehetetlenítését célzó intézkedések nemzetközi szinten történő bevezetése.

A terroristák erre válaszul egyrészt a hagyományos pénztranszferálási módszerhez, a havalához nyúltak vissza, másrészt a modern kor pénztovábbítási rendszereit, az elektronikus fizetőeszközöket és a Bitcoint használják, pénzügyi műveleteiket igyekeznek anonim módon végrehajtani.

A módszereket a pénzmosás során is alkalmazzák.

A cikk szerzője az ezekben rejlő kockázatokat tárja fel.

The terror attacks of September 11. 2001 (9/11) did not only mean the start of a new era in the history of terrorism but also the initiation of new methods against it and the implementation of the available strategies more effectively.

Detecting of the financial background of terrorism and the initiation of making the funding impossible on international levels received special attention.

In response, terrorists have returned to the traditional money transferring methods of hawala, and use modern money transferring systems, electronic payment methods, and Bitcoin. They are trying to carry out their financial transactions anonymously.

These methods are being applied in money laundering as well.

The author of this article reveals the risks of the above-mentioned strategies.

BEVEZETÉS

A 2011 szeptemberi terrortámadások alapjaiban megváltoztatták a terrorizmus elleni harcot. Mind a politikai és katonai, mind a rendészeti összefogás világméretűvé vált. A közös ellenséggel egyesített erővel kell szembenézni. Ez a küzdelem mind a gondolkodásmód, mind a fellépés stratégiai súlypontjainak megváltozását eredményezte. Egyfelől megkezdődtek a nagy méretű katonai műveletek, másrészről előtérbe került egy erősebb törekvés a terrorizmus anyagi bázisának megszüntetésére, finanszírozásának lehetetlenné tételére.

A globalizáció egyik legfontosabb „sajátossága a gazdasági folyamatok, a különböző gazdasági tevékenységek virtualizálódása, másképpen elektronizálódása."[1]

Ezzel párhuzamosan – ugyan némileg megkésve – a banki és pénzforgalmi tevékenység ellenőrzése megszigorodott, s erre a terroristák és a bűnözők is reagáltak.[2] Ezek a szervezetek egyrészt pénzeik gyors és „láthatatlan" továbbítására visszanyúltak a tradicionális *havala*[3]-rendszerhez, másrészt fizetéseiket, beszerzéseiket internetes, anonimizált pénzutalási módszerek segítségével (Bitcoin,[4] Ukash, Paysafecard[5]) eszközlik, kihasználva a digitális világ, az internet

[1] Rostoványi Zsolt: A terrorizmus és a globalizáció, In: Válaszok a terrorizmusra, Chartapress Kiadó, Budapest, 2002, p. 72

[2] Az egyszerűség kedvéért a bűnszervezeteket ebben a tanulmányban nem tárgyalom elkülönítetten a terrorszervezetektől. Ugyan céljaikban, struktúrájukban, tevékenységükben különböznek egymástól, finanszírozás szempontjából ezúttal azonosként kezelem őket, szükség szerint kihangsúlyozva a különbözőségeket.

[3] Havala: Bizalomra és személyi kapcsolatrendszerre épülő alternatív pénztovábbítási rendszer.

[4] Bitcoin: Nem hivatalos, virtuális pénz.

kínálta lehetőségeket.[6] A mobiltelefonhálózattal összekötött pénzügyi szolgáltatások rendszere új dimenziót ad az anonimitásnak és a mobilitásnak az illegális felhasználók számára.

Nagyon fontosnak tartom leszögezni, hogy a bemutatandó rendszerek mindegyikét *legális* felhasználásra tervezték. Törvénybe ütköző célokra történő alkalmazásukkal ugyan a felhasználók töredéke foglalkozik, a tanulmány célja éppen ezért az, hogy az *illegális tevékenység*ben rejlő bűnügyi potenciálra, s az ezzel kapcsolatos nemzetbiztonsági kockázatokra hívja fel a figyelmet.

A terrorizmus finanszírozásának lehetséges forrásai lehetnek:[7]

- állami finanszírozás;[8]
- a terrorszervezet legális üzleti tevékenységéből származó bevételek;
- illegális bevételek, szervezett bűnözői csoportokkal való együttműködésből (például emberrablás, embercsempészet, kábítószer előállítás, -értékesítés, csempészet, fegyverkereskedelem);
- egyesületektől, egyházaktól érkezett adományok;
- radikalizálódott diaszpórában érkezett adományai;
- zakát;[9]
- interneten történő csalások, zsarolások.

A felsorolásból látható, hogy a pénz zöme kis összegekből tevődik össze. Ezen pénzösszegeknek kell a rendeltetési/felhasználási helyükre megérkezni. A terrorista tevékenységgel kapcsolatos kiadások nagysága is változatozó. Az egészen ki tételektől kezdve egészen a hatalmas beruházásokig, eszközvásárlásokig.[10]

A HAVALA-RENDSZER[11]

A havala a korai középkor tradicionális vallási értékeire épülő, személyes kapcsolatokon és a bizalmon alapuló informális pénztovábbítási rendszer. Lényege, hogy két, általában különböző országban levő személy vagy vállalkozás között teremti meg a pénzek továbbítását, akár perceken belül. Mivel a bankrendszeren kívül működik, ezért olyan országokban is alkalmazható, ahol hiányzik, vagy nem megbízhatóan funkcionál a bankrendszer.

Működési elve a következő: az „A” országban tartózkodó X. személy pénzt akar küldeni „B” országban élő családjának (Y nevű hozzátartozójának). X megkeres egy havalabrókert, odaadja neki a pénzt és az továbbítási jutalékot. A havalabrókertől kap egy kódot, amit X elmond Y-nak. Eközben a havalabróker tájékoztatja „B” országban dolgozó havalabróker-kollégáját a kifizetendő összegről és a kódról. Y felkeresi „B” országban az adott havalabrókert, akinek elmondja a kódot, és megkapja a küldött összeget.

---

[5] PAYSAFECARD, Ukash: Elektronikus fizetőeszközök.
[6] Katona László: A terrorizmus és a szervezett bűnözés elhatárolásának aktuális dilemmái, Felderítő Szemle, XII. évfolyam 3. szám, 2013. december, p. 69.
[7] Felsorolás a NATO-Rewue alapján. Forrás: http://www.nato.int/docu/review/2007/issue2/hungarian/analysis2.html (Letöltés: 2013. október 05.)
[8] Ezen tanulmánynak nem témája, az azonban már most biztosan megállapítható, hogy a 2014-ben kezdődött és jelenleg is tartó orosz-ukrán konfliktus nemcsak az *állami terrorfinanszírozás fogalmát*, de a terrorizmusról általánosságban alkotott képet is átírja. Az aktuális történések későbbi elemzése átértékelheti a *szeparatista, szakadár, terrorista* fogalmakat is, ezek fizikai megjelenési formáit az ukrajnai aszimmetrikus hadviselésben, valamint szükségszerű kapcsolatukat a reguláris katonai műveletekkel, illetve az azzal történő fenyegetéssel.
[9] zakát: az iszlám vallásgyakorlók által kötelezően fizetendő adó
[10] Ide soroljuk a terrorszervezetek, terrorista akciók bármilyen jellegű anyagi támogatását, valamint a terrorista tevékenységet támogató illetve abban részt vevő személyek anyagi támogatását. Ez lehet pénzügyi részesedés, készpénz(számla), biztosítás(ok), betét (lekötés). Forrás: Wesley J. L. Anderson: Disrupting Threat Finances: Utilisation of Financial Information to Disrupt Terrorist Organisations in the Twenty-First Century, School of Adwanced Military Studies, Kansas, 2007. p. 8.
[10] Felsorolás a NATO-Rewue alapján. Forrás: http://www.nato.int/docu/review/2007/issue2/hungarian/analysis2.html (Letöltés: 2013.október 05.)
[11] Tekintettel arra, hogy a havala-rendszerrel egy korábbi tanulmányomban részletesen foglalkoztam, itt csak a tevékenység összefoglalása olvasható. Eredeti cikk: Katona László: A terrorizmus finanszírozása, In: A Hadtudomány és a 21. század Konferenciakötet, Budapest, 2014., pp. 135-149

A művelet visszafelé ugyanúgy működik. Pénzek lényegében nem mozognak az országhatárokon. A havalarendszerrel árut is ugyanúgy ki lehet fizetni. Ekkor „A" országból az áru elindul „B" országba, a vevő pedig érkezéskor a helyi havalabrókernek adja a vételárat. Ezt az összeget veszi át „A" országban az eladó az ottani havalabrókertől.

Ezt a rendszert nemzetközi szinten tevékenykedő bűnszervezetek (például kábítószertermelők, -kereskedők) a mai napig használják.

A rendszer előnyei: az első az igen *kedvező ár*. Nincsenek banki, illetve átváltási költségek. A havalabróker tevékenysége *bürokráciamentes*, nem üzemeltet irodaházakat, egyéb infrastruktúrális hálózatot. Általában irodája sincs, legtöbbször kávézókban feltalálható, más esetben valamilyen legális, viszonylag kis befektetést igénylő üzleti vállalkozása mellett (például gyrossütő vagy más vendéglátóipari egység, fodrászüzlet, kisközért, internet-kávézó) fejti ki havalabrókeri tevékenységét. Technikai eszköz-igénye egy (mobil)telefonra, telefaxra, esetleg egy számítógépre terjed ki.

A *havalaügylet rendkívül gyorsan* (általában 24-48 órán belül, vagy akár ennél is hamarabb) *intéződik*, nem kell figyelembe venni hétvégi banki szünnapokat, ünnepnapokat, eltérő időzónákat.

A banki rendszerekben időnként „eltűnik" a pénz, aztán valamikor megtalálják, illetve egyes országokba történő utalásnál közvetítőbankokat kell igénybe venni,[12] ami irreálisan meglassítja a folyamatokat. Ezzel szemben a havalabrókerek ismerik egymást, megbíznak egymásban, a pénz útja akadálymentes akár a legeldugottabb szomáliai faluban is megkapja a pénzét a címzett. A *bizalom* fontos összetevője a rendszenek, ám ez is a tradicionális törvényeken alapul. Egyes országokban még napjainkban is kézlevágás lehet annak a büntetése, aki lop.

Mindezekből következik, hogy a hiányzó nehézkes, körülményes adminisztrációs háttér sem „nyomasztja" a havala használóit. A *rendszer nem kívánja meg bankszámla nyitását*, a pénz eredetét sem firtatja.

Nem elhanyagolható a *kulturális faktor* sem. Számos európai nagyvárosban élnek olyan ázsiai, illetve afrikai kolóniák, amelyek – gyakran nyelvtudás hiánya vagy kulturális különbségek miatt – egyáltalán nem tudják és nem is akarják a nyugati bankokat felkeresni. A tradicionális vallási értékek szerint élő nők, feleségek is minimális kapcsolatot ápolnak a környezetükkel. Számukra is kézenfekvő megoldás a havalabrókereken keresztüli pénzküldés.[13]

A havala legális felhasználóinak szempontjából nem elsődleges szempont, de aki bűnös szándékkal alkalmazza annak a legfontosabb a *havala anonimitása*.

Összességében megállapítható, hogy a havala *rendkívül felhasználóbarát*.

BITCOIN

A Bitcoin[14] egy digitális pénz, mely gyors és biztonságos lehetőséget nyújt személyek közötti átutalásra vagy áruk, szolgáltatások megfizetésére. Rövidítése: BTC, alapja a Bitcoin-rendszer. Jelentősége abban rejlik, hogy ez a világ első teljesen decentralizált digitális fizetőeszköze.[15] Ez a rendszer teljesen alkalmas illegális pénzek anonim átutalására,

[12] Ha például Magyarországról Ugandába szeretne valaki utalni, igénybe kell venni egy közvetítő bank szolgáltatását. Ez a banki költségeket és a tranzakció lebonyolításának időtartamát mindjárt a többszörösére növeli.
[13] The World Bank And The International Monetary Fund: Informal Funds Transfer Systems: An Analysis of the Informal Hawala System (a Világbank és az IMF közös kiadványa, 2003. március 21.) http://www-wds.worldbank.org/servlet/WDSContentServer/WDSP/IB/2003/05/03/000094946_03041904002082/Rendered/PDF/multi0page.pdf (Letöltés: 2013. szeptember 04.)
[14] A Bitcoin egy nyílt forráskódú digitális fizetőeszköz, amelyet 2009. január 3-án egy ismeretlen (fórum nevén Satoshi Nakamoto) bocsátott ki, közvetlenül a 2008-as amerikai bank válság kirobbanása után. Az elnevezés vonatkozik továbbá a fizetőeszközt kezelő nyílt forráskódú szoftverre, és az azzal létrehozott elosztott hálózatra is. A Bitcoin a peer-to-peer hálózat csomópontjai által tárolt elosztott adatbázisra támaszkodik. Az adatbázis tartalmazza a fizetések adatait, garantálva az elektronikus fizetőeszközökkel szembeni alapvető követelményeket. Forrás: http://hu.wikipedia.org/wiki/Bitcoin (Letöltés: 2014.február 05.)
[15] Jerry Brito a George Mason Egyetem Mercatus Center vezető kutatója, legfőbb kutatási területe a Bitcoin. Bitcoin A Primer for Policymakers, p. 3, Forrás: http://mercatus.org/sites/default/files/Brito_BitcoinPrimer_embargoed.pdf (Letöltés: 2014. február 06.)

ebben a tekintetben terrorfinanszírozással kapcsolatos pénzek mozgatására, valamint pénzmosásra.[16] Működésére a peer-to-peer (P2P) alkalmazás jellemző,[17] ily módon – a többi elektronikus fizetőeszköztől eltérően – nem köthető kormányokhoz illetve (jegy)bankokhoz.

Jelen tanulmánynak nem témája a Bitcoin-rendszer működésének bemutatása,[18] csak a nemzetbiztonsági szempontból jelentős elemeket emelem ki, és az azokban rejlő kockázatokra hívom fel a figyelmet.

A Bitcoin egy összetett kriptografikus jel, mely egy virtuális pénztárcában tárolható a számítógépen (vagy okostelefonon). Ez a jel a keletkeztetésekor (Bitcoin-bányászat) a Bitcoint használó valamennyi személy számítógépre elküldésre kerül. A kriptografikus jelek (most már Bitcoinok) egy lánc[19] részeiként ettől a pillanattól – a nyílt forráskódú rendszernek köszönhetően – bármikor megkereshetőek, visszaellenőrizhetőek.

A Bitcoin használata leegyszerűsítve: valaki egy másik személynek pénzt akar utalni. Ha ezt a Bitcoin-rendszeren keresztül teszi, akkor ez az utalás megtörténhet nagyon gyorsan, közvetlenül, anonim módon és ingyenesen.[20] A virtuális pénztárcájából e-mailen elküldi a Bitcoinját jelentő kódolt jelet. A tranzakció ebben a pillanatban visszafordíthatatlanul lezajlott, a Bitcoin új helye az interneten visszakövethető.

Számos üzlet is elfogadja a Bitcoint, mint fizetőeszközt, míg a kormányok hozzáállása változó. Az országok egy része – a nemzeti, központi banki kibocsátás hiánya miatt – nem tartja pénznek, más ország magánpénznek definiálja, megint másik – éppen a szabályozás hiánya miatt – nem tiltja.[21] Valamennyi ország azonos álláspontot foglal el abban a tekintetben, hogy bizonyos potenciális veszélyforrást jelent a Bitcoin megjelenése és terjedése.

A Bitcoin-rendszer biztonsági kockázatai szembeötlőek. A rendszer anonimitást ígér felhasználóinak, ami több ponton is realizálódik. A Bitcoin-tranzakció mindkét résztvevője névtelenségben tud maradni. A virtuális pénztárca programokat számos cég kínálja, letöltésük számítógépre vagy okos telefonra installálhatóak, alkalmazásuk ingyenes. Ezek a programok azonnal 5-8 darab különböző pénztárcát nyújtanak, de ez a továbbiakban a végtelenségig bővíthető. Megtehető, hogy valaki minden egyes Bitcoin tranzakcióját más és más virtuális pénztárcából kezdeményezze, illetve fogadja. Feltételezve a felhasználó „megfelelő" számítógépes titkosítási ismereteit (és a tranzakciók nagy számát), a továbbiakban nem visszakereshető. Kizárólag abban az esetben azonosítható a felhasználó, ha például sportszerüzletként, nyilvános címmel és email-címmel folytat adásvételt Bitcoinok felhasználásával. Ha ennek a cégnek egy hétköznapi vásárló például egy kerékpárért Bitcoinnal fizet, akkor beazonosítható, hogy az X kódjelű Bitcoint XY küldte a sportboltnak.

Azok a személyek, szervezetek, akik a Bitcoint tehát illegális tevékenység finanszírozására, illetve pénzmosás során használják fel, kezdeményezhetnek vele utalásokat, kaphatnak pénzt, fizethetnek eszközökért, szolgáltatásokért, illetve egyszerűen diszlokálhatják a pénzt más felhasználási helyre. A pénzmosás folyamatában leginkább ez utóbbi a jellemző.

Miután a Bitcoin a rendeltetési helyére került, át lehet váltani lényegében bármely más hivatalos pénzre. Természetes, hogy az átváltásnak is van hivatalos és illegális módja.

Számos elektronikus szolgáltatás, adat, információ is átváltható Bitcoinra, vagy közvetlenül pénzre. Ilyenek lehetnek elektronikus, online játékok hozzáférései, egyéb elektronikus információk, valamint ezen alkalmazásokban (játékokban)

[16] Letartóztatták a Bitcoin Alapítvány alelnökét, Forrás: http://hvg.hu/tudomany/20140128_Letartoztattak_a_Bitcoin_Alapitvany_aleln (Letöltés: 2014. április 05.)
[17] A peer-to-peer rendszer lényege, hogy az informatikai hálózat végpontjai közvetlenül egymással kommunikálnak, központi kitüntetett csomópont nélkül. Forrás: http://hu.wikipedia.org/wiki/Peer-to-peer (Letöltés: 2014. február 06.)
[18] A Bitcoin működésével kapcsolatos ismeretek a www.bitcoin.hu oldalon összegyűjtve elolvashatóak.
[19] A lánc neve: blockchain, összegyűjtő portálja: http://blockchain.info/hu.
Ezen az oldalon a Bitcoinnal kapcsolatos tranzakciók ellenőrizhetőek, statisztikák, átváltási kurzusok olvashatóak.
[20] Egy 0.01 BTC nagyságú önkéntes utalási díj esetén a tranzakció felgyorsítható.
[21] http://en.wikipedia.org/wiki/Legality_of_Bitcoins_by_country (Letöltés: 2014. május 05.)

létező virtuális pénzek is bizonyos árfolyamon valódi pénzre válthatóak (World of Warcraft, egyéb MMORPG[22]-ok). Érzékelhető tendencia, hogy egész iparági szegmens épül(t) arra, hogy elektronikus, fizikai valóságban nem létező, kézzel nem fogható információk, adatok kerülnek előállításra és valódi pénzben történik értékesítésük. Az eljárásban megtalálható a fentiekben is leírt „visszaélési" lehetőség, azaz nem tudható, hogy kik, melyik országban dolgoznak az információ előállításán, mely gépek végzik a számításigényes feladatokat, ezek ily módon elfedhetőek.

AZ ELEKTRONIKUS PÉNZ

Elektronikus pénz: készpénz-helyettesítő fizetési eszköz, az elektronikus pénz kibocsátójával szembeni követelés által megtestesített, elektronikusan tárolt – ideértve a mágneses tárolást is – összeg, melyet pénzeszköz átvétele ellenében bocsátanak ki a pénzforgalmi szolgáltatás nyújtásáról szóló törvényben meghatározott fizetési műveletek teljesítése céljából, és amelyet az elektronikus pénz kibocsátóján kívül más természetes és jogi személy, jogi személyiség nélküli gazdasági társaság és egyéni vállalkozó is elfogad. Nem minősül elektronikus pénznek az e törvény 2. *számú melléklet* I. fejezete 9.1. pontjának *k)* alpontja szerinti eszközön tárolt vagy *l)* pontjában rögzített fizetési műveletekre használt érték.[23]

Az elektronikus pénzek az egész világon terjedőben vannak. A velük kapcsolatos kezdeti ellenszenv és idegenkedés, mely leginkább a vásárlásokkal járó többletköltség és a bizalmatlanság miatt alakult ki, mára alábbhagyott.

Az elektronikus pénzek közös jellemzője, hogy mögöttük minden esetben valamilyen pénzintézet vagy központi szolgáltató van. Az elektronikus pénzeket egy elektronikus pénztárcában kell tárolni. Ennek megjelenési formája lehet valamilyen mágneses/elektronikus adathordozó, vagy akár egy kódszám. Kiadása kiterjedhet az egész világra (ahol ezt elfogadják),[24] vagy csak bizonyos földrajzi területre,[25] esetleg üzleti elfogadóhelyre.[26] Jelentős részük on-line, tehát elfogadóhelyi banki kapcsolat szükséges hozzá, más részük off-line, ezeket egyszer kell megvásárolni, utána szükség szerint felhasználhatóak.[27] Az elektronikus pénztárcákhoz általában számla kapcsolódik.[28] A számlához nem kötött szolgáltatások személyhez sem kapcsolódnak, ebben az esetben a fizetést az elektronikus adathordozó birtoklása teszi lehetővé.[29]

A mögöttes szerződéses feltételek alapján az elektronikus fizetés – a tranzakció időbeni sorrendje szerint – lehet előre fizetett (prepaid), azonnal fizetett (direct paid) és utólag fizetett (postpaid) elektronikus pénz.[30]

Az elektronikus pénzek csoportosításában több területen átfedés tapasztalható.

Az áttérés a készpénzforgalomról a készpénzt helyettesítő eszközökre a hatóságoknak is lehetőséget biztosít arra, hogy szinte valamennyi felhasználó összes tranzakcióját figyelemmel kísérjék. Ily módon fény derülhet adóelkerülésre, pénzmosásra, illegális tevékenységek finanszírozására, keresett személyek támogatására, cégek, személyek közötti kapcsolatokra, vagy akár vásárlási szokásokra. Számos statisztika is készül az adatok felhasználásával.

---

[22] A MMORPG *(Massively Multiplayer Online Role-Playing Game – nagyon sok szereplős online szerepjáték)* interneten, online játszható szerepjáték. A nagyon sok szereplős online szerepjáték a számítógépes játékok azon műfaja, ahol nagyszámú játékos képes egymással kapcsolatot teremteni egy virtuális világban.
Forrás: http://hu.wikipedia.org/wiki/MMORPG (Letöltés: 2014. május 05.)

[23] 1996. évi CXII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról, 2. számú melléklet, 5.1 és 5.2 pont, Beiktatta: 2009. évi CL. törvény 57. §., Hatályos: 2010. január 01-től.

[24] Ilyen például a MasterCard vagy a Visa.

[25] Például: Magyarországon felhasználható Shell Smart kártya, vagy a feltölthető parkolókártya.

[26] Például: T-Mobile pontgyűjtő kártya.

[27] Például: Mobiltelefon-feltöltőkártya.

[28] Bankszámla kapcsolódik a bank- illetve hitelkártyákhoz, a többihez általában ügyfélszámla.

[29] KPMG Tanácsadó Kft.: Elektronikus fizetési megoldások, Gazdasági és Közlekedési Minisztérium részére készített tanulmány, 2007. április 13., p. 19

[30] Pétervári Kinga: Az elektronikus fizetés és az elektronikus pénz joga, p. 4, Forrás: http://www.academia.edu/1592735/E-penz_e-fizetes_2012 (Letöltés: 2014. május 02.)

A nagyszámú felhasználó azonban az illegális célú felhasználókat részben el is rejtheti, másrészt érzékennyé teheti őket az anonim lehetőségek kihasználására.

A kíbertér[31] többféle bűncselekmény elkövetésére is lehetőséget teremt a bűnözők és a terroristák számára:

- bizalmas banki ügyféladatok megszerzése (adathalászat);
- kutatási és biztonsági adatok, információk megszerzése;
- bűnüldöző hatóságok, rendvédelmi szervek szervereinek feltörése nyomozási információk megszerzésére;
- internetes zsarolások;
- közérdekű üzemek tevékenységének megzavarása, megbénítása;
- bankok, pénzintézetek tevékenységének megzavarása;
- illegális áruk adás-vétele;
- pénzmosás;
- rongálás, kártevés.

A felsorolt tevékenységek egy részének célja direkt módon a pénzszerzés, másik részük estében a motiváció az információszerzés, illetve más, politikai vagy katonai jellegű, esetleg terrorista célú támadó akciók végrehajtása.

Jelen tanulmány az elektronikus fizetési rendszerek közül az előre fizetett on-line fizetési eszközöket, az ezekkel történő bűnös célú tevékenységeket teszi vizsgálata tárgyává.

Számos cég kínálja előre megváltott on-line fizetőeszköz-rendszerét a piacon. Ezek közös jellemzője, hogy egy „kaparós" kártyán vagy egy kinyomtatott értékkártyán az ügyfél a vásárlás után kap egy kódot. Felhasználáskor ezt a kódot kell a megfelelő internetes felületen beírni, ezáltal megtörténik a fizetés. Miután a vásárló megvette az ilyen on-line fizetőeszközét – lévén, hogy nem kapcsolódik számlához, illetve személyhez – az szabadon átruházható, bárki által ellenőrzés nélkül felhasználható. Európában ezek közül legismertebbek többek között az Ukash és a PaySafeCard.

Ezen fizetési rendszerhez kétféle bűncselekmény is kapcsolódhat anonimitása miatt. Egyfelől alkalmas illegális célok anyagi támogatásra, így terrorista akciók finanszírozására, terrorszervezetekhez kapcsolódó személyek tagjainak anyagi bázisának megteremtésére.

Másik – igen elterjedt – kriminális jelenség az internetes zsarolások alkalmával a zsarolt összegnek a sértettel ily módon történő kifizettetése. Az eredetileg Oroszországból származó, de időközben az egész világon elterjedt rosszindulatú számítógépes vírus (ransomware) blokkolja a számítógépet, miközben a képernyőn egy hivatalosnak látszó üzenet jelenik meg.[32] Ebben az üzenetben figyelmeztetik a felhasználót, hogy gépével illegális tartalmat töltött le (általában pornográf tartalom letöltésével vagy szerzői jogokkal kapcsolatos bűncselekményeket sorolnak fel) és közlik, a számítógépet egy összeg megfizetése után, büntető feljelentés megtételét mellőzve ismét feloldják, használhatóvá teszik. A Windows-képnek csak egy felülete használható, ahová be kell írni az előre megváltott PaySafeCard, MoneyPak vagy Ucash on-line fizetőeszközt. A vírust az on-line elektronikus pénz szolgáltató nevei alapján PaySafeCard, Ucash vagy MoneyPak[33] vírusnak hívják, de a Windows-képben megjelenő bűnüldöző hatóság neve alapján is elnevezték. Ily módon az alábbi elnevezések fordulnak elő leggyakrabban: Nemzeti Védelmi Szolgálat vírus, Nemzeti Nyomozó Iroda vírus, BKA (Bundeskriminalamt – Szövetségi Bűnügyi Hivatal – Németország) vírus, Metropolitan Police (Egyesült Királyság) vírus, FBI-vírus, stb. A szöveg magyar nyelvű változata nyelvtanilag nem helyes,[34] innen is gyanítható, hogy nem hivata-

[31] *globális kibertér:* a globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttese; 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról 1. § (1) 22.

[32] http://yszerviz.hu/cikkek/rendorsegi-virus-eltavolitasa/ (Letöltés:2014. május 02.)

[33] MoneyPak: Egyesült Államokban elterjedt on-line prepaid fizetőeszköz.

[34] „FIGYELEM! A számítógépe meg van blokkolva a biztonsági megfontolásokból a következő okok miatt. *Önt vádolják a tiltott tartalmú pornográf anyagok megtekintésével/tárolásával és/vagy terjesztésével gyermekpornográfia/bestialitás/nemi erőszak, stb.). Ön megsértette A gyermekpornográfia terjesztése elleni küzdelemről szóló Nemzetközi Nyilatkozatot,*

los szervtől érkezett üzenetről van szó. Bűnüldözési hatóság nem blokkol számítógépet (technikailag nincs is rá szüksége számítógéppel elkövetett bűncselekmény bizonyításához), az pedig nem fordulhat elő, hogy a bűnüldözési kényszerről lemond a hatóság egy relatíve kisebb összeg megfizetésének fejében. 2013-ban a Budapesti Rendőr-főkapitányság sajtóközleményben hívta fel a vírusra a figyelmet.[35]

A vírus, melynek időközben többféle változata létezik, a pénz átutalása után nem oldja fel a gépet (ezt nem is tudja a program). Az eltávolítás egyébként házilag is elvégezhető.

Legfontosabb különbség a Bitcoin és az e-készpénz között, hogy míg utóbbi egyszer használható fel, addig a Bitcoin a vásárlás/elküldés után (virtuálisan) megmarad, új tulajdonosánál a továbbiakban fellelhető.

A MOBILTELEFON-HÁLÓZATTAL ÖSSZEKAPCSOLT FIZETÉSI RENDSZEREK

A mobiltelefon-hálózathoz kötött fizetés az elektronikus készpénzek közé tartozik. A SIM-kártya és a hozzá tartozó hívószám mögött egy számla (nem bankszámla) van. Az e-pénztárca maga a mobiltelefon, akinek ez birtokában van, az tud vele vásárolni. Az előfizetéses ügyfelek általában utólag fizetik a megvásárolt termékek ellenértékét, oly módon, hogy az eredeti eladóval a mobiltelefon-hálózat üzemeltetője áll szerződésben, a vevő neki téríti meg utólag az összeget, ő fizeti aztán tovább az eredeti eladónak. Ez a rendszer előnyös az eladónak, ugyanis ő a mobiltelefon-szolgáltatótól mindenképpen megkapja a termék vagy szolgáltatás árát, és a mobiltelefon-szolgáltatónak is kedvező, mert a vevő mobiltelefonja a késedelmes fizetés (vagy nemfizetés) esetén letiltható, részletre vásárolt készüléke blokkolható, stb. Végső soron az ügyfél telefonszámlájával egyidejűleg fizeti meg a termék vagy szolgáltatás árát is.

Kártyás ügyfelek a feltöltött (előre befizetett) összeg erejéig jogosultak mobil fizetésre vagy vásárlásra.

Jelenleg hazánkban a megvásárolható termékek és szolgáltatások köre igen szűk. A mobiltelefonálással összefüggő eszközökön kívül legelterjedtebb az autópálya-matrica és közterületi parkolási díj mobiltelefonnal történő megfizetése, valamint ide tartoznak az emelt díjas szolgáltatások (interneten történő hirdetések, internetes tartalmak letöltése, on-line szerencsejáték) igénybevételével kapcsolatos kiadások is. Néhány bank és kártyakibocsátó is kínál mobilfizetési szolgáltatást, ám ebben az esetben az ügyfélnek rendelkeznie kell bankszámlával és bankkártyával, ezáltal a mobiltelefonja gyakorlatilag a POS-terminált és a bankkártyát helyettesíti fizetés esetén.[36]

A mobiltelefon-hálózatra épülő elektronikus fizetési szolgáltatások azokban az országokban fejlődtek leggyorsabban, amelyekben nincs kialakult bankrendszer. Ilyen országok jellemzően az afrikai államok, Kenya, Tanzánia, Uganda,[37]

és Önt vádolják a Magyarország Büntető Törvénykönyve 161. cikkében meghatározott bűncselekmény elkövetésével. Magyarország Büntető Törvénykönyve 161. cikke büntetésként meghatározza a 5 és 11 év közötti szabadságvesztést. Önt szintén gyanúsítják 'A szerzői és szomszédos jogokról szóló törvény'-t megsértésében (a kalózzene, videó, nem engedélyezett szoftver letöltése) és a szerzői joggal védett tartalom felhasználásában és/vagy kiterjesztésében. ugyanaz! Önt gyanúsítják a Magyarország Büntető Törvénykönyve 148. cikke megsértésében.
Magyarország Büntető Törvénykönyve 148. cikke büntetésként meghatározza a 150 és 550 alapegység közötti bírságot vagy a 3 és 7 év közötti szabadságvesztést. Az Ön bírsága összege HUF 25000 (Ft) magyar forint. A bírságot voucherekkel PaySafeCard fizetheti. Miután kifizeti a bírságot, és a pénz kerül az állam számlájára, a számítógépét szabaddá teszik 24 órán belül. Ezek után meg van kötelezve 7 napon belül eltávolítani minden megsértést, amely meg van kapcsolva az Ön számítógépéhez. Amennyiben a megsértések nem lesznek távolítva, az Ön számítógépe újra lesz blokkolva, és Ön ellen büntető eljárást fogják indítani (a bírság fizetésének a lehetősége nélkül).Felhívjuk figyelmét, hogy érvényes pénz voucherek kódjait be kell vezetnie a bírság fizetésénél, és nem váltani készpénzzé a bevezetett vouchereket fizetés után. A pénz voucherek helytelen kódjai bevezetése esetén vagy a pénz voucherek megszüntetési kísérlete esetén a fizetés után, ráadásul a fent említett megsértésekhez Önt fogják vádolni a csalással (Magyarország Büntető Törvénykönyve 301. cikke; a megadott cikk meghatározza az 1 és 3 év közötti szabadságvesztést), és Ön ellen büntető eljárást fogják indítani."

[35] http://www.police.hu/hirek-es-informaciok/bunmegelozes/aktualis/interneten-terjedo-csalas (Letöltés: 2014. május 02.)
[36] http://mc-mobile.hu/hogyanhasznalhatod.html (Letöltés: 2014. május 03.)
[37] http://www.somalilandmonitor.com/index.php/opinion/356-somaliland-mobile-money-in-a-dusty-land (Letöltés: 2014. május 05.)

Szomália, illetve a Közel-Kelet, Irak és Afganisztán. A két legelterjedtebb hálózat az M-Pesa,[38] melyet Kenya felnőtt lakosságának mintegy nyolcvan százaléka használ[39] és a szomáliai Zaad.[40]

Ezek a rendszerek eredetileg a mikrohitelek visszafizetésére lettek létrehozva, használatuk csupán egy regisztrációhoz kötött. Ezután a felhasználó küldhet pénz magánszemélynek vagy cégnek, fizethet vele, kis kioszkokban feltöltheti, és pénzt is vehet fel (1. számú fénykép).

1. számú fénykép: M-Pesa kioszk Ugandában (A Szerző gyűjteményéből)

SIM-kártyához (akár többhöz) bárki hozzájuthat, ezután a pénzeket ellenőrzés nélkül utalhatja, illegális tevékenységet finanszírozhat, illetve kifizethet vele például hadianyagokat. A Zaad ugyan jelenleg a személynek történő utalást 500, a vásárlást 2.000 amerikai dollárban maximálja, de a terrorista akciók költségéhez mérten ezek is bőségesen elegendő összegek.

Az M-Pesa időközben már megtakarítási ajánlatot is kidolgozott, s olcsó, felhasználóbarát működésének köszönhetően gyorsan terjed a világban, sőt – az egyébként viszonylag alacsony szintű mobil bankolási kultúrával rendelkező – Romániában történő 2014. márciusi bevezetéssel már Európába is megérkezett.

Ország	*Indulás időpontja*	*Szolgáltató*	*Termék neve*
Kenya	2007. március	Safaricom	M-Pesa
Tanzánia	2008. április	Vodacom	M-Pesa
Fidzsi	2010. július	Vodafone	M-Paisa
Dél-Afrikai Köztársaság	2010. augusztus	Vodacom	M-Pesa
DRC	2012. november	Vodacom	M-Pesa
India	2013. április	Vodafone	M-Pesa
Mozambik	2013. május	Vodacom	M-Pesa

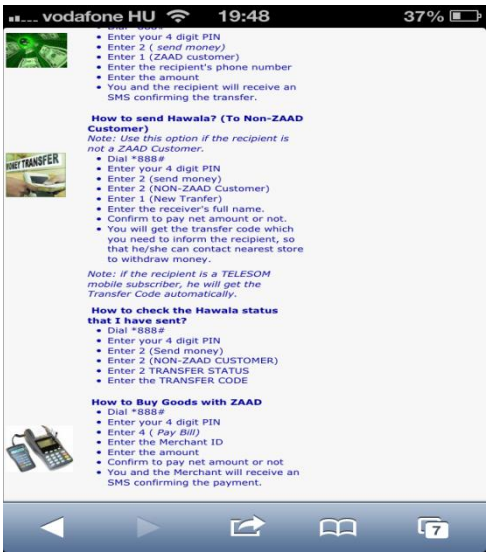
[38] M: a mobiltelefonos alkalmazásra utal, Pesa: szuahéli nyelven *pénz*t jelent.
[39] http://www.economist.com/news/finance-and-economics/21574520-safaricom-widens-its-banking-services-payments-savings-and-loans-it (Letöltés: 2014. május 26.)
[40] 2010-as adat szerint Szomália lakosságának egyötöde használta fizetésre és utalásra, és ennél többen kaptak pénzt, vagy kerültek más módon kapcsolatba a Zaad-dal.
Forrás: http://www.somalilandmonitor.com/index.php/opinion/356-somaliland-mobile-money-in-a-dusty-land
(Letöltés: 2014. május 02.)

Egyiptom	2013. június	Vodafone	Vodafone Cash
Lesotho	2013. július	Vodacom	M-Pesa
Románia	2014. március	Vodafone	M-Pesa

1. számú ábra: Az M-Pesát használó országok

Forrás: http://www.vodafone.com/content/index/about/about-us/money_transfer.html (Letöltés: 2014. május 05.)

A szomáliai Zaad mobiltelefonos rendszere fokozza a leginkább az átláthatatlanságot: segítségével havala küldést is lehet kezdeményezni, illetve ellenőrizni lehet vele a havala státuszát.



2. számú fénykép: a Zaad havala-küldő és státusz-ellenőrző mobiltelefonos felülete

(a Szerző gyűjteményéből)

Mindkét hálózat képes a rendszeren kívüli ügyfelekkel történő tranzakciók lebonyolítására is.

ÖSSZEGZÉS

Az általam röviden bemutatott rendszerek – mint azt a bevezetésben is leszögeztem – legális pénzküldési és –fizetési célokra lettek létrehozva, azonban anonim vagy anonim módon megszerezhető mivoltuk miatt komoly veszélyt jelentenek, amennyiben illegális célokra kerülnek felhasználásra. A felderítés szempontjából fontos a technikai fejlődés követése, a rendszerek működésének megismerése, az esetleges biztonsági rések feltárása, valamint az online jelenlét ezen rendszerekben, alkalmazásokban, közösségekben.

Egy rendszer illegális célokra történő felhasználása mindig egy biztonsági deficit nyújtotta lehetőséggel kezdődik. Egy fejletlenebb biztonsági és ellenőrzési rendszerrel rendelkező ország bankjában fizethet be illegális pénzt az, aki pénzmosással vagy terrorfinanszírozással foglalkozik, de erre off-shore cégeken keresztül is lehetőség nyílik. A SIM-kártyához jutás is könnyű azokban az országokban, ahol ennek nincs meg a hatékony ellenőrzési háttere. Ha pedig a

rendszerbe bekerült egy bankszámla, vagy már az illegális pénzösszeg, akkor a tranzakciók sokasága miatt valószínűleg csak a végrehajtott tranzakciók utólagos értékelésére kerülhet sor. Nincs szükség az elektronikus pénz valós pénzre történő visszaváltására sem,[41] mert a világ másik pontján már lehet is vele vásárolni az interneten például nagy értékű festményt vagy részvénycsomagot.

Másik lehetőség a HUMINT-tevékenység[42] fokozása ezen a területen. Mind az informális pénztovábbítási módszerekről, mind a digitális pénzről és az elektronikus pénzhelyettesítő eszközökről (amennyiben használatuk direkt módon az anonim lehetőségeket célozza) csak akkor juthatnak a felderítő hatóságok hiteles és naprakész információkhoz, ha megfelelő hatékony együttműködőket alkalmaznak. Az így beszerzett információk egyrészt orientálják a felderítést konkrét bűncselekményekhez vagy elkövetőkhöz, amelyekre a továbbiakban más eszközökkel is lehet irányítani, másrészt bemutathatnak olyan legális lehetőségeket, amelyek a jövőben esetlegesen potenciális veszélyforrást jelenthetnek.

Kulcsszavak: terrorizmus, terrorizmus finanszírozása, pénzmosás, elektronikus készpénz, Bitcoin, havala

Keywords: terrorism, the funding of terrorism, money laundering, electronic cash, Bitcoin, hawala

FELHASZNÁLT IRODALOM

1. Rostoványi Zsolt: A terrorizmus és a globalizáció, In: Válaszok a terrorizmusra, Chartapress Kiadó, Budapest, 2002.
2. Pétervári Kinga: Az elektronikus fizetés és az elektronikus pénz joga, Forrás: http://www.academia.edu/1592735/E-penz_e-fizetes_2012 (Letöltés: 2014. május 02.)
3. Katona László: A terrorizmus és a szervezett bűnözés elhatárolásának aktuális dilemmái, Felderítő Szemle, XII. évfolyam 3. szám, 2013. december, pp. 60-73.
4. KPMG Tanácsadó Kft.: Elektronikus fizetési megoldások, Gazdasági és Közlekedési Minisztérium részére készített tanulmány, 2007. április 13.
5. NATO-Rewue, Forrás: http://www.nato.int/docu/review/2007/issue2/hungarian/analysis2.html (Letöltés: 2013.október 05.)
6. Wesley J. L. Anderson: Disrupting Threat Finances: Utilisation of Financial Information to Disrupt Terrorist Organisations in the Twenty-First Century, School of Adwanced Military Studies, Kansas, 2007.
7. 1996. évi CXII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról
8. The World Bank And The International Monetary Fund: Informal Funds Transfer Systems: An Analysis of the Informal Hawala System (a Világbank és az IMF közös kiadványa, 2003. március 21.)
9. Lilley, Peter: Piszkos ügyletek – A pénzmosás világa, Budapest, 2001.
10. Nemzetbiztonsági alapismeretek, Szerk.: Kobolka István, Budapest, 2013.

[41] Lilley, Peter: Piszkos ügyletek – A pénzmosás világa, Budapest, 2001., p. 133
[42] HUMINT (HUMan INTelligence): a nemzetbiztonsági tevékenység azon eljárása, amelynek középpontjában az ember áll, akinek ismeretét, képességét a nemzetbiztonsági szolgálatok tervszerűen és szervezett formában használják fel. Forrás: Nemzetbiztonsági alapismeretek, Szerk.: Kobolka István, Budapest, 2013., p. 147

11. http://www-wds.worldbank.org/servlet/WDSContentServer/WDSP/IB/2003/05/03/000094946_03041904002082/Rendered/PDF/multi0page.pdf (Letöltés: 2013. szeptember 04.)

12. A Hadtudomány és a 21. század Konferenciakötet, Budapest, 2014.