Nagy Károly
PROTAN Informatikai Biztonsági Tanácsadó Rt.

A virtuális világok biztonsága*

A következő tíz évben a lokális virtuális világok létrehozása annyira elterjedtté válik, mint ma a televíziózás. Az új lehetőségek új kihívásokkal járnak. Gyökeresen új szemléletű megközelítésre van szükség. A virtuális világok alapfunkcióiból kiindulva lehet a kibertér biztonságfilozófiai alaptételeit megfogalmazni.

„Egy virtuális világban olyan környezetben vagyunk, amely tiszta információból áll, amit látunk, hallunk és érzékelünk. A technológia láthatatlan, és igazodik az emberi tevékenységhez, hogy természetesen viselkedhessünk. Megalkothatunk bármilyen képzeletbeli környezetet, és teljesen új perspektívákat és lehetőségeket tapasztalhatunk meg. A virtuális világ lehet tájékoztató, hasznos és vicces, de ugyanakkor unalmas és kényelmetlen is. A különbség a tervezésben van" [1].

Tágabb értelemben a *virtuális világok* egyidősek az emberi közösségi tudattal. Az ókori mitológia, a dráma, az egyéb művészetek, de akár a misztériumjátékok, vagy a shakespeare-i színház, a japán kabuki, majd később a film és a televíziózás mind-mind felfoghatók a virtuális világ megteremtésének egy-egy formájaként.

Az elektronika, a komputerizáció, a telekommunikáció fejlődése a virtuális világok létrehozásának új szakaszát nyitotta meg. Az új infrastruktúra bázisán teljesen új lehetőségek nyíltak. Megkezdődött a *tiszta információból álló* új virtuális világok globális integrációja. A globális számítógéphálózatokban végbemenő kölcsönhatások eredményeképpen megszületett a kibertér (cyberspace), a kibernetikus világegyetem.

A kibertér-technológia összekapcsolja a számítógép funkcióit az ember képességeivel. Ez azt követeli meg, hogy a technológiát hozzáigazítsuk az emberekhez. Így egyéni kölcsönhatásba kerülhetünk az információ egyedi formáival, ami kibővíti személyes intelligenciánkat, és szélesíti látókörünket.

A kibertérbe a lokális virtuális világokon keresztül kapcsolódhatunk be. Ennek a bekapcsolódásnak a lényege a következő – *Meredith Bricken* által kidolgozott – analógiával fejezhető ki. Egy háromdimenziós kép megjelenítése a képernyőn olyan, mintha az óceánt szemlélnénk egy üvegfenekű hajóról. A sík üvegen keresztül szemlélt megjelenített világ olyan élményt nyújt, mintha egy hajón lennénk.

A virtuális világot szemlélni sztereografikus képernyőn keresztül olyan, mint lemerülni egy tengeralattjáróval. A háromdimenziós környezet határán vagyunk, beleláthatunk az óceán mélységeibe, és az az érzetünk, mintha a víz felszíne alatt lennénk. Sztereoszkopikus virtuális sisakot (HMD-t) használva olyan érzésünk támad, mintha búvárfelszerelést viselnénk, és lemerülnénk az óceánba. Elmerülünk a környezetben: korallzátonyok mellett haladunk el, bálnák énekét hallgatjuk, kagylókat veszünk fel, és más búvárokkal érintkezünk, minden érzékünkkel érezhetjük a víz alatti világot.

Feltehető, hogy a bekapcsolódáshoz – akár mint a mozi, a televízió vagy egy regény esetében – egyáltalában nem szükséges a fenti analógia minden fokozatának a végigjárása. Egy dolog azonban bizonyos: tarthat a bekapcsolódás csak néhány másodpercig, vagy hosszú órákig, amíg a virtuális világban vagyunk, nem létezünk a fizikai világban.

A belépés mélysége az interfész környezet fejlettségétől függ. Az „adatkesztyűs" kapcsolat eredetileg egyirányú közvetítő funkciójától mára eljutottunk az aktív visszacsatolást biztosító interfész környezetekig. Ez a visszacsatolás nemcsak abban nyilvánulhat meg, hogy valamely „virtuális rózsakertben" sétálva érezhetjük a rózsák illatát, de akár az is lehetséges, hogy az adatkesztyűs kezünkkel megsimogatni kívánt „virtuális kutya" konkrétan a nadrágunkba harapjon.

A virtuális világok technológiája felhasználható a közvetlen érzékszervi kapcsolat, illetve tárgyi cselekvés nagy távolságokra történő kiterjesztésére is. Ily módon válik lehetségessé, hogy megfelelő interfészek alkalmazásával valamely nagy tudású sebész egy másik földrészen lévő műtőben fekvő emberen, vagy akár egy űrben keringő asztronaután műtétet hajtson végre.

---

* Elhangzott *Az Internet biztonsága* című konferencián (Kongresszusi Központ, Budapest, 1995. október 17.).

A virtuális világok változatossága igen nagy. Óriási hiba lenne ha a kibertérre bármilyen nagy számú konkrét, egyedi, virtuális világokhoz fűződő tapasztalatok alapján próbálnánk általánosító következtetéseket levonni. A probléma itt ugyanaz, mint amit a nagy matematikus, *Péter Rózsa* sokak által ismert példájában az alábbiak szerint világított meg: „Vannak, akik mindenre érvényes logikai elvnek tekintik, hogy a rész kisebb az egésznél. Íme egy ellenpélda:

1	2	3	4	5	6	7
10	20	30	40	50	60	70" [2].

Nyilvánvaló, hogy a felső sorban lévő természetes számoknak csak minden tizedik tagja (a tízzel maradék nélkül osztható természetes számok) szerepel az alsó sorban is, mindazonáltal bármilyen hosszan folytatjuk a felsorolást, mindig találunk párt a felső sorban szereplő számokhoz az alsó sor természetes számaival.

„Az ilyen általános logikai elveket (ti. a rész kisebb az egésznél) a tapasztalatok egész sokaságával vonta le az ember, de minden tapasztalat csak a végesben játszódhatott le. Sok zavarra vezetett már, hogy a végesben tapasztaltakból leszűrt elvet rá akarták húzni a végtelenre is" [2].

Ha a kibertér végtelen dimenzióit nem ragadhatjuk is meg, a virtuális világok alapfunkcióinak meghatározására mindenképpen kísérletet kell tennünk, hogy az utóbbiak biztonságáról értekezhessünk. A biztonság ugyanis alapvetően és kizárólagosan *rendszerfogalom*. Ez azt jelenti, hogy csak a rendszerként megalkotott (újra alkotott), a rendszerként lokalizált létezők biztonságával vagyunk képesek módszeresen foglalkozni. A rendszeralkotás kiindulópontja az alapfunkciók meghatározása.

A virtuális világok alapfunkciói

Feltesszük, hogy a virtuális világok megalkotásával az ember, az emberi közösségek az alábbi három, objektív szükségletek kielégítésére irányuló funkciót kívánják szolgálni:

- a tapasztalati tudás megszerzésének felgyorsítása,
- a virtuális szükségletek felismerésének elősegítése,
- a totális érzékszervi kommunikáció, közvetlen fizikai ráhatás és érzékelés távolsági kiterjesztése.

Legnagyobb aktualitása a tapasztalati tudás megszerzése felgyorsításának van. Sajnos a leginkább rászoruló területen, a kormányzati tevékenység támogatásában a legelmaradottabb a szoftver- és hardverbázis, valamint az interfészek fejlesztése. Az egész világon súlyos problémát okoz, hogy a weberi értelemben vett bürokratikus, azaz centralizált hierarchikus struktúrájú szervezetek minden ellenkező erőfeszítés ellenére tovább élnek, sőt tovább burjánzanak az államhatalomban, a kormányzatban éppúgy, mint a nemzetközi intézményekben, vagy akár a multinacionális óriásvállalatoknál. A kormányzati működés megreformálása még az olyan gazdag és fejlett országokban is, mint az Amerikai Egyesült Államok, központi kérdéssé vált. Az ezzel kapcsolatos erőfeszítések kiváló példája a *Clinton*-kormányzat hivatalba lépése után kidolgozott, és 1993. szeptember 7-én *Al Gore* alelnök által előterjesztett *Creating a government that works better and costs less* (Egy jobban működő és olcsóbb kormányzat megteremtése) című program. Ha a sajtóban megjelenő értékeléseknek hinni lehet, igazán átütő sikert ez idáig ezzel a programmal sem sikerült elérni.

A bürokrácia elleni frontális támadások eleve kudarcra ítéltségét tudomásul véve jómagam sokáig hittem benne, hogy a bürokratikus szervezetek „éltető alapfunkciójuk", az aggregációs funkció kiiktatásával leépíthetők, elosztott paraméterűvé alakíthatók át. Rá kellett ébredni azonban arra, hogy az aggregáció alternatívájaként kezelt redukció nem képes lépést tartani a komplexitás iránti igények fokozódásával. Még a legradikálisabb, már-már a relevancia határait átlépő redukció révén sem válnak a jelenségek kiszámíthatóvá. Ezzel párhuzamosan azonban az is nyilvánvalóvá vált, hogy semmiféle egy központú program (vagy „csomag"!) véghezvitele sem szorítható a kezelhető komplexitás keretei közé. A bürokrácia ezt a kudarcélményt nemigen hajlandó elfogadni, illetve feldolgozni, hanem a nehézségekre fokozott „burjánzással" válaszol. Ez a burjánzás ma már nem kizárólag, és nem is elsősorban a szervezetek létszámának növekedésével, hanem sokkal inkább az ezen szervezetek által alkotott szabályok szaporodásával, illetve egyre feltűnőbb irracionalitásával jellemezhető.

A tapasztalati tudás jelentősége éppen az irracionalitás térnyerésével kerül előtérbe. A bürokratikus szervezetek ugyanis abban az esetben működnek jól, ha egy alapvető értékpár, nevezetesen a tapasztalati tudáson alapuló szakértelemmel párosult racionalitás töretlenül érvényre jut működésükben. Ha a tapasztalati tudás szintje lecsökken, akkor a racionalitást legázolva utat tör az irracionalitás. Sajnos ebben az évszázadban is több társadalmi, sőt globális méretű katasztrófa vezethető vissza erre.

Minthogy a bürokratikus „szamárlétra" bejárása mára már kiment a divatból, és a rövid választási ciklusok nem adnak elegendő időt a szükséges tapasztalati tudás „természetes úton történő" megszerzéséhez, ezt a folyamatot mesterségesen kell

felgyorsítani. Ezt a célt szolgálhatják a célszerűen megalkotott, „szimulációs rendeltetésű" virtuális világok.

A második alapfunkció jelentősége abban áll, hogy az objektív társadalmi szükségletek virtuális tartományban történő kielégítése gyakorta lehetővé teszi bizonyos, az adott körülmények közt elfogadható szinten kielégíthetetlen effektív szükségletek önmaguktól való megszűnését. Bizonyos virtuális szükségleti konstellációk megvalósítása előidézője lehet az egész gazdaságot új növekedési pályára állító minőségi ugrásnak is. Ezzel kapcsolatos tervező tevékenységünk megalapozásának, tudatossá, célirányossá tételének alapfeltétele a lehetséges virtuális szükségletfajták felismerése. Az e célból megalkotott virtuális világokban megszerezhető tapasztalatok visszacsatolása a társadalmi innováció alapvető forrása lehet.

A harmadik alapfunkció megvalósítása leginkább a térben nehezen, vagy nem kellő gyorsasággal mobilizálható erőforrások igénybevételének kiterjesztését jelenti. Nyilvánvaló, hogy ez a kiterjesztés ezen erőforrások kihasználásának új hatékonysági dimenzióit képes megnyitni.

Elágazások, válaszutak, veszélyek

Nyilvánvaló, hogy a fenti alapfunkcióknak akárcsak részleges megvalósítása is teljesen új lehetőségeket kínálna a sokasodó társadalmi, illetve globális problémák megoldására. Sajnos, a dolgok jövőbeni kimenetele korántsem egyértelműen vezet jó irányba. Ahogy annak idején a század eleji nagy atomfizikus nemzedék kutatási eredményei egyaránt elvezettek az emberiség energiagondjait enyhítő felhasználásokhoz, és Hirosima vagy Nagaszaki tragédiájához, a kibertér meghódítására irányuló erőfeszítéseknek is lehet jó, de nagyon rossz kimenetelük is. A felelősség tehát óriási. A helyes döntések meghozatalát elősegítheti, ha tudatosan megvizsgáljuk a felmerülő alternatívákat, és szembenézünk a fenyegetésekkel. Nyilvánvaló, hogy az alternatívákra nincs egyértelmű válasz, nincs kizárólagos út. Reális célként csupán az fogalmazható meg, hogy hosszabb távon a jó dominanciája érvényesüljön. Vizsgáljunk meg néhány, ma még csak virtuálisan létező fejlődési alternatívát.

Az egyik válaszút: a teljes elidegenedés, vagy a közvetlen emberi kommunikáció iránti igények felerősödése, ezen igények hatékonyabb kielégítése. Az elidegenedés és az ennek következtében megjelenő teljes kiszolgáltatottság éppen az új technológia legmegszállottabb híveit, az Internet-narkósokat fenyegeti leginkább. Idézet egyikük vallomásából (vagy inkább segélykiáltásából): „Már annyira elfajultak a dolgok, hogy egész nap mást sem csinálok, mint e-mailt olvasok és írok, fájlokat töltök le, letárolom, rendezem, iktatom és kinyomtatom őket. A telefonhívásokra már jó ideje nem válaszolok. Egyszerűen nincs rá időm. A munkatársaimmal sem beszélgettem már hónapok óta. Mindent elektronikus postán kérek és küldök. Az emberekkel már csak e-mail útján beszélek. Fekszem az ágyamban éjjel, és azon aggódom, hogy egy nap megszüntetik az e-mail postafiókomat. Egyszerűen nem tudom az életet e-mail nélkül elképzelni. Már a barátaimat sem láttam egy ideje, különösen mióta itthonra is vettem egy gépet ... Segítség!" (Lásd [3].) Mint látni fogjuk, a kibertér e megszállott utazója a legsúlyosabb visszaéléseknek, fenyegetéseknek van kitéve, és egyetlen reménye, hogy élő emberi kapcsolatait sikerül gyorsan helyreállítania.

A másik elágazás: a „fantomrendszerek", a giccs elburjánzása, vagy a lehetséges struktúrákat hordozó rendszerek, a művészet térnyerése. A hirtelen támadt lehetőségekkel számos felkészületlen, tehetségtelen, műveletlen ember is megpróbál élni. Az általuk létrehozott torz virtuális világokban szerzett tapasztalatok semmiféle értelmes cél érdekében nem csatolhatók vissza, és súlyos személyiségtorzulásokhoz, tudatzavarhoz vezetnek. Ezt a veszélyt persze az új technológia kisajátítására törő, különérdeket képviselő elosztási koalíciók is sikerrel aknázzák ki. A kirekesztés érvtárának gyarapítása helyett azonban a kevésbé felkészültek által is helyesen használható eszközök fejlesztésére kellene törekedni. E téren a mesterséges intelligencia kutatási eredményeinek hasznosítása kiváló eredménnyel kecsegtet.

A harmadik fontos elágazás: az információhoz, az ismeretekhez való totális hozzáférés, vagy a fontos ismeretek, információk kisajátítása, monopolizálása. Paradox módon a kibertér minden eddiginél jobb lehetőséget kínál a tudás, az információ monopolizálásához, a rossz szándék elleplezéséhez, a hatalom erőszakos megszerzéséhez.

Mint látni fogjuk, a mindhárom felvázolt alternatívapárban kifejezésre jutó fenyegetések kivédésének, értékrendünk szerinti jó dominanciájának alapvető feltételét a valós, közvetlen emberi kapcsolatok kiteljesedése, a kibertér-közösségek aktív, élő kooperációja jelenti.

Míg a lokális virtuális világok – szerencsés esetben – helyes elvonatkoztatással megalkotott, konkrét fizikai rendszerek működtetése révén történő információfeldolgozáson alapulnak, addig a kibertér nem modellezhető, legalábbis csak végtelen számú modellben lenne leképezhető. Ennek következtében a virtuális világoknak a kibertérben történő interakciói következtében teljesen új, kiszámíthatatlan, előre jelezhetetlen folyamatok bontakozhatnak ki. Ezek a folyamatok rossz esetben igen károsak is lehetnek. Egyetlen dolog

azonban reménykeltőnek mutatkozik: ahogyan nyilvánvalóvá válik az egy központból való kiszámíthatóság lehetetlenülése, és ezáltal a nagyobb komplexitású problémák egy központban való kezelhetetlensége, ezzel egyidejűleg a kibertér elosztott paraméterű világában kibontakoztatható kooperációs mechanizmusok szinergetikai konstrukciók alakításával megoldást kínálhatnak a kezelhetetlen komplexitásból eredő problémákra.

Biztonság

A virtuális világok alapfunkcióinak megvalósítását fenyegető biztonsági problémák végső soron mindig a felhasználó, pontosabban a „résztvevő" szintjén jelennek meg. A biztonsági problémák okai egészen egyszerű műszaki zavaroktól az emberi jogokat komolyan érintő morális, illetve jogi problémákig terjedhetnek. Vizsgáljunk meg a példa kedvéért először néhány egyszerű zavartípust.

A legtöbb „egyszerű" virtuális világ nem képes komplex módon szimulálni a természetes emberi ingerkörnyezet alapvető elemeit (például a gravitációt). Ha egy székben ülve végigszáguldunk egy virtuális városon, akkor arra a képre összpontosítunk, amely előttünk mutatkozik. Ez általában szédülést okoz. A rendszer hosszú reagálási ideje szintén okozhat kellemetlenségeket. Ha az ember elfordítja a fejét, és a táj késik, dezorientáló lehet. Ez komoly tervezési kihívást jelent a mérnökök számára, mert semmilyen környezetkialakítási fogás nem kompenzálhatja a késést.

Ugyancsak komoly gondot okozhatnak a virtuális világok „testreszabottságának" a hiányosságai, bár viszonylag könnyen kezelhetők például az adatkesztyű konfigurálásakor. A mozdulat felismerése ugyanis a kéz méretétől és arányaitól függ. A kezek nagyon különbözőek lehetnek. Így mindegyik ember, aki felveszi a kesztyűt, csinál három gyors kalligrációs mozdulatot, ami után ennek a kéznek a mozdulatait már meg fogja ismerni a rendszer. De nem mindig ilyen egyszerű a fiziológiai különbségek felismerése. Az emberek például különbözőképpen reagálnak a rezgésre, magasságukból, súlyukból, sőt még izmaik feszüléséből is következően. A feszült embereket nagyobb mozgásra, aktivitásra készteti a vibráció, mint a nyugodt embereket. Ezért nem lehet triviális feladat a képernyőt az egyénre igazítva stabilizálni.

Súlyosabb problémát okozhat, ha a résztvevő saját interakcióinak felügyelete kikerül a résztvevő hatásköréből. Egy kísérlet során volt megfigyelhető, hogy valaki átvette az ellenőrzést a résztvevőtől egy bemutató közepén; csendben átkapcsolt a résztvevő kesztyűjéről egy másik irányító eszközre, amelyet a résztvevő nem ellenőrizhetett. A beavatkozó figyelmeztetés nélkül elforgatta a résztvevő perspektíváját minden irányban tíz fokkal. Ez szó szerint megrázó hatással volt a résztvevőre: elsápadt, megzavarodott, és szemmel láthatólag izgatott lett. Olybá tűnt, mintha egy támadásnak lettünk volna szemtanúi.

A virtuális világok biztonságának központi kérdése, hogy a résztvevő jogosult legyen teljes mértékben ellenőrizni saját interakcióit. Ez a kérdés napjainkban legerőteljesebben az Internet felhasználóinak-résztvevőinek interakcióival kapcsolatban jelenik meg.

Egyre inkább nyilvánvalóvá válik, hogy a saját interakciók feletti ellenőrzés alapvető eszközét a különböző kriptográfiai alkalmazások jelentik. Az Internet esetében ilyen a *Pretty Good Privacy* (PGP) rendszer, amelyet *Philip Zimmermann* fejlesztett ki. Ez hamar a legnépszerűbb és legszélesebb körben elterjedt nyilvános kulcsú titkosító rendszerré vált, részben működése, részben ingyenessége miatt. A nyilvános kulcsú rejtjelezés hasonló elven alapszik, mint a régi kínai pecsétek. Ha valakinek üzenetet akarunk küldeni, és azt akarjuk elérni, hogy csak és kizárólag a címzett olvashassa el, akkor az illetőnek a „telefonkönyvben" szereplő nyilvános kulcsával kódolva az üzenetet, bizonyosak lehetünk benne, hogy ez az üzenet csak a címzett „magánkulcsával" fejthető meg, tehát csakis ő ismerheti meg. Ha azt akarjuk, hogy üzenetünket bárki elolvashassa, aki hajlandó a mi nyilvános kulcsunkat valamely nyílt „kulcslerakatból" (telefonkönyvből) kikeresni, akkor az üzenetet a saját magánkulcsunkkal kell kódolni. A nyilvános kulcsú rejtjelezési eljárások – adott esetben a PGP – megengedik a többszintű kódolást. Üzenetünket a címzett nyilvános kulcsával, majd a saját titkos kulcsunkkal egyaránt lekódolva bizonyosak lehetünk benne, hogy az üzenetet csak és kizárólag a címzett olvashatja, ugyanakkor azt is igazoljuk, hogy az üzenet kizárólag tőlünk származhatott.

A PGP és a többi nyilvános kulcsú rejtjelezési eljárás gyenge pontjait a titkos kulcs védelme, illetve a nyilvános kulcs személyhez kötése jelentik. Ha titkos kulcsunk illetéktelenek kezébe jut, lehetségessé válik, hogy a nevünkben üzeneteket küldjenek, pénzügyi tranzakciókra utasítást adjanak, kötelezettségeket vállaljanak. A nyilvános kulccsal való „megszemélyesítéses" visszaélések (például valaki a nevünkben nyilvános kulcsot helyez el a telefonkönyvben) azt eredményezhetik, hogy mások jutnak a nekünk szánt üzenetek birtokába.

A köznapi ember általában nem képes kellő hatékonysággal védeni sem a titkait, sem pedig egyéb értékeit; így titkos PGP-kulcsait sem. Mindazonáltal a védelem erősítésével kapcsolatban megszívlelendőek Zimmermann tanácsai. Még súlyosabb problémának tűnik a megszemélyesítés

útján történő visszaélés elleni védelem. A legbiztonságosabb, ha levelező partnerünk személyesen adja át nekünk a lemezt, amelyen rajta van a nyilvános kulcsa, és ezt töltjük be a számítógépünkbe. Ez azonban nem mindig oldható meg egy nemzetközi hálózat esetében. Ahogy Zimmermann a PGP dokumentációjában elmagyarázza, az ügy végül is bizalmi kérdéssé válik. Az Internet-hálózaton ma már több nyilvános kulcsokat szolgáltató gép is van, amelyről letölthetők mások kulcsai. E kulcslerakatok közül többet komoly hozzáférhetőségi ellenőrző rendszerek is védenek, mégis kérdéses marad, hogy megbízhatunk-e ezekben a rendszerekben.

Érdekes probléma az anonimitás iránti igények és az anonimitással való visszaélés lehetősége között feszülő ellentmondások feloldása. Vannak esetek, amikor méltányolható igény fűződik ahhoz, hogy valaki úgy vehessen részt egy Usenet-vitában, vagy úgy küldhessen elektronikus levelet, hogy nem fedi fel személyazonosságát. Mondjuk, az illető bűncselekmény áldozata, és szeretné másokkal megvitatni az ügyet. Több névtelen (anon) szolgáltatás működik a világon, amely biztosítja az anonimitást, ha éppen arra van szükség. Valószínűleg a legismertebb ezek közül az Espoo városában (Finnország) lévő anon.penet.fi, melyet *Johann Helsingius* üzemeltet. Ezt a rendszert is fel lehet azonban törni, maga Helsingius is elismeri ennek a lehetőségét. A levelek jelszóval történő védelme csak akkor működik, ha azok előbb Finnországot érintik. Ha valamilyen okból az üzenet hibás útvonalra téved, vagy „visszapattan" valahonnan, akkor esetleg más is elolvashatja [4].

Gondot okoz, hogy az anon rendszerek menedéket jelenthetnek a hálózattal visszaélő embereknek. A névtelenségbe való rejtőzésre persze lehet reagálni. Az anonim levelezés ellenzői közül sokan figyelmen kívül hagynak mindent, amit egy névtelen Usenet üzenetben tettek közzé. Mások odáig mennek, hogy olyan szoftveres megoldásokat javasolnak, amelyekkel – lényegében minden Usenet szolgáltatónál – automatikusan törölni lehet minden levelet, amely egy ilyen, anonimitást nyújtó rendszerről érkezett. A kérdés megoldása azért nem egyszerű, mivel léteznek mindenképpen méltánylandó igények is. Ezek elsősorban a pénzügyi szolgáltatások világában jelennek meg.

Már ma is működnek a digitális szignalizáció vívmányának alkalmazásán alapuló olyan pénzügyi tranzakciós rendszerek, amelyek lehetővé teszik, hogy a tranzakció mindhárom résztvevője (vásárló, eladó, bank) egyaránt teljes biztonságban tudhassa magát. Az eladó nem tagadhatja le, hogy fizettek neki, a bank sem, hogy kibocsátotta az „elektronikus bankjegyeket", majd elfogadta őket az üzlettől, és végül a vásárló egyrészt szintén nem tagadhatja le, hogy felvette őket a banktól, másrészt nem fizethet velük kétszer.

Ez a rendszer tehát biztonságos, de nem hagyja a résztvevőket ismeretlenségben. Ha a bank feljegyzést vezet a bankjegyszámokról, akkor az üzlettől érkezett befizetéseket összekapcsolhatja a megfelelő pénzátutalásokkal, így azt is pontosan megállapíthatja, hol és mikor költött pénzt a vásárló (vagy bármely más számlatulajdonos). Az így összeállítható személyi akta még a ma lehetségesnél is jóval „tapintatlanabb" lenne. Emellett a digitális szignón alapuló feljegyzéseket avatatlan kezek könnyebben használhatnák nemkívánatos célokra, mint a hagyományosakat.

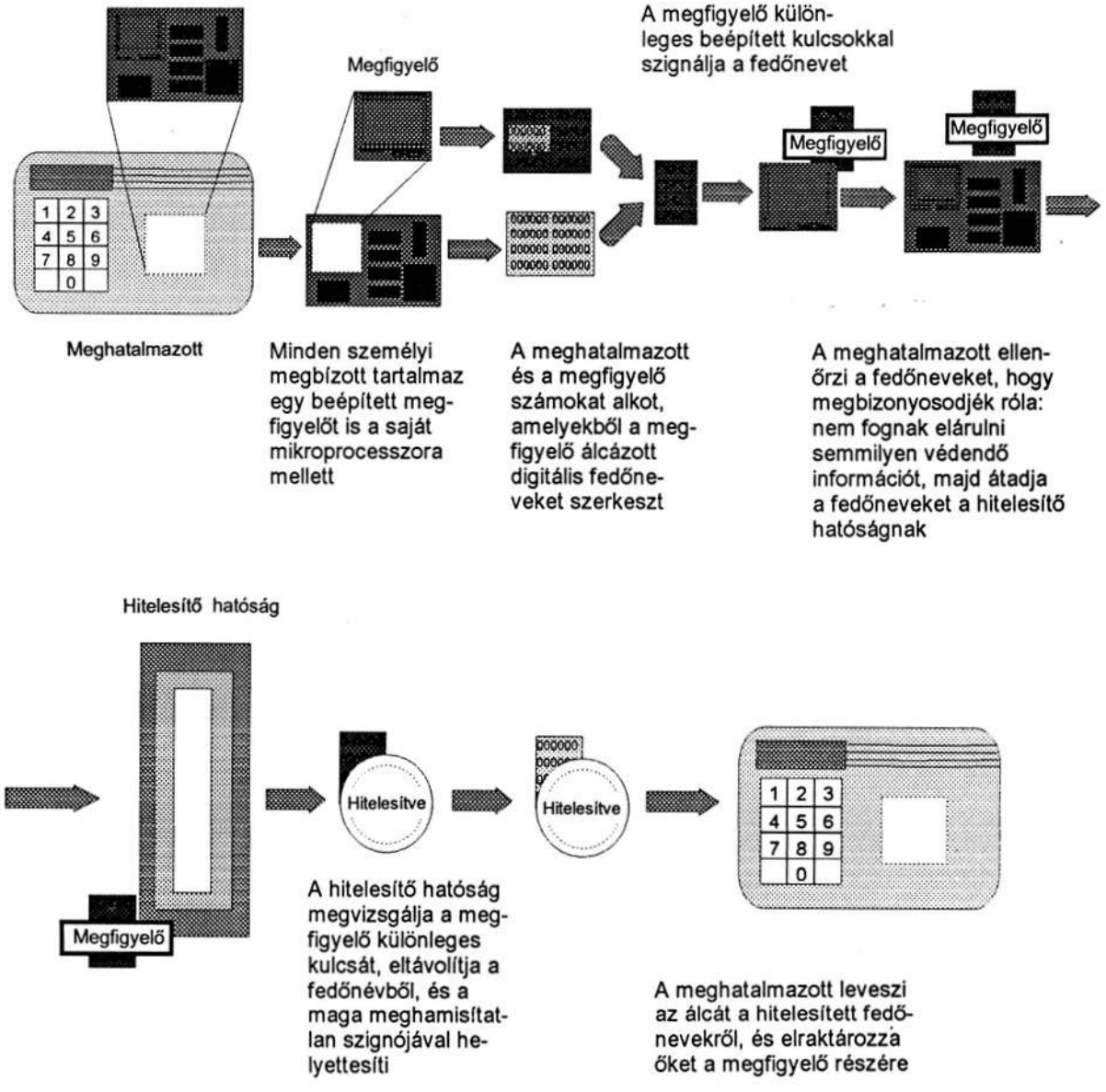
Úgy tűnik, mindenféle technikai hókuszpókuszon (például ujjlenyomat-azonosításon) alapuló – egyébként ugyancsak támadható – hozzáférési ellenőrző mechanizmusok alkalmazása nélkül is tökéletes megoldást nyújt a *David Chaum* által leírt *biztonságos digitális fedőnév* alkalmazását biztosító rendszer [5].

A rendszer két lényegi eleme egy rejtjelezési feladatokat ellátó számítógép, a *meghatalmazott*, valamint egy, ebbe a számítógépbe épített módosíthatatlan számítógéplapka, a *megfigyelő*. A meghatalmazott lehet például egy okos, hitelkártya méretű számítógép, amely a memóriaegységen kívül saját billentyűzettel és kijelzővel is fel van szerelve, hogy tulajdonosa ellenőrizhesse a tárolt és kicserélt adatokat. A megfigyelőt valamely bizalmat élvező szervezet bocsátja ki, és jegyzőként működik közre, igazolva a meghatalmazottal lebonyolított ügyleteket. A biztonságos digitális fedőnév szerkesztésének folyamatát az *1. ábra* szemlélteti.

Amellett, hogy e rendszer általános elterjedésének infrastrukturális feltételei a közeljövőben még nem látszanak megteremthetőnek – többek közt azért, mert még a kártya is csak a fejlesztés stádiumában van –, a digitális fedőnév alkalmazása a pénzügyi tranzakciók és az igazolványok körén túl nem nyújt minden vonatkozásban kielégítő védelmet a lehetséges visszaélésekkel szemben.

A megszemélyesítéssel való visszaélések kivédése leghatékonyabban továbbra is a személyes, egymást hitelesítő, élő emberi kapcsolatok révén képzelhető el. A virtuális világok minden résztvevőjének kell, hogy legyenek olyan hiteles emberi kapcsolatai, amelyek más, őt személyesen nem ismerők számára igazolják valóságos létezését, illetve megbízhatóságát.

A probléma érzékeltetése végett képzeljünk el egy olyan virtuális világot, amelyet egy nagy hatalmú, megfelelő erőforrások birtokában lévő „Intézet" hozna létre. Az Intézet foglalkozhat például szociológiai vagy közvélemény-kutatási feladatokkal. Tevékenységének elősegítése végett sok ezer fiktív személyiséghez kapcsolt „végpon-



1. ábra **Biztonságos digitális fedőnév szerkesztése** *Forrás:* [5]

tot" hoz létre a kibertérmátrixon. A végpontokon keresztül egyedi személyként célszerűen megszerkesztett üzeneteket küld a kiszemelt résztvevőnek, és a válaszokat hatalmas elemző-értékelő kapacitások, szakértői hátterek segítségével elemzi. Azon túlmenően, hogy az Intézet képes lehet a fentiekben említett, Internet-narkósokhoz hasonló magányos résztvevők teljes „bekerítésére" és „elvarázsolására", egyébként is nagy befolyásoló hatalomra tehet szert. Egy ilyen feltételezett Intézet felfedése, az ál-megszemélyesítésekkel való visszaélések kiszűrése szintén csak élő emberi kapcsolatok útján lehetséges.

A megszemélyesítéssel kapcsolatos problémakör aspektusából vizsgálva új megvilágításba helyezhető a kommunikáció ellenőrzéséhez fűződő vélt vagy valós intézményi érdekek és a kriptográfiai alkalmazások központi kontroll nélküli elterjedéséhez fűződő alapvető kibertérérdekek között feszülő ellentmondás is. Az Amerikai Egyesült Államok kormányzata amellett, hogy szorgalmazza egy országos titkosítási szabvány bevezetését, javaslataiban szerepelteti egy „kulcslerakat" adatbázis létrehozását is. Ez az összes kulcsot tartalmazná, és így bármilyen, a szabványban alkalmazott NSA rendszerrel titkosított kommunikáció visszafejthető lenne [6]. Sajtóhírek alapján valószínűsíthető, hogy több más ország államhatalmi szervei is hasonló gondolatokkal foglalkoznak.

A kibertér paradoxonból kiindulva bizonyosra vehető, hogy semmiféle egy központú konstrukció (még akkor is, ha ez a központ megosztott kapacitásokon alapul) nem védhető teljes biztonsággal a visszaélésekkel szemben. A hatalom magánszfé-

rába történő beavatkozása az „elektronikus pénz" megjelenésével, és az elektronikus pénzforgalom elterjedésével kőkemény ellenállásba ütközhet. A polgárok az „intim szférájukba" való beavatkozást még csak-csak elviselik, de ha ez a beavatkozás a pénzügyi biztonságukat is veszélybe sodorhatja, akkor várhatóan minden eddiginél komolyabb ellenállást fognak kifejteni. Egyébként is nehezen hihető, hogy például a szervezett bűnözés vagy a különleges szolgálatok azokat a kommunikációs eljárásokat alkalmaznák ügyleteik leplezésére, amelyek kulcsait letétbe helyezték a központi kulcslerakatban.

Természetesen jogilag elő lehet írni minden kulcsletéttel nem biztosított rejtjelezett üzenetváltás felfedése esetében a szankcionálhatóságot. De hogyan védhető ki például a konspirációs adattovábbításnak azon formája, amelyben a valódi közlemény hordozója olyan élő nyelvű szöveg, amelyről nem állapítható meg, hogy kódolt üzenetet hordoz. Itt már valóban csak a végső logikai érv bevetésétől remélhetnek a kíváncsi intézmények sikert, mégpedig azon az alapon, hogy „az a gyanús, ami nem gyanús".

A kibertér az emberiség történetében példa nélkül álló ütemben fejlődik. Egyes szakértők, például *Peter Wojciechowski* tíz évre teszik, hogy a lokális virtuális világok alkalmazása olyan elterjedté válik, mint ma a televíziózás [7]. Bízvást állíthatjuk, hogy igen gyorsan kell reagálnunk a már ma is sokasodó biztonsági problémákra. Valószínűsíthető, hogy gyökeresen új szemléletű megközelítésre van szükség. A copyrightjogok Interneten való védelme hagyományos jogi megközelítésének teljes kudarca figyelmeztet, hogy valószínűleg más dimenzióban sem használhatók az eddig beváltnak hitt eljárások.

Mindezek alapján a kibertér biztonságfilozófiájának néhány alaptételét az alábbiakban fogalmazzuk meg:

- A kibertérben a résztvevők személyes biztonságának és egyben a virtuális világok alapfunkciói megvalósításának alapfeltétele a résztvevők közti egymást hitelesítő közvetlen, élő emberi kapcsolatok kifejlődése. Létre kell jönniük az egymást hitelesítő résztvevők közösségeinek, majd a tagjaik révén egymást hitelesítő közösségeken alapulhat a kiberteret kitöltő hálózat.
- A résztvevők, a résztvevői közösségek kooperációjának biztosítania kell, hogy szükség esetén gyorsan és hatékonyan alakulhasson ki bármilyen hosszúságú „hitelesítési lánc".
- A kibertérben részt vevők és az intézmények kapcsolatában az egyoldalú ellenőrzést és a szembenállást fel kell váltania a kölcsönös bizalmon alapuló együttműködésnek. E követelmény legfontosabb vonzata, hogy az intézmények erőforrásait a kibertér-kommunikáció feletti kontroll fenntartására irányuló reménytelen és ugyanakkor értelmetlen erőfeszítések helyett a résztvevői közösségekkel való együttműködésre, a kibertérben menthetetlenül kialakuló „fekete lyukak" (különérdek-érvényesítésre törekvő, zárt elosztási koalíciók) felfedésére, lokalizálására és felszámolására kell összpontosítani.

Remélhető, hogy az ilyen hozzáállás számos, manapság megoldhatatlannak tűnő, az emberi társadalmat sújtó más természetű biztonsági probléma megoldása terén is sikerhez vezethet.

Irodalom

[1] BRICKEN, M.: Virtual worlds: no interface to design. = Cyberspace: First Step. The MIT Press. Cambridge, Massachusetts, London, England, 1992. p. 363.

[2] PÉTER R.: Játék a végtelennel. Tankönyvkiadó, Budapest, 1969. p. 30., 31.

[3] Egy Internet-narkós vallomásai. Replika, 14. sz. 1994. p. 239.

[4] GAFFIN, A.: Nagy Internet kalauz mindenkinek. I. I. F. Budapest, 1994. p. 198.

[5] CHAUM, D.: Személyes adatvédelem rejtjelzéssel. = Tudomány, 10. sz. 1992. p. 72–77.

[6] Lásd [4], p. 196.

[7] Interview with Peter Wojciechowski.

[8] NAGY K.: Adatvédelem–informatikai biztonság. A HISEC '93 konferencia anyaga. Neumann János Számítógéptudományi Társaság, 1993.

Beérkezett: 1995. XII. 30-án.