Dénes Tamás
matematikus-kriptográfus

www.titoktan.hu

email: tdenest@freemail.hu

N*em* **I***rhatsz* **BE***szélhetsz* **K***orlátlanul*: **NIBEK**

vs.

H*atalmi* **I***nformáció* **B***irtoklás* **E***llen* **K***riptográfia*: **HIBEK**

A BÖLCS EMBER nem legyőzi,
hanem meggyőzi az ellenfelét.
Különösen igaz ez …
a bölcs politikusokra!
(T.D.T.)

Nem véletlen, hogy az elmúlt 10 év során 39 dolgozatban foglalkoztam a globális információalapú társadalom biztonsága, a hatalom és az információs szabadság antiszimmetriája témával (lásd a mellékelt publikáció válogatást) és még kevésbé véletlen, hogy az eddigieknél is aktuálisabb a jelen 40. dolgozat megírása. Ebben a dolgozatomban a címbeli disszonáns jelenség megvilágítása ürügyén, egyúttal összefoglalom az eddigi 39 dolgozat általános érvényű gondolatait. Bár a fenti mottóban igyekeztem bölcs tömörséggel megfogalmazni dolgozatom célközönségét, el kell ismernem, hogy nem sikerült túltennem az angol nyelv tömörségének bravúrján, így hát *„To Whom it may concern!”*, vagyis *„Annak, akit illet!”*[1]

1. Nyelvújítás vagy állami ideológia a NIBEK?

Az *akrosztichon*, azaz a verssorok, strófák kezdőbetűinek értelmes szavakká, szövegekké való összeolvashatósága, régi időktől ismert. Ennek egyszerűbb, hétköznapi változata a *mozaikszó*, vagy *betűszó*.[2] Sokszor az így képzett szavak a nyelvújítás sikeres termékeivé váltak és kitörölhetetlenül beépültek a köznyelvbe. Ma már természetes szókincsünk részei például az angolból származó WC (vécé), HIFI (hifi), VIP (vip), UFO (ufo), vagy a magyar BKV (békávé), TV (tévé) és természetesen Kellér Dezső örökbecsű *„maszek”* (magán szektor) szava.
Bizonyos értelemben a NIBEK szó már majdnem beépült nyelvünkbe, hiszen a sajtó, a média, és ezáltal az emberek sokasága beszél róla. Abban az értelemben is hasonlít sikeres elődeihez, hogy szinte senki nem ismeri a betűszó eredeti szövegét, amely nemcsak hosszú, de az „egyszerű” állampolgárok számára fenyegetően is hangzik: **N**emzeti **I**nformációs és **B**űnügyi **E**lemző **K**özpont.
A közbeszéd afféle magyar FBI-ként emlegeti, ezzel próbálja barátságosabbá tenni, mint sok más fogalmat, szervezetet, terméket és szolgáltatást, amelyet a „nagy testvértől” vettünk át kritikátlanul. Valóban az FBI (Federal Bureau of Investigation) is betűszó, de ezen kívül más valódi hasonlóság nem is marad. Magyar fordítása a Szövetségi Nyomozóiroda jóval rövidebb, mint a NIBEK eredeti kifejtése, de ennél fontosabb, hogy tartalmilag sem felel meg

[1] Nem szószerinti fordítás, de a cikk tárgyának megfelelőbb értelmezés: *„Mindenkinek, akit illet!”*
[2] A *betűszó*, vagy *mozaikszó* valamely többszavas kifejezés szavainak kezdőbetűiből képzett szó.

az FBI-nak. Magyarország természetes államberendezkedéséből fakadóan ugyanis nem lehet „szövetségi”, a NIBEK pedig a létrehozók definíciója szerint egyáltalán nem „nyomozóiroda”. E felszínesnek tetsző nyelvi megközelítésnél mélyebbre áshatunk, ha magának a törvényhozónak, illetve a törvény javaslattevőjének meghatározását tekintjük:

A Belügyminisztérium javaslata rendkívül széles hatáskörrel rendelkező szervezetet hoz létre, amely

a. *az összes rendvédelmi és nemzetbiztonsági szerv adatbázisából adatokat kérhet le*, akár személyes, bűnügyi, vagy különleges adatokat is.

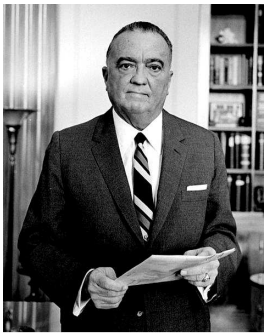
Az *"egységes információfúziós központra"* azért van szükség a Belügyminisztérium szerint, mert a ma létező hasonló szervezet, a SZEBEK (Szervezett Bűnözés Elleni Koordinációs Központ) nem tud *"minden biztonsági kihívásra reagálni"*, amit a kor megkövetel.

b. A globális biztonsági kihívások között *egyre nagyobb a szerepe a terrorizmusnak* - olvasható a javaslat indoklásában, amely példaként a 2001. szeptember 11-i terrortámadást említi. Az új szabályozásban kulcsszó a *„hatékonyság”* – hangsúlyozza a Belügyminisztérium.[3]

c. *A NIBEK feladata az, hogy elemezze és értékelje az információkat és tájékoztassa a kormányt minderről.* Vagyis egy olyan szerv, amely "a bűnözésre, a nemzetbiztonsági kockázatokra vonatkozó adatokat összesíti, szintetizálja, és a kormány döntéseit globális biztonsági szemlélettel készült *taktikai és stratégiai elemzésekkel, javaslatokkal segíti*".

Az *a.-c.* szempont és célrendszer kétséget sem hagy az 1. fejezet címében feltett kérdésre adható válasz tekintetében. A továbbiakban csupán egyetlen lehetőségünk marad a nyelvújításra, ha megadjuk a NIBEK betűszavának *a.-c.* pontok szerinti valóságos kifejtését:
N*em* **I***rhatsz* **BE***szélhetsz* **K***orlátlanul*

Mindeközben sajnálattal jegyezzük meg, hogy ezzel az állami ideológiával ismét a haladó világra nem figyelő, a történelmi tapasztalatokat és zsákutcákat semmibe vevő rossz tanulók képzeletbeli hátsó padjába ült a magyar állam, és sokadszor hagyja figyelmen kívül A. Einstein bölcs intelmét: *„A történelem arra tanít meg minket, hogy az emberiség semmit sem tanul a történelemből.”*


John Edgar Hoover (1895-1972)

2. Déjá vu *„valahol már láttam”* érzés, avagy az FBI magyar torzója

A *déjá vu* érzés magyarázatát sokan a vallásban, különösen a reinkarnációban keresik. A NIBEK esetében nem szükséges sem a vallás, sem a misztikumok világába kalandozni, elegendő csupán az Amerikai Egyesült Államok történetében 70-80 évet visszalapozni.
John Edgar Hoover (1895-1972) az FBI igazgatója volt 1924-től haláláig, azaz majdnem fél évszázadon át, ami akkor is rekord teljesítmény lenne, ha „uralkodása” nem az USA és az egész 20.

[3] Forrás: az [origo] kérdéseire Samu Attila, Pintér Sándor belügyminiszter főtanácsadója válaszolt. (2011. december 2.)

századi világtörténelem legkritikusabb korszakán ívelt volna át. A II. világháború és a hidegháború évei a titkosszolgálatok és a bűnüldözés területén igazán koncentrált munkát igényeltek. J.E. Hoover gondolatait tehát egészen hiteles forrásnak tekinthetjük, amikor az FBI-ról van szó. Nos, éppen a hidegháborús időszak közepén, 1956-ban a *Look magazin*-nak nyilatkozta a következőket:
„Mi csak egy tény összegyűjtő szervezet vagyunk. Nem ítélünk el és nem semmisítünk meg senkit." Look magazine (1956.06.14.)[4]

Talán nem véletlen, hogy Hoover eme állításával tökéletesen összecseng a Belügyminisztérium fenti *a. pontbeli* célkitűzése és annak lakosságot megnyugtató, az új betűszó szerinti félelmeket elaltató igazolása. Ki kell emelni a *c. pontban* idézett „hatékonyságra" való hivatkozást, melynek zászlaja alatt – főleg válságos időkben – az állami ideológia szerint *minden korlátozást el kell fogadni*, amely az állampolgári jogok csorbítására irányul.
Még megdöbbentőbbek az *a. pontbeli* NIBEK jogosítványok, ha figyelembe vesszük, hogy a Belügyminisztérium javaslata szerint a korlátlan adatgyűjtés „alanyi joga" eme (nyelv)újított szervezetnek, és az adatok tulajdonosai képviseletében semmiféle ellenőrzési, felügyeleti, kontroll mechanizmus nem épül a rendszerbe.
Mindezek alapján a NIBEK-et legfeljebb az FBI magyar torzójának nevezhetjük. Különös tekintettel a *b. pontbeli* jogosítványokra, amelyek veszélyéről maga J.E. Hoover ugyanebben az 55 évvel ezelőtti nyilatkozatában ezt mondta: *„Amint az FBI elkezd javaslatokat készíteni, hogy mit kellene tenni a megszerzett információival, abban a percben Gestapóvá válik."* Look magazine (1956.06.14.)[5]

A Belügyminisztérium *c. pontbeli* érvei már valamivel újabb keletű biztonságpolitikai zsákutca *déjá vu érzését* keltik.
Húsz évvel J.E. Hoover idézett nyilatkozata és mindössze 3 évvel halála után, az Egyesült Államokban már kiszivárogtak az addig szigorúan titkos ECHELON kémműhold rendszer[6] létezéséről információk. Ezek alapján, a felvilágosult és a civil társadalomért, az emberi szabadságjogokért felelősséget érző politikusok megvalósulni látták az Orwell-i NAGY TESTVÉR 1949-es utópiáját.[7] Magának az ECHELON rendszernek és az erre épülő korlátlan megfigyelési lehetőségek megteremtésének indoka, akkor és azóta mindig egyfajta fenyegető *közös ellenség, amely ellen globális háborút kell viselni* (természetesen maximális „hatékonysággal").

---

[4] Eredeti angol szöveg: *„We are a fact-gathering organization only. We don't clear anybody. We don't condemn anybody."*

[5] Eredeti angol szöveg: *„Just the minute the FBI begins making recommendations on what should be done with its information, it becomes a Gestapo."*

[6] Az ECHELON rendszer gyökerei az 1948-as UK-USA megállapodásra (szövetségre) nyúlnak vissza, amelynek alapvető indoka a közös nagy ellenség, a szocialista világrendszer réme volt. Az ECHELON vált a hidegháború titkos eszközévé, majd a hidegháború „elmúltával" a *„terrorizmus elleni küzdelem"* felirat került alkalmazásának virtuális zászlójára. A valóságban azonban a hatalmas költségvetéssel működtetett titkos lehallgató rendszer egyre inkább a civil társadalom megfigyelését szolgálja.

[7] Pedig a Földünket és mindennapi életünket behálózó „információ pajzs" valódi működéséről csak az 1990-es évek végén -történelmi időléptékkel mérve- percekkel a 2001. szeptember 11-i események előtt jutottunk részletesebb információkhoz. Az ECHELON rendszer „hatékonyságával", illetve annak a terrorizmus elleni védekezésben betöltött szerepével, valamint a 2001. szeptember 11-i és azt követő terrorcselekményekkel, részletesen foglalkozik jelen szerző több tanulmányában (lásd [DÉNES T. 2001/2], [DÉNES T. 2002/7] , [DÉNES T. 2004/3], [DÉNES T. 2004/4], [DÉNES T. 2010], [DÉNES T. 2011/2])


Frank Church (1924-1984)
USA senator (1957-1981)

Frank Church szenátor 1975-ben így figyelmeztette az amerikai társadalmat a korlátlanul koncentrált hatalmi információbirtoklás szinte beláthatatlan veszélyeire (lásd [NBC 1975]):
„Ugyanakkor, amikor az amerikai emberek lehetőségei gyökeresen megváltozhatnak és minden amerikai teljes magánéletet élhet, ugyanezek az eszközök teszik lehetővé, hogy minden megfigyelhető legyen (telefonbeszélgetés, távirat, fax, email, stb.) Nem lesz egyetlen rejtett hely sem az emberek számára. Ha a kormányzat valaha zsarnoksággá válik, ha egy diktátor kezébe kerül ez az ország, ez a technológiai kapacitás, amelyet a hírszerzés biztosít a kormánynak, tökéletes eszközt ad a kezébe egy totális uralomhoz, amely ellen lehetetlen lesz küzdeni, mert ez az „információs pajzs” tökéletes védelmet biztosít a kormánynak .... Én nem akarom látni azt az országot, amelyik átmegy ezen a „hídon”, mert ez a „híd” olyan szakadékon vezet keresztül, ahonnan nincs visszaút.”

Church szenátor veszélyérzete látnoki módon jelzett, hiszen akkor még a globális „harcrend”[8], vagyis az ECHELON valódi rendszeréről töredékes információk is alig álltak rendelkezésre. A mai technikai lehetőségek és kapacitások Orwell és Church szenátor fantáziáját is messze túlhaladták, éppen ezért egyre nagyobb kísértésnek van kitéve az ezeket birtokló hatalom, amely általában a kormányok kezében összpontosul. A 20. századi történelem, majd a 21. század első évtizedében a *„hidegháború”* helyett *„terrorizmus elleni küzdelem”* feliratú zászló alatt végrehajtott globális megfigyelő rendszerek terjedése, megmutatta eme álságos *„bűnmegelőzési”* stratégia minimális hatékonyságát, miközben maximális költségvetéssel *tartja a függőség félelmében a civil társadalmat* (lásd [DÉNES T. 2011/2]).

Talán még megdöbbentőbb, hogy a **N***em* **I***rhatsz* **BE***szélhetsz* **K***orlátlanul* = NIBEK ideológia *a.-c.* konstrukciójának antihumánumáról, már jóval Hoover, Orwell és Church szenátor előtt írt Kosztolányi Dezső (1885-1936), tehát karnyújtásnyira van az eredeti magyar gondolat:


Kosztolányi Dezső (1885-1936)

„Beírtak engem mindenféle Könyvbe és minden módon számon tartanak. Porzó-szagú, sötét hivatalokban énrólam is szól egy agg-szürke lap.
Ó, fogcsikorgatás. Ó, megalázás, hogy rab vagyok és nem vagyok szabad. Nem az enyém már a kezem, a lábam és a fejem, az is csak egy adat. Jobb volna élni messze sivatagban, vagy lenn rohadni, zsíros föld alatt, mivel beírtak mindenféle Könyvbe és minden módon számon tartanak.”
(Kosztolányi Dezső: „A bús férfi panaszai”-ból, 1921.)

Kosztolányi látnoki módon írta le napjaink NIBEK ideológiáját, a koncentrált hatalmi információbitorlás veszélyét. Hiszen valahányszor pénzügyi, egészségügyi, e-kommunikációs vagy bármely hivatali e-szolgáltatást veszünk igénybe, adataink mindannyiszor (nyíltan vagy észrevétlenül) egy-egy adatbázisba jutnak és általunk a továbbiakban követhetetlenül „önálló életet élnek”. Sőt, eme -életünk folyamán keletkező- temérdek adat, akár *„személyi aktává”* (digitális *„agg-szürke lappá”*) is összekapcsolható, melynek felhasználása, vagy éppen az adatok manipulálása, számunkra kideríthetetlen.
Az információalapú társadalom kulcsproblémája, hogy minden korábbinál nagyob a veszélye annak, hogy mindezek az adatok, a Kosztolányi által látnoki módon megjósolt *„agg-szürke lap”-ok, a Church szenátor által vizionált rossz kezekbe kerülnek.* Legalább ekkora bizonytalanságot kelt az állampolgárokban, hogy digitális „személyes aktájuk” a különböző

[8] Az ECHELON angol jelentése: *harcrend, harcvonal.*

állami intézmények között elméletileg szabadon áramolhat. Megállapíthatjuk tehát, hogy minél több adat birtokába jutnak a hatalom intézményei, annál inkább kikerül a civil társadalom, azaz az emberek kezéből a magántitok, a személyesség és az afölötti rendelkezés, azaz az *információs szabadság* lehetősége.
Különösen fontos e veszélyekre felhívni a figyelmet egy olyan információalapú világban, amelyben az e-kommunikációtól, az e-banki és e-kereskedelmi szolgáltatásokon keresztül, az e-ügyintézésig, egyre növekvő mértékben virtuálissá válik az információk tárolása, továbbítása és felhasználása. Mindennek korlátlan és gyakorlatilag ellenőrizetlen birtoklását és felhasználását jelenti a NIBEK ideológia. Sötét jövőkép ez egy információalapú társadalomban!

3. A 21. század „csodafegyvere”

Az állam (hatalom) mindig választhat aközött, hogy megteremti-e az információk birtoklásának és azok felhasználásának szimmetrikus egyenszilárdságát[9], vagy az állampolgárok számára *tökéletes fekete-doboz rendszert hoz létre* a birtokában lévő hatalmas információtárolókban tárolt gigászi mennyiségű információból. Az egyik irány a civil emberek és szervezetek *„magán szférájának”* minden eddiginél mélyebb kifürkészése és egyre erősebb befolyásolása felé vezet[10], a másik azonban az egyének és az intézmények *információs egyenjogúsága* felé. A 21. század e-társadalmának körvonalai nem csekély mértékben attól függnek, hogy melyik irányzat kerekedik felül.

„Szitáljuk át a sivatagot egy elegendően nagy és megfelelő lyukméretű szitán.
Ami kihullik az a homok, ami fennmarad az az oroszlán.”
„Tekintsd a 99.9% becsületes embert bűnözőnek, hogy a 0.1% bűnözőt megpróbáld kiszűrni!”[10]

---

[9] Egyenszilárdság alatt az információs rendszerek azon tulajdonságát értjük, hogy a rendszer bármely pontjának biztonsága azonos erősségű biztonsági alrendszerrel védett (lásd [VASVÁRI 2009]). A szimmetria a civil információkat tartalmazó rendszereknél azért kiemelendő, mert itt az információ tulajdonosa (állampolgár, civil szervezet, stb.) nem azonos az információtároló tulajdonosával (állam). Ezáltal már az információkhoz való hozzáférés sem szimmetrikus!

[10] Erre épül a mára már globalizálódott ***anti-bűnmegelőzési filozófia***, amelyet a *„Hogyan fog az elméleti fizikus oroszlánt a sivatagban?”* gondolatkísérlet jól illusztrál: *„Szitáljuk át a sivatagot egy elegendően nagy és megfelelő lyukméretű szitán. Ami kihullik az a homok, ami fennmarad az az oroszlán.”* A modell-analógia jól értelmezhető a mindent behálózó megfigyelő és azonosító rendszerekre, ha „a sivatag homokjaként” értelmezik a 99.9% becsületesen és békésen élő állampolgárt, akiket ez a „szitáló eljárás” állandó megalázó zaklatásnak tesz ki, és a maradék 0.1% a tulajdonképpen zsákmányul ejtendő oroszlán. Vagyis, ha a modell arányokra vonatkozó aspektusát tekintjük, akkor a NIBEK-típusú anti-bűnmegelőzési filozófia így fogalmazható meg: ***„Tekintsd a 99.9% becsületes embert bűnözőnek, hogy a 0.1% bűnözőt megpróbáld kiszűrni!”*** (lásd [DÉNES T. 2010])

Tehát a 21. század *„információs fegyvere”*, az eddigi történelem legördögibb *„csodafegyvere”* (lehet), amely nem rombol le épületeket, nem pusztít el fákat, erdőket, állatokat és növényeket, gyártására nem épülnek monumentális gyárak, üzemek sem a föld felett, sem a föld alatt. *Ez a csodafegyver a globális információs társadalom milliónyi digitális e-cérnaszálán függő embert helyezi marionett bábuként, olyan aszimmetrikus, kiszolgáltatott, védtelen helyzetbe, amelyben a hatalom képes az e-cérnaszálakat szinte korlátlanul manipulálni, sőt bármikor elvágni. Ördögi eszköz tehát az "információs fegyver", amellyel észrevétlenül lehet láthatatlan információs rabszolgaságba sodorni emberek millióit.*

Meglepő, egyben az emberi társadalom működésének általános törvényszerűségeire utal, hogy már a 17. században Coménius így vélekedett: *„Milyen siralmas látni, hogy a tudományokat alig lehet megkülönböztetni a fegyverektől.”*

A magas technikai fejlettségű országokban felismerték a problémát és éles küzdelem folyik az állampolgári jogok és a hatalom által *„nemzetbiztonsági érdek”*-ként előadott harcban. El kell ismernünk, hogy ez az emberiség egészét, kiváltképpen a „fejlettnek mondott” társadalmakat tekintve nemtelen küzdelem, a hatalom és a civil társadalom között eléggé egyenlőtlen.
Ez az egyenlőtlenség a társadalmi evolúció új szintje, amely éppen az információalapú társadalom alapját képező *információ birtoklásán alapul*. Így válhat az információ birtoklása „csodafegyverré”. Az információalapú társadalom alapvető működési formájává válik a ***tömeges titkosítás és egyéni biztonság paradoxon.*** (lásd [DÉNES T. 2005/3], [DÉNES T. 2005/4])


Norbert Wiener (1894-1964)

Nem véletlen, hogy eme folyamat lényegét a 20. század közepén, az információrobbanás korának kezdeti pillanataiban, Orwellel azonos időben, egy másik látnok gondolkodó Norbert Wiener így fogalmazta meg:
„A tipikus amerikai világban az információ sorsa az, hogy áru lesz, venni és eladni lehet. Nem az én dolgom, hogy azon akadékoskodjam, hogy ez a kereskedői álláspont erkölcsös-e vagy nem, durva-e vagy finom. Az én dolgom az, hogy kimutassam: ez az álláspont az információ és a vele kapcsolatos fogalmak félreértéséhez és félrekezeléséhez vezet.” (Norbert Wiener) [DÉNES T. 2002/4]

Természetesen a napjainkban rendelkezésre álló, minden eddigi látnok gondolkodó képzeletét felülmúló digitális e-technikát lehet jól, jó célokra és minden résztvevő számára biztonságosan tervezni és megvalósítani. Azonban a 21. század információs „csodafegyverei” jóval könnyebben kerülhetnek rossz kezekbe, és ha valóban rossz kezekbe kerülnek (lásd Church szenátor intelmét), akkor sokkal nagyobb kárt tudnak okozni a társadalomnak, mint amekkorát a célorientált fizikai, kémiai, biológiai fegyverek!
Ugyanis a technika robbanásszerű fejlődésével nem fejlődik arányosan *veszélyérzetünk*. Erre hívta fel Albert Einstein (1879-1955) kora társadalmának figyelmét, amikor ezt mondta: *„Az atom hatalmának szabadon engedése mindent megváltoztatott, kivéve gondolkodásmódunkat, és így példátlan katasztrófák felé sodródunk.”*
Nekünk már történelmi rálátásunk van, ezért tudnunk kell, hogy A. Einstein intelme a 21. század *„információs csodafegyverére”* hatványozottan érvényes. Ne ismételjük meg a történelmi hibákat!

Figyeljünk Kosztolányi, Orwell, Church szenátor napjainkig ívelő gondolataira, mert ma már minden technikai eszköz rendelkezésére áll a hatalomnak, hogy megvalósuljanak Orwell (akkor még) utópiának szánt gondolatai:


George Arthur Orwell
(1903-1950)

„Bizonytalan volt, hogy a Gondolatrendőrség milyen gyakran és milyen rendszer szerint kapcsolódik be egy-egy magán-teleképkészülékbe. Még az is elképzelhető volt, hogy mindenkit állandóan figyelnek. Mindenesetre akkor kapcsolódhattak be akárkinek a készülékébe, amikor csak akartak. Az embernek abban a tudatban kellett élnie – s abban a tudatban is élt, ösztönné vált megszokásból-, hogy minden hangját hallják, s kivéve, ha sötét van, minden mozdulatát megfigyelik." ([ORWELL 1989] 8.old.)

Az Orwell által utópiaként megteremtett NAGY TESTVÉR hatalomkoncentráció megvalósulásának törvényszerű következménye a szintén Orwell által megalkotott *newspeak*, azaz *újbeszél nyelv* létrehozása.

„Az orwelli *újbeszél* nyelv funkciója az, hogy ne lehessen megérteni az irányadótól eltérő véleményeket, hogy eltávolítsa azokat a szavakat (gondolatokat), amelyek a nézetkülönbségek kifejezésére használhatók lennének. Így a *Gondolatrendőrség*nek nem is kell kifejleszteni olyan módszert, amellyel megtalálja a véleményeltéréseket az emberek gondolataiban, hiszen *újbeszél*ül ilyenek létre sem jöhetnek. Az *újbeszél* tehát egyre több szót, kifejezést, azaz ezekre épülő gondolatot, fogalmat takarít meg a szótárakból, vagyis a szópusztítás és ezáltal a gondolatirtás nyelve." [DÉNES T. 2010]

Talán éppen a 2001. szeptember 11-i terrortámadás 10 éves évfordulójára rímel a magyar kormány NIBEK ideológiájának, erre a dátumra időzített törvénybe iktatása?

Kriptográfusként és az információalapú társadalom biztonságával évtizedek óta foglalkozó kutatóként, kötelességemnek érzem e vészesen felgyorsult folyamat veszélyeire felhívni a figyelmet, valamint a kriptográfia tudománya és a digitális technika legújabb eredményei szerint javaslatokat tenni az egyenszilárdságú, a társadalom szereplői számára minél szimmetrikusabb biztonság megteremtése érdekében.

Ahogy az eddigiekben, úgy a jelen dolgozat 1.-3. fejezeteiben is, a civil társadalom és a hatalom *aszimmetrikus biztonsága*, a *titok kettős értelmezése*, a *„sivatagban oroszlánt fogni"*[11] *anti-bűnmegelőzési filozófia*, a 21. század ördögi *„információs csodafegyverének"* veszélyeit igyekeztem összefoglalni. A *veszélyérzet* ugyanis alapvetően szükséges a probléma tiszta megfogalmazásához, amely Pólya György[12] örökérvényű gondolata szerint, *fél út a megoldáshoz*.

Ahogy az eddigiekben, úgy a jelen dolgozat záró fejezetében is fontos felhívni a figyelmet arra, hogy a hálátlan utókor köszönettel tartozik azon látnok-gondolkodóknak[13], akiknek „válláról" az adott kor határainál jóval távolabbra látni. Az információalapú társadalom civil

[11] Lásd a 9-es lábjegyzetet!

[12] Pólya György (1887-1985) magyar származású matematikus, a matematikaoktatás megreformálásának egyik elindítója, a *heurisztika* matematikai alapjainak kidolgozója. 1945-ben írt művét, a *Gondolkodás iskoláját* 16 nyelvre fordították le. Örökérvényű gondolata: *„A probléma megfogalmazása fél út a megoldáshoz."*

[13] Akik közül itt csak néhányról ejtettem szót, de a többi dolgozatomban, a TitokTan köteteimben és a www.titoktan.hu honlapom Titkos-arc-KÉP-tár oldalán, igyekeztem gondolatemléket állítani számos hasonló óriásnak.

emberiségének marionett bábusodása elleni felelős veszélyérzet megfogalmazásával, láthatóvá vált a problémák megoldása felé vezető „fél út”.

Ahogy az eddigiekben, úgy a jelen dolgozat záró fejezetében is szeretném megosztani az Olvasóval a jó hírt, amely egyelőre csak a kriptográfia szemüvegén át látható: ***az információs csodafegyver nélküli, emberközpontú e-társadalom felé vezető út másik fele is járható!***

A következő 4. és 5. fejezetben csupán jelzésszerűen foglalom össze kriptográfus gondolataimat, mely szerint az információalapú e-társadalomnak van szimmetrikus egyenszilárdságú biztonságot nyújtó megoldása, mivel *az információs fegyver jó kezekben csoda (lehet).*

4. Az INFOSANCE társadalomban van megoldás: NIBEK helyett HIBEK!

„Próbáltam súgni, szájon és fülön,
mindnyájotoknak, egyenként, külön.”
(Karinthy Frigyes: Előszó)

Különös gondolati kalandtúrát ajánlok a kedves Olvasónak, melynek során átélhetünk egy új felvilágosodást és a végén egy egészen új világba érkezünk, ahol *(egyszer) minden világos lesz.*

Képzeljük el, hogy a renaissance mintájára egy INFOSANCE (INFOrmációs renaisSANCE) társadalom víziója valósul meg[14]. Az analógia első hallásra meglepő lehet. De gondoljunk bele, hogy a renaissance szélesre tárta az ablakot a középkor csőlátásával szemben, amikor az egyház birtokolta a világról szóló információk nagy részét, így kezében volt az emberek gondolkodásának *„marionett-vezérlése”*, ami sokszor az inkvizícióhoz vezetett.
Mára ez átalakult a digitalizált, elektronizált technika-centrikus világ csőlátásává, az Internet, a globalizálódó információs hálózatok fekete dobozává, amelynek „marionett-vezérlése” a hatalom, az óriás adattárak és informatikai rendszerek birtoklóinak kezében van. Ezt testesíti meg a NIBEK ideológia.

A jelen szerző által az ezredfordulón bevezetett fogalom, az INFOSANCE a szabadon gondolkodó ember klasszikus képességeinek optimális egyesítése a mindent átszövő, globalizálódó e-technikával és az egyre teljesebb, biztonságosabb információ birtoklásával. Az INFOSANCE olyan e-társadalom képét rajzolja fel, melynek középpontjában új, modern renaissance *e-mber* áll, akinek történelmi lehetősége egy *új ablak nyitás*, amely a felhalmozott e-technikát, a globális e-kommunikációs és információs rendszereket egyesíti a renaissance mintájú szabad, szárnyaló, kreatív, emberi gondolkodással. *Az INFOSANCE társadalma tehát kreatív társadalom, amely akárcsak az emberi kreativitás, a társadalmi túlélés alapfeltétele.*

Az utóbbi 20 évben folytatott kutatásaim meggyőztek arról, hogy a 20. századi titkosítás fejlődésének szemüvegén át lehet csak igazán megérteni korunk információalapú társadalmának biztonsági problémáit, így azokat a megoldási lehetőségeket is, amelyek már átvezetnek jelen századunkba, a 21. századba.

[14] Az INFOSANCE kor (társadalom) gondolatát jelen szerző az ezredfordulón [DÉNES T. 2001/1] dolgozatában vezette be (lásd még [DÉNES T. 2002/4]).

Meg kell érteni mindenkinek, döntéshozóknak és a társadalom testét alkotó tömegeknek egyaránt, hogy az infromációalapú társadalom mélyén, a szó összes jelentése szerint, a BIT[15] munkál. A rohamos sebességgel növekvő technikai fejlődés, a totális elektronizációhoz és a digitális technika hétköznapi elterjedéséhez, vagyis a soha nem látott bonyolultságú globális e-társadalomhoz vezet.
Márpedig egy tömeges információt kibocsátó, továbbító és tároló társadalomban csak a tömegesen alkalmazható, ám mégis egyedi biztonságot nyújtó rendszerek jelentenek társadalmi méretű biztonságot. Ez Jókai utópisztikus regényére asszociálva a *„jelen század reménye”*.

A NIBEK intézményének megteremtése, csupán a civil társadalom információs kiszolgáltatottságának, mint jéghegynek a csúcsa. Egyelőre még kevés szó esik nyelvünk új betűszaváról, a NEK[16]-ről, azaz az *egységes állampolgári igazolványkártya programról*[17], amely egyetlen intelligens chipkártyára vonná össze az egy-egy állampolgárhoz tartozó alapvető igazolványok információit. Ezzel a személyes adataink feletti önrendelkezéshez és biztonságos felhasználásához való jogunk sérülékenysége tömegjelenséggé válik. Hiszen a zsebünkben hordott plasztik kártya, ekkor már nem néhány adat tárolására alkalmas egyszerű adattároló, hanem személyes *„agg-szürke lapunk”*, azaz egy óriási tárolókapacitással rendelkező mikroszámítógép, amely általunk nem ismert adatfeldolgozó programokat tartalmaz. Ráadásul ezekhez a programokhoz csak a kártyák kibocsátójának van hozzáférése, így változtatási lehetősége is. Szemléletesen az *állampolgári igazolványkártya* úgy fogható fel, mintha *egy széfbe mi gyűjtjük a pénzt, de annak kulcsát más birtokolja*, így a pénzzel is csak ő tud gazdálkodni.

Az intelligens chipkártyák ugyanakkor kitűnő technikai lehetőséget teremtenek azokhoz a kriptográfiai megoldásokhoz, amelyek a szimmetrikus biztonságot megteremthetik.[18]

5. A *digitális képviselő* és *megfigyelő* szimmetrikus biztonsága (Digitális igazolvány)

Vannak a kriptográfia tudományának gyakorlatban is alkalmazható modern eredményei, amelyek alapján lehet mindkét (látszólag ellenérdekű) fél számára biztonságos, azaz szimmetrikus biztonságú informatikai rendszereket konstruálni. Ezek a technikák a statikus, egyirányú hozzáférést és felhasználást biztosító titkosítás helyett, dinamikus egyenszilárdságú és osztott titkosító rendszereket használnak. Ha e módszerek beolvadnak a hatalom mindennapi gyakorlatába, akkor van esélyünk a *„marionett bábu effektus”*-t közép- vagy hosszabb távon megakadályozni és a *„sivatagban oroszlánt fogni” anti-bűnmegelőzési NIBEK ideológiát*, a biztonság valódi, hatékony konvergencia programjára lecserélni. (lásd [DÉNES T. 2007])

---

[15] BIT: **B**iztonság az **I**nformációalapú **T**ársadalomban

[16] **NEK**: **N**emzeti **E**gységes **K**ártyarendszer, amely a Digitális Megújulás Cselekvési Tervének egyik fő pontja és a 2010. december 27-ei Magyar Közlönyben megjelent kormányhatározat alapján, 2012-13-ban kerül bevezetésre.

[17] Ezt a témát egy következő dolgozatban tárgyalom részletesen. Itt csupán azért említem meg, mert szinte azonos információbiztonsági problémákat vet fel, és azonos kriptográfiai modellek (technikák) jelentik a megoldást, mint általában a NIBEK ideológia ellen.

[18] Éppen ezért nevezhetjük felesleges zsákutcának az utóbbi 20 év igazolvány „fejlesztési” programját, amely a papíralapú igazolványokat egyszerűen plasztik kártyákra cserélte. E „fejlesztési” program kezdetén pontosan tudható volt, hogy mind technikai, mind biztonsági szempontból, ez csupán drága átmeneti megoldás.

Tehát nyitottnak kell lennie a hatalomnak az *„információs cérnaszál”* két végén egyenlő biztonságot nyújtó technikák alkalmazására. Ezek a technikák olyan emberi alkotások, amelyek lehetővé teszik a biztonsági rendszereket veszélyeztető leggyengébb láncszem, az emberi tényező[19] nagyfokú kiküszöbölését, és ezzel megteremtik a biztonságos információs egyenlőség alapjait. Így válhat az *„információs csodafegyver”* az INFOSANCE tudástársadalmának alapjává. (lásd [DÉNES T. 2002/3], [DÉNES T. 2002/9], [DÉNES T. 2003/7])

Az évszázadok során kialakultak, a papíralapú dokumentumok szimmetrikus biztonságát biztosító eljárások, amelyek alapvetően az emberi tényező megbízhatóságára (etikai, erkölcsi, szakmai normákra) épültek[20], így az elektronikus dokumentumok virtuális világában már nagyon sérülékenyek. A civil társadalom információbiztonságát csak kismértékben, vagy egyáltalán nem biztosítják, sem a NIBEK típusú hatalmi, sem a haszonszerzésre irányuló illetéktelen beavatkozások ellen.
Ezt a kulcsproblémát olyan kriptográfiai modellek oldják meg, amelyek az INFOSANCE kor szellemében alkalmazzák a legkorszerűbb digitális eljárásokat és eszközöket a biztonsági rendszerben, az emberi tényező maximális kiküszöbölésével. Vagyis a digitális aláírást[21] úgynevezett *digitális fedő aláírás (szignó) rendszer* egészíti ki. Mindezeket a kriptográfiai lépéseket elvégző eszközt[22], a [DÉNES T. 2003/4] és [DÉNES T. 2003/5] dolgozatokban bemutatott *digitális (elektronikus) képviselőnek és megfigyelőnek nevezzük.* E dolgozatokban az információbiztonság két legnagyobb területére, a pénzügyi és a személyes dokumentumokra vonatkozóan található, a *digitális pénz* és *digitális igazolvány* leírása.

A *digitális képviselő rendszer* mélyén az alig 30 éves múltra visszatekintő nyilvános kulcsú titkosítás, valamint a sztegonográfia, a titokmegosztás és a szimmetrikus biztonságot dinamikussá tevő „zero-knowledge proof” (előismeretek nélküli bizonyítás) kriptográfiai protokolljai működnek. (lásd [DÉNES T. 2001/3], [DÉNES T. 2002/8], [DÉNES T. 2004/2], [DÉNES T. 2005/5], [DÉNES T. 2006/2], [DÉNES T. 2008])

Mindezek eredményeként válik lehetővé, hogy bármely személy a digitális képviselője segítségével léphet kapcsolatba a különféle intézményekkel úgy, hogy mindegyik intézmény teljes biztonsággal azonosítani tudja a személyt, de a rá vonatkozó adatokat mégsem kapcsolhatják össze. A digitális képviselő által létrejövő dinamikus kapcsolatban, a kriptográfiai protokoll (az emberi tényezőt kiküszöbölve) biztosítja, hogy az adott intézmény csak a személy azon adataihoz férhet hozzá, amelyre jogosultsága van, függetlenül attól, hogy az adott chipkártyán még milyen adatok találhatók.

---

[19] Az *emberi tényező* minden biztonsági rendszer legintelligensebb és egyúttal legsebezhetőbb eleme. A gépi intelligenciával ellentétben ugyanis számtalan szubjektív elem hat az ember működésére, amelyek közül a biztonsági rendszer szempontjából legkritikusabbak: fáradékony, megfélemlíthető, zsarolható, korrumpálható, esetleg érdekvezérelten a hatalmával visszaélő. Az emberi tényező szerepét a biztonsági kultúra kialakulásában, így a szervezeti, sőt társadalmi szintű biztonsági rendszerekben, átfogóan tárgyalja Vasvári György [VASVÁRI 2009] kötetében.

[20] Ezek az eljárások olyan semleges –közjegyzői, ügyvédi típusú- hitelesítő szervezetekre, személyekre épülnek, amelyek képesek egy dokumentumban szereplő összes fél érdekeit egyszerre szavatolni. Ez a szavatolás azonban főleg törvényi és más emberi tényezőkre épül, így a dokumentumban szereplő információk (adatok) illetéktelen hozzáférését, felhasználását csak e (biztonsági szempontból) leggyengébb láncszem biztosítja.

[21] A hagyományos aláírástól eltérően, a digitális aláírás nem csak az aláíró személyét, de az aláírt dokumentumot is hitelesíti (lásd [DÉNES T. 2002/2]).

[22] Ez az eszköz az alkalmazási területtől függően, egy személyi számítógép (laptop, palmtop), de ma már akár egy chipkártya, vagy egy mobiltelefon is lehet.

A digitális képviselő úgy biztosítja az általa képviselt személy anonimitását, ezáltal információs önrendelkezési jogát, hogy ugyanakkor az intézmény a jogosultságának megfelelő pontos adatokhoz jut hozzá, így teljesül mindkét fél számára a szimmetrikus biztonság.

Szakmai megközelítésben tehát van megoldás: a NIBEK ideológiát HIBEK-re kell cserélni, azaz **H***atalmi* **I***nformáció* **B***irtoklás* **E***llen* **K***riptográfia*: **HIBEK**
A szimmetrikus biztonság megteremtésének lehetősége a szakemberek, a döntése a politikusok kezében van.

Jelen dolgozatot azzal az ajánlással zárom, amellyel megjelenés előtt álló ***A Globális Titok*** *(A 21. század kulcsa:* ***B****iztonság az* ***I****nformációalapú* ***T****ársadalomban)* című kötetem kezdődik:

Ajánlom ezeket a gondolatokat minden fiatal figyelmébe, akik egy olyan világba születnek, amely az e-társadalmat hajlamos technikai bravúrnak tekinteni.
Legalább ennyire ajánlom eme gondolatokat mindazoknak a döntéshozóknak, akik egyszerre az információs fegyver (hatalom) birtokosai és kiszolgáltatottjai.

Vagyis

„Mindenkinek, akit illet!”

Dénes Tamás publikációi e tárgyban:

[DÉNES T. 2001/1] Biztonságos Információ (s) Társadalom (Két paradoxon egy címben)
INFO TÁRSADALOMTUDOMÁNY, 2001/53.
http://www.titoktan.hu/_raktar/_e_vilagi_gondolatok/4.GondolINFTARS.htm

[DÉNES T. 2001/2] ECHELON az e-társadalom információpajzsa ?
Híradástechnika, 2001/6. 14-19
http://www.titoktan.hu/_raktar/_e_vilagi_gondolatok/1.GondolECHELON.htm

[DÉNES T. 2001/3] SZTEGONOGRÁFIA - rejtett információk rejtjelzés nélkül
Híradástechnika, 2001/8. 15-21
http://www.titoktan.hu/_raktar/_e_vilagi_gondolatok/2.GondolSZTEGANOGR.htm

[DÉNES T. 2002/1] Új eredmények az RSA kulcsok megfejtéséhez
Híradástechnika, 2002/1. 47-55
http://www.titoktan.hu/_raktar/_e_vilagi_gondolatok/HTRSA.htm

[DÉNES T. 2002/2] e-aláírás vagy d-aláírás
CEO Magazin, III.évf. 2002/2-3.
http://www.titoktan.hu/_raktar/_e_vilagi_gondolatok/E-DALAIR.htm

[DÉNES T. 2002/3] „Rejtett csodafegyver”!
Népszabadság, 2002. június 6. /Fórum rovat/

[DÉNES T. 2002/4] INFOSANCE, a jövő INFOrmációs renaisSANCE társadalmának esélye
eVilág, I.évfolyam 4.szám, 2002/július
http://www.titoktan.hu/_raktar/_e_vilagi_gondolatok/5.GondolINFOSANCE.htm

[DÉNES T. 2002/5] A globális e-társadalom és a terrorizmus „szövettana” a kriptográfia mikroszkópján át (Gondolatok 2001.szeptember 11-e első évfordulóján)
CEO Magazin, III.évf. 2002/4.
http://www.titoktan.hu/_raktar/_e_vilagi_gondolatok/3.GondolSZEP11.htm

[DÉNES T. 2002/6] e-MBER avagy egy új veszélyeztetett faj keletkezése
eVilág, I.évfolyam 6.szám, 2002/szeptember
http://www.titoktan.hu/_raktar/_e_vilagi_gondolatok/7.Gondole-mber.htm

[DÉNES T. 2002/7] Kriptográfia-politika „szeptember 11” előtt és után
Híradástechnika, 2002/9, 45-48

[DÉNES T. 2002/8] Az adathordozók „ujjlenyomata” (Digitális ujjlenyomat)
CEO Magazin, III.évf. 2002/6.
http://www.titoktan.hu/_raktar/_e_vilagi_gondolatok/DIGUJL.htm

[DÉNES T. 2002/9] A Turing-teszt az e-társadalom napi gyakorlata
eVilág, I.évfolyam 9.szám, 2002/december
http://www.titoktan.hu/_raktar/_e_vilagi_gondolatok/6.GondolTuringteszt.htm

[DÉNES T. 2003/1] A leggyengébb láncszem
Népszabadság, 2003. április 30. /Fórum rovat/

[DÉNES T. 2003/2] Turing-teszt az információs társadalomban, avagy valós vagy virtuális e-társadalom? *Társadalomkutatás, 21.kötet 2003/3.szám 275-310*
http://www.titoktan.hu/_raktar/_e_vilagi_gondolatok/6.GondolTuringteszt.htm

[DÉNES T. 2003/3] Nem elektronikus adathordozók „ujjlenyomata” (Dokumentumok biztonsága ma és holnap) *Híradástechnika, 2003/7, 40-44*

[DÉNES T. 2003/4] e-dokumentumok és személyesség
CEO Magazin, IV.évf. 2003/5.
http://www.titoktan.hu/_raktar/_e_vilagi_gondolatok/E-DOKUM.htm

[DÉNES T. 2003/5] Biztonságos digitális pénz és igazolvány
Híradástechnika, 2003/10, 27-30

[DÉNES T. 2003/6] Globális információ és személyes titkosítás
eVilág, II.évfolyam 11.szám, 2003/november

[DÉNES T. 2003/7] Bank-biztonság avagy a leggyengébb láncszem
http://www.titoktan.hu/_raktar/_e_vilagi_gondolatok/Leggyengebb_lancszem.htm

[DÉNES T. 2004/1] e-világi dramaturgia
eVilág, III.évfolyam 3.szám, 2004/március
http://www.titoktan.hu/_raktar/_e_vilagi_gondolatok/INFFEGYV.htm

[DÉNES T. 2004/2] Információbiztonság az e-társadalomban
eVilág, III.évfolyam 6.szám, 2004/június
http://www.titoktan.hu/_raktar/_e_vilagi_gondolatok/Inf_bizt_etarsadban.htm

[DÉNES T. 2004/3] Információbiztonság kontra polgári szabadságjogok 1-3.rész
eVilág, III.évfolyam, 2004/augusztus, november, december

[DÉNES T. 2004/4] Kódolatlan gondolatok (2001. szeptember 11-e harmadik évfordulóján)
eVilág, III.évfolyam 9.szám, 2004/szeptember
http://www.titoktan.hu/_raktar/_e_vilagi_gondolatok/SZEP11_3evf.htm

[DÉNES T. 2004/5] Globális fenyegetettség ellen globális információbiztonság
CEO Magazin, V.évf. 2004/3-4.

[DÉNES T. 2005/1] Latin négyzetek alkalmazása a kísérlet-tervezésben és kódolásban
Híradástechnika, 2005/1, 40-45
http://www.titoktan.hu/_raktar/_e_vilagi_gondolatok/Latinn_cikk2.htm

[DÉNES T. 2005/2] Latin négyzetek a titkosításban
Híradástechnika, 2005/3, 46-51
http://www.titoktan.hu/_raktar/_e_vilagi_gondolatok/Latinn_cikk3.htm

[DÉNES T. 2005/3] A dokumentumvédelem új módszerei (Személyhez kötött és tömeges dokumentumok) *eVilág, IV.évfolyam 4.szám, 2005/április, 26-29*
http://www.titoktan.hu/_raktar/_e_vilagi_gondolatok/Dokumentum_vedelem.htm

[DÉNES T. 2005/4] Biometrikus azonosítás, avagy a személy egyedisége és a dokumentum személyessége *eVilág, IV.évfolyam 5.szám, 2005/május, 34-38*

[DÉNES T. 2005/5] Információbizonytalanság az e-társadalomban, avagy a Közös Fiók Rendszer (Common Boksz System), mint egy új, biztonságos e-levelezési rendszer vázlata
Társadalomkutatás, 23.kötet 2005/2.szám 263-279
http://www.titoktan.hu/_raktar/_e_vilagi_gondolatok/CBS.htm

[DÉNES T. 2005/6] Digitális aláírás, avagy a dokumentum tartalmának és tulajdonosának hitelessége
eVilág, IV.évfolyam 6.szám, 2005/június, 6-10

[DÉNES T. 2005/7] Digitális ujjlenyomat, avagy a dokumentumvédelem periódusos rendszere
eVilág, IV.évfolyam 7.szám, 2005/július, 20-24

[DÉNES T. 2005/8] Digitális csőlátás, vagy az információs társadalom felkiáltójelei (interjú)
eVilág, IV.évfolyam 12.szám, 2005/december, 24-29
http://www.titoktan.hu/_raktar/_e_vilagi_gondolatok/Digitalis_csolatas.htm

[DÉNES T. 2006/1] Kiáltanék, … talán nem késő!
Népszabadság, 2006. június 20. /Fórum rovat/

[DÉNES T. 2006/2] Az Internet és a globális hálózatok biztonságáról
CEO Magazin, VII.évf. 2006/3. Melléklete (16 o.)
http://www.titoktan.hu/_raktar/_e_vilagi_gondolatok/INTERNET-biztonsag.htm

[DÉNES T. 2007] A biztonság konvergencia-programja
eVilág, VI.évfolyam, 2007/június, 1-8
http://www.titoktan.hu/_raktar/_e_vilagi_gondolatok/Biztonsag%20konvergencia.htm

[DÉNES T. 2008] Titok-megosztás
http://www.titoktan.hu/_raktar/_e_vilagi_gondolatok/TitokMegosztas.htm

[DÉNES T. 2009] „Meg kéne állni egy percre és elgondolkodni.” (interjú)
http://www.titoktan.hu/_raktar/_e_vilagi_gondolatok/DenesTamas-interjuPenzesL.htm

[DÉNES T. 2010] (Információ)biztonság a Nagy Testvér 60. születésnapján – I-II. rész.
Társadalomkutatás, 28.kötet 2010/4.szám 447-463, 29.kötet 2011/1.szám 112-130
http://www.titoktan.hu/_raktar/NagyTestver1.htm

[DÉNES T. 2011/1] Nyílt globalizáció ellen rejtett háború, avagy a terrorizmus „biztonsága”
CEO Magazin, XII.évf. 2011/3. melléklet

[DÉNES T. 2011/2] A terrorizmus „biztonsága” avagy a globális „harcrend” kudarca?
Gondolatok 2001. szeptember 11. tizedik évfordulóján
Társadalomkutatás, 29.kötet 2011/4.szám 475-493
http://www.titoktan.hu/_raktar/_e_vilagi_gondolatok/Terrorizmus-Biztonsaga.htm

További hivatkozások:

[DIFFIE-HELLMAN 1976] W.Diffie, M.Hellman: New Directions in Cryptography
IEEE Transaction on Information Theory, November 1976. (644-645)
http://www-ee.stanford.edu/~hellman/publications/24.pdf

[NBC 1975] Meet the Press
National Broadcasting Company, "Meet the Press" (Washington D.C.: Merkle Press, 1975), transcript of August 17, 1975, p. 6; quoted in Puzzle Palace, p. 477.
http://www.ncoic.com/nsapoole.htm#FN65

[ORWELL 1989] *G.Orwell: 1984, Európa Könyvkiadó, Budapest, 1989.*

[PFITZ 1996] Brigit Pfitzmann: Digital Signature Schemes.
Springer, Berlin, 1996
http://www.semper.org/sirene/people/birgit/BlurbPfit8_96.html

[SCHNEIER 1995] Bruce Schneier: e-mail security (How to Keep Your Electronic Messages Private), *Johns Wiley and Sons, Inc. New York, 1995.*

[SIMMONS 1982] Gustavus J.Simmons: Secure Communications and Asymmetric Cryptosystems, *Boulder, Westview Press, 1982.*

[VASVÁRI 2009] Vasvári György: A társadalmi és szervezeti (vállalati) biztonsági kultrúra,
AD-LIBRUM Kiadó, Budapest, 2009. (recenzió)