



Gazdag Ferenc

Bruce Schneier a biztonságról

Minden korszaknak megvannak a divatos fogalmai, amelyek a szokásosnál – s főként az indokoltnál – jóval gyakrabban szerepelnek a tömegkommunikációs és a köznapiszóhasználatban. Napjainkban kétségtelenül az egyik ilyen divatos ernyőfogalom a biztonság. Egy átlagos napi sajtótermékben könnyű fellelni a fogalom akár több tucat változatát is. Olvashatunk élelmiszerbiztonságról, közbiztonságról, ellátásbiztonságról, energiabiztonságról, katonai biztonságról, környezeti biztonságról, informatikai biztonságról, fizikai biztonságról, humánbiztonságról, adatbiztonságról, kollektív biztonságról, nemzetközi biztonságról, s a sor még könnyedén folytatható. A téma egyik osztrák szakértője, Heinz Gärtner egy 2005-ben kiadott írásában a biztonság fogalmának több mint száz különféle értelmezését gyűjtötte egybe. A jámbor olvasó bőséggel szemezgethet, s bizonyára megelégedi az igényei szerinti legmegfelelőbb változatot. Ha megtalálta is (minden felmérés a közbiztonsággal kapcsolatos értelmezések dominanciáját mutatja), ezzel még egyáltalán nem oldódik meg sem az alapfogalom – a biztonság – értelmezése, sem pedig az alapértelmezés alá besorolható ágazati értelmezések – a részbiztonságok – viszonya. Holott a konkrét területekre vonatkozó biztonságértelmezések önmagukban is külön világot, külön értelmezési területet képviselnek. Legyen elég csak a rendészettudományt említeni, amelyet külön bizottság képvisel az MTA keretein belül. Az elérhető információs csatornák sem könnyítik meg nemcsak az átlagolvasó, de még a téma iránt mélyebben érdeklődők

helyzetét sem. Az internetes kereső közel kétmillió találatot jelez a biztonság szóra, ami annak illusztrálására több mint elégséges, hogy valóban a divatos (s egyre inkább inflálódó) fogalmak egyikéről van szó. A témával foglalkozó szerzők sem jeleskednek áttekintő értelmezések készítésében, inkább a szakterületük biztonsági vonzatait taglalják.

Ilyen részterület az informatikai biztonság is, amelynek egyik nemzetközileg legjobban ismert „evangélistája” – az informatikusok egymás között így hívják a számítógépes ismeretek terjesztését szívügyüknek tekintő kollégákat – az amerikai Bruce Schneier. A 2008-ban angolul, s két évvel később magyarul is megjelent kötet nem az akadémiai értekezés kategóriájába tartozik, hanem a szerző 2002 és 2008 között megjelent cikkeinek tematikusan rendezett gyűjteménye. Amennyiben a kötet csak az informatika világról, a számítógépes rendszerek, adatbázisok és az információ biztonságáról szólna, valószínűleg nem fordították volna le a művet közel tucatnyi nyelvre, hanem megmaradt volna az informatikus szakma berkein belül. Azonban a szakmájában a legismertebbek közé tartozó Schneier messze túlnéz az informatika konkrét határain, s a biztonságot a határterületek terejében is értelmezi. A kötetben összegyűjtött, egy levegővételel olvasható írásai – amelyek egyébiránt mind megjelentek vagy a szerző Crypto-Gram című elektronikus hírlevelében, vagy saját honlapján – érintik az adatvédelmet, a repülésbiztonságot, az USA nemzetbiztonság működtetésének egyes kérdéseit, a biztonság

gazdasági és pszichológiai vonatkozásait, no és természetesen a számítógépek biztonságos működtetésének világát.

Nézzünk néhány gondolatmenetet a tu-
catnyi téma közül! Mindjárt a legelején ezt olvashatjuk: „A terrorizmus lényege a ré-
műletkeltés. Nem azok az emberek a való-
di célpontok, akiket a terroristák megölnek.
Ők csupán járulékos veszteség. Nem a re-
pülőök, a vonatok, piacok vagy buszok fel-
robbantása a cél. Ez csupán taktikai mű-
velet. A terrorizmus valódi célja mi többiek
vagyunk: az a több milliárd ember, akiket
nem ölnek meg, de ezekkel a gyilkos cse-
lekedetekkel megfélemlítenek. A terroriz-
mus valódi lényege nem maga a cselek-
mény, hanem az arra adott reakciónk. Mi
pedig pontosan úgy cselekszünk, ahogy a
terroristák szeretnék.”

Ezért a szerző arra hívja fel a figyelmet,
hogy a politikusok, valamint a sajtó munka-
társai ne játsszanak – akár szándék nélkül
is – a terroristák kezére sem azzal, hogy
politikai kampánytémává emelik a félelem
társadalmi hatásmechanizmusát, illetve,
hogy a sajtó ne nagyítsa fel az egyébként
is tragikus történeteket. Ezzel csak a terro-
risták által óhajtott rettegést növelik. A leg-
célszerűbb magatartás a terrorizmussal
szemben, ha egy társadalom nem hagyja
magát terrorizálni, azaz nem hagyja magát
megfélemlíteni. A szakértőknek pedig hi-
deg szakmaisággal kell elemezniük az
összes elérhető adatot. Akkor is, ha a fe-
nyegetés irreális, s végrehajthatatlan ele-
meket tartalmaz, mint a chicagói Sears to-
rony felrobbantását tervező Miami-7 cso-
port esetében történt. A vizsgálat végén
ugyanis kiderült, hogy a csoportnak se
eszközei, se szaktudása, se pénze, se pe-
dig tapasztalata nem volt a tervezett akció
végrehajtásához.

Schneier mélyebb rétegekbe is leás a
terrorizmus kapcsán, főként az *Attribúcióel-*

mélet és terrorizmus című írásában. Ebben
Max Abrahams értelmezésével vitatkozva
rámutat: bár az valós megfigyelés, hogy az
emberek jellemzően egy-egy cselekedet
hatásai alapján következtetnek a cselekvő
indítékaira (ez az attribúcióelmélet alaptézi-
se), a politika terrorizmusra adott válasza
– a kognitív torzítások jellemző példájaként
– többnyire hasonló logika alapján történ-
nek. Holott nem egyszer előfordul – mint
más elméletek esetén is –, hogy az esemé-
nyekből levont következtetés téves. A terro-
ristacsoportokat nem lehet sikeresnek mi-
nősíteni sem a társadalom meggyőzése,
sem a politikai változások kikényszerítése
tekintetében.

Külön írások foglalkoznak a kötetben a
kettős célú technológiákkal. A fogalom ere-
detileg azon termékeket jelöli, amelyeknek
– a felhasználó szándékától függően – egy-
aránt létezik polgári és katonai alkalmazá-
sa. E termékek nemzetközi forgalmát ezért
a hidegháború befejeződése után is egy
külön szabályozás regulálja (Wassenaar
Arrangement, 1995). De míg például a ra-
darrendszerek esetében, vagy a kémiai
alapanyagok feldolgozásának módjainál
nagyobb nehézségek nélkül azonosítható
a civil és a katonai felhasználás különbsé-
ge, addig az információs technológiák pol-
gári és katonai felhasználása között gy-
akorlatilag lehetetlen különbséget tenni. Ré-
szint azért, mert az informatika egészében
kettős felhasználású (ugyanazon operáci-
ós rendszereket, ugyanazon hálózati proto-
kollokat, ugyanazon alkalmazásokat, sőt
helyenként ugyanazon biztonsági szoftve-
reket használnak), továbbá azonos techno-
lógiát használnak mind a kibertámadások-
hoz, mind a védekezéshez. Az USA hadi-
tengerészetének Számítógépes Műveleti
Parancsnoksága ugyanazokat az eszközö-
ket használja hálózatai védelmére, mint
bármelyik nagyvállalat. Ráadásul felettébb



nehéz különválasztani a kiberháborút, a kiberterrorizmust és a kiberbűnözés fogalmát. Mivel a támadók és a védekezők ugyanazt az informatikai technológiát használják – írja a szerző –, alapvető feszültség jött létre a számítógépes támadási technikák és a védelmi megoldások között: amikor a fegyveres erő gyenge pontot fedez fel a kettős felhasználású technológiában, két dolog közül választhat. Riaszthatja a gyártót (amely kijavítja a sebezhető pontot, amellyel ezzel védi a jó- és rosszfiúkat egyaránt), vagy pedig titokban tartja a felismert biztonsági rést, nem szól senkinek sem, viszont ily módon egyaránt veszélyezteti a védekezőket és támadókat is. A szerző amelletts teszi le a garast, hogy a nemzeti biztonsági hivatalok igenis segítsék az informatikai cégeket a futtatott rendszerek biztonságosabbá tételében.

A szerző több oldalról is érinti a biztonság gazdasági és üzleti szempontjait. Kérdései egyidejűleg evidensek és teoretikusak, egyszerre gazdasági és műszaki jellegűek: a fejlett társadalmak elegendő pénz költenek-e arra, hogy távol tartsák a hackereket a számítógépes rendszerektől? Költenek-e eleget a rendőrségre és a hadseregre? A költségvetés biztonságra fordított hányadát megfelelő dolgokra használják-e fel? Mit lehet kezdeni a digitális szerzői jogokkal? A számítástechnikai cégek kezdeményezései valóban a biztonságot növelik-e, vagy csak a vevőket próbálják még jobban a Windows, a Media Player és az Office programokhoz láncolni? Az ilyen és ehhez hasonló kérdések jól mutatják, hogy

a modern gazdasági és üzleti szféra napjainkban elválaszthatatlan a számítástechnikától, azaz a biztonsági gondolkodástól. A szerző véleménye az, hogy a biztonság eleve speciális látásmódot kíván: „a biztonsági szakemberek nem tudnak belépni egy bolt ajtaján anélkül, hogy észre ne vegyék, miként lehet onnan bármit ellopni. Nem tudnak használni egy számítógépet anélkül, hogy el ne töprengjenek a biztonsági réseken. Nem tudnak szavazni anélkül, hogy meg ne próbálnák kideríteni, miként lehetne kétszer szavazni.”

Schneier konklúziójával csak egyetérteni lehet: „Ha az emberek megtanulják, hogyan kell gondolkodni saját, szűk látókörükön kívül, és nagyobb lesz a rálátásuk a dolgokra, akár a technológia, a politika, vagy a mindennapi életük területén, akkor sokkal rafináltabb fogyasztókká, szkeptikusabb polgárokká, és kevésbé hiszékeny emberekké válnak.”

Bruce Schneier könyve elvontnak tűnő tárgya dacára egyszerre élvezetes és tanulságos olvasmány: korunk a számítástechnika korszaka, s az információtechnológia a fejlődés egyik centrális eleme. Az informatikai biztonság mindennapjaink velejárója, akár tetszik, akár nem. A biztonság szélesen értelmezett terepében egyre nagyobb helyet követel, s számtalan felületen érintkezik annak politikai vetületével, a biztonságpolitikával. Jó kiadói döntés volt a válogatás közzététele.

(Schneier, Bruce: Schneier a biztonságról. Budapest, 2010, HVG Kiadó, 295 o.) ■