9. Bűnmegelőzés a kiberbűncselekmények területén

Dornfeld László

Az ENSZ meghatározása szerint a bűnmegelőzés „azon stratégiák és intézkedések összessége, amelyek a bűnelkövetés veszélyének, és az egyénekre, valamint a társadalomra potenciálisan káros következményeinek visszaszorítását célozzák a kiváltó okokra irányuló beavatkozásukkal", ugyanakkor a büntető igazságszolgáltatás szerepét is elismeri.[1] A bűnmegelőzés irodalma az elmúlt évszázadban jelentősen kibővült, és a kriminológia egyik legtöbbet kutatott területévé vált. A hagyományos bűnmegelőzés terén számos különböző irányzat alakult ki, a büntetőpolitikán belüli és azon kívüli eszközök igénybevételét irányzó beavatkozással (Borbíró 2011). Ugyan nem lehet elvitatni a büntetések szerepét az elrettentésben, ám az elkövetőn túlmutató, társadalmi mértékű elrettentő erejének (az úgynevezett generális prevenció) mértéke a mai napig vitatott. A bűnmegelőzésben kiemelkedő szerepet töltenek be a kormányok, a minisztériumi és hatósági együttműködések és partnerségek, a közösségi és civil szervezetek, a piaci szereplők és az egyének.[2] A bűnmegelőzési politika nélkülözhetetlen részei az alapelvek, a struktúra (bűnmegelőzési tervek), az implementáció eszközei (tudásbázis kialakítása) meghatározása és ezek átültetése a gyakorlatba (UNODC 2013, 225.). A kiberbűnözés újszerűsége és sajátosságai a kialakult bűnmegelőzési struktúrák számára is kihívást jelentenek. Ezek között említhetjük az online kapcsolódásra képes eszközök (számítógépek, laptopok, táblagépek, mobiltelefonok stb.) egyre növekvő számát és csökkenő árát, amelyek jelentősen növelik a potenciális elkövetők és áldozatok számát; az online teret igénybe vevő emberek nagyobb hajlandóságát arra, hogy deviáns módon cselekedjenek; az anonimitás és a nyomok elrejtésének lehetőségét az elkövetői oldalon; a transznacionális bűnözésből eredő bűnüldözési problémákat és az elkövetési technikák gyors fejlődését (UNODC 2013, 226.). A kiberbűncselekmények prevenciója esetén egyrészt fontos a megfelelő, specializált stratégia kialakítása, a minden érdekelt féllel történő együttműködés, valamint a hagyományos módszerek mellett a technológiai megoldások szerepét is fontos hangsúlyozni.

9.1. Stratégiák

2013-ban az ENSZ által vizsgált 53 állam mintegy egyharmada rendelkezett saját nemzeti kiberbiztonsági stratégiával (UNODC 2013, 227.), amely arány azóta bizonyosan magasabb. Ugyan erős kapcsolat áll fent a kiberbiztonsági és kiberbűnözés elleni stratégiák

[1] ENSZ Gazdasági és Szociális Tanács 2002/13. sz. határozata 3. §.
[2] ENSZ Gazdasági és Szociális Tanács 2002/13. sz. határozata 7–9. §.

https://doi.org/10.36250/00782_09

között, mégis fontos a kettőt megkülönböztetni egymástól. A fő különbség, hogy míg a kibervédelem egy reaktív tevékenység, addig a kiberbűnözés üldözése aktív magatartást igényel az érintett felektől (9. ábra). A további különbségeket a mellékelt ábra szemlélteti. A jelentősebb hatalmak közül az Amerikai Egyesült Államok, Ausztrália és az Európai Unió az előbbit, míg az Egyesült Királyság, Oroszország és Kína az utóbbit preferálja (LEVIN–ILKINA 2013).

9. ábra

Kiberbűnözés elleni kiberbiztonsági stratégiák

Forrás: SEGER 2011

A nemzeti stratégia megalkotása alapvető lépés a kiberbűncselekmények megelőzésében, hiszen ebben történik meg a működési és stratégiai prioritások meghatározása, amely alapján aztán normatív erejű jogszabály születhet. A stratégia ezen kívül alapdokumentumként szolgálhat a bűnüldöző és igazságszolgáltatási szervek számára saját belső eljárásrendjük kialakításában. A vizsgált stratégiák fele jelölte meg a megelőzést, a magánszektorral való együttműködést és a jogszabályalkotást prioritásként, míg kétharmaduk a nemzetközi együttműködés és a tudatosságnövelés fontosságát hangsúlyozta (UNODC 2013, 228.). A vezető szerep terén nincs általánosan elfogadott szerv: a vizsgált stratégiák mintegy harmada rendőri szervet jelölt meg, hasonló arányban került kijelölésre a feladatra az ügyészség és az igazságügyi minisztérium. Tíz százalék jelölt meg hatóságközi koordinációt, és hasonló arány kommunikációs vagy belügyminisztériumot, kiberbűnözés elleni szervet vagy CERT-et (UNODC 2013, 229–230.). Ez jól mutatja, hogy a legtöbb állam számára a kiberbűnözés elsősorban bűnügyi és nem technológiai kihívás. Kiberbiztonsági vonalon a hazánkban is jelentőséggel bíró nemzetközi dokumentumok közül ki kell emelni az Európai Unió kiberbiztonsági (JOIN/2013/01) és biztonsági [COM (2015) 185] stratégiáját, amelyek megszövegezése az eszközrendszer kialakítása terén egyenrangú prioritást biztosít a kiberbűncselekmények megelőzésének és felderítésének. Különösen fontos megemlíteni, hogy a Magyarország Nemzeti Kiberbiztonsági Stratégiájának [1139/2013. (III. 21.) Korm. rendelet] integráns része a megelőzésre törekvés. Már a dokumentum 1. szakaszában, a célok meghatározása között szerepel a „megelőzésre épülő hatékony védelmi intézkedések" megfogalmazása, a 9. szakasz *a)* és *d–e)* pontja pedig az ország számára követelményként rögzíti a hatékony megelőzést, a megfelelő oktatást, valamint a gyermekek számára biztonságos kibertér kialakítását. A 10. szakaszban megtalálható tényleges feladatok között helyt kapott a kormányzati koordináció, az együttműködés a civil, a gazdasági és a tudományos területek képviselőivel, a felhasználók

és vállalkozások körében tudatosság kialakítása, a megfelelő oktatás és kutatás-fejlesztés és a gyermekvédelem. A kiberbűnözés elleni stratégiák közül példaként hozható az Egyesült Királyság kiberbűnözési stratégiája, amelyet 2010-ben fogadtak el. A dokumentum első fele a kiberbűnözés különböző megjelenési formáira fókuszál, és azokat csoportosítja aszerint, hogy kire jelentenek veszélyt (a felhasználókra, a vállalkozásokra és a kormányzatra). A motiváció terén megkülönbözteti a pénzügyi előnyt eredményező, illetve nem eredményező bűncselekményeket. Ezután a dokumentum második fele a kormányzat, illetve a Belügyminisztérium fenyegetésekre adott válaszait mutatja be. A 39. pont a kiberbűnözés megelőzéséhez szükséges megfelelő védelmi intézkedések szükségességét tartalmazza, azzal az analógiával élve, hogy miként a gépjárművek és az otthonok védelméhez szükséges eszközök fontosak a bűncselekmények megelőzéséhez, úgy ugyanez igaz a kibertérben is. A prevenció számos bűncselekményi formánál és a különböző kormányzati szerveknél is kimondott prioritásként jelenik meg a dokumentumban.

Az átfogó stratégiák mellett szót kell ejteni az egy területre fókuszáló stratégiákról is. Ilyen például a gyermekvédelem területe, amely önmagában is elég jelentős ahhoz, hogy külön stratégia foglalkozzon vele. Az EU 2012-ben fogadta el az *A gyermekbarát internet európai stratégiája* (COM/2012/0196) dokumentumot, amely az Európai Unió, a tagállamok és az ágazati szereplők számára is határoz meg feladatokat. Hazánkban erre a területre fókuszál Magyarország Digitális Gyermekvédelmi stratégiája, amelyet a Digitális Jólét Programról szóló 2012/2015. (XII. 29.) Korm. határozat végrehajtásának részeként, a gyermekek és a személyiségi jogok védelmét szolgáló szabályok és intézkedések hangsúlyosabb érvényesítése érdekében alkottak meg. A dokumentum először meghatározza a digitális gyermekvédelem alapvető fontosságú tételeit, így a káros tartalmak és magatartások felismerését, az oktatás helyzetét, az érintettek szerepét és tapasztalatait. A második fejezet a védelmi megoldásokat (például a szűrőszoftvereket), illetve a gyermekek jogait tekinti át. A harmadik fejezetben a szankcióalkalmazás és segítségnyújtás eszközei kerülnek bemutatásra. A stratégia utolsó nagy része a cél- és eszközrendszert mutatja be.

Ez utóbbin belül a stratégia három pillért különböztet meg: tudatosság és médiaműveltség, védelem és biztonság, végül pedig szankcióalkalmazás és segítségnyújtás. A pilléreken belül meghatározott eszközök igen változatosak, némelyek a gyermekvédelem már meglévő eszközrendszerére támaszkodnak, vagy azt erősítik, mások a digitális kor vívmányainak tesznek eleget. Fontos kiemelni a tudatosítás és médiaműveltség fejlesztésének előtérbe helyezését az első pillérnél, a szűrőszoftverek fejlesztését és elérhetővé tételét, a veszélyes tartalmak korlátozását a másodiknál, a jogsértések monitorozását és adatbázis építését a harmadikban.

9.2. Programok, koordináció, ajánlások

A bűnmegelőzési programok a bűnelkövetés kockázati tényezőit veszik célba, és konkrét akcióterveket tartalmaznak ezek kezelésére, így csökkentve a bűnelkövetést. Ezek száma minden bűncselekmény esetén nő, és igaz ez a kiberbűnözésre is. Számos program kiindulópontja nemzetközi vagy szupranacionális szervezet, így az ENSZ, az EU vagy az Európa Tanács. Az ENSZ Közgyűlésének 65/230. sz. határozata, valamint a Bűnmegelőzési és Bűnügyi Igazságszolgáltatási Bizottság 22/7. és 22/8. sz. határozata kezdeményezte

2010-ben a Kiberbűnözés Elleni Általános Programot, aminek a végrehajtásával az ENSZ Kábítószer-ellenőrzési és Bűnmegelőzési Hivatalát (UNODC) bízták meg (UNODC 2013). Ez korántsem volt előzmény nélküli, ugyanis az ENSZ már ezt megelőzően számos kiberbűnözéssel kapcsolatos határozatot fogadott el, amiben a hatékonyabb globális fellépést, valamint a potenciális veszélyek korlátozását, megelőzését hangsúlyozza. Az Európai Bizottság *A gyermekbarát internet* európai stratégiájának részeként finanszírozza a tagállamokban működő *Safer Internet programokat*.[3] Ezek célja a tudatosság növelése és a digitális írástudás terjesztése a fiatalok, a szülők és a tanárok körében. Hazánkban 2010 óta zajlik a program keretében az iskolások biztonságos internethasználatra való oktatása. A program ezenkívül segélyvonalat és hotline-t is biztosít.

A 2015-ös Európai Bűnmegelőzési Díjra *(European Crime Prevention Award)* 19 tagállam nyújtott be valamilyen tervet. Ennek elsődleges témája volt a gyermekek és az internet problematikája.[4] Ezek közül az egyik a *TABBY (Threat Assessment of Bullying Behavior among Youth) in Internet* kutatás volt, ami az iskolai és online bántalmazás gyakoriságát vizsgálta öt országban (Bulgária, Ciprus, Görögország, Magyarország és Olaszország) 2011–2012-ben. A hazai program négy egymásra épülő modulból állt: a pedagógusok és diákok felkészítése az online bántalmazási esetek felismerésére és kezelésére, első panelfelvétel, érzékenyítő foglalkozások, végül a második panelfelvétel.[5] A kutatás eredményei önmagukban is sokat árulnak el a vizsgált jelenségről, valamint a későbbi iskolai bűnmegelőzési és devianciakezelési programok kidolgozása során a gyakorlatban is hasznosíthatók. Bár a program maga nem gyakorolt hatást az elkövetőkre, az áldozatok bántalmazásnak kitettsége jelentősen csökkent (PARTI et al. 2011). A luxemburgi *Bibi és barátai* program a 3–6 évesek első online tapasztalatait próbálta meg pozitív irányba befolyásolni. Ezeken kívül lengyel és litván online bántalmazás elleni program is volt a megvalósítottak között.

Az Európa Tanács és az Európai Unió 2013 és 2016 között futó közös programja, a Globális Akció a Kiberbűnözés Ellen (*Global Action on Cybercrime,* GLACY) hét ázsiai és afrikai országot érintett, akiket a Számítástechnikai Bűnözés Elleni Egyezmény iránti elkötelezettségük miatt választottak ki. Ennek részeként 135 eseményre került sor, amik a jogalkotástól és a bűnüldöző egységek felállításától kezdve az együttműködésen át a magánszektorral való együttműködésig széles spektrumon igyekeztek a kiberbűnözés elleni fellépést és a megelőzést előmozdítani.[6] A program tapasztalatai alapján indult el 2014-ben a *Cybercrime@Octopus* program.

Az Európai Unió a kiberbűnözés elleni küzdelem részeként, szervezeti alapként létrehozta a Számítástechnikai Bűnözés Elleni Európai Központot (*European Cybercrime Centre,* a továbbiakban: EC3) az Europol keretein belül, a szervezet meglévő infrastruktúrájának a felhasználásával. Ennek stratégiai központja foglalkozik a megelőzéssel és a tudatosság növelésével (DORNFELD 2016). Az EC3 az összegyűjtött adatok alapján elemzi

---

3 Safer Internet Program. Elérhető: https://ec.europa.eu/digital-single-market/en/content/creating-better-internet-kids-0 (A letöltés dátuma: 2018. 06. 01.)

4 EUCPN. Elérhető: https://eucpn.org/sites/default/files/content/download/files/toolbox_8.pdf (A letöltés dátuma: 2018. 06. 01.)

5 Eszter Alapítvány. Elérhető: www.eszteralapitvany.hu/wp-content/uploads/2013/03/Iskolaknak-TABBY-2013.03.12..pdf (A letöltés dátuma: 2018. 06. 01.)

6 Capacity building on cybercrime & e-evidence. Elérhető: https://rm.coe.int/16807069d8 (A letöltés dátuma: 2018. 06. 01.)

a kiberbűnözés kialakult trendjeit, és az ez alapján kiadott ajánlások segítik a hatékonyabb bűnmegelőzést.[7] A szervezet a főszervezője a Kiberbűnözés Megelőzési és Tudatossági Fórumnak, amelyen a tagállamokon kívül uniós szervek is képviseltetik magukat. A rendezvény célja a tevékenységek és kampányok összehangolása, a témába vágó tudásanyag megosztása, új megoldások kidolgozása és a jó gyakorlatok cseréje.[8]

Már 2004 óta működik az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA), amely az Európai Unió, a tagállamok, a magánszektor és az európai polgárok szolgálatában álló hálózat- és információbiztonsági szakértői központ. A szervezet feladatkörét 2013-ban jelentősen kibővítették. Feladata alapvetően a kapcsolódó uniós politikák kidolgozásában és alkalmazásában való részvétel, de segítséget nyújt a tagállamoknak is a felkészültségük fejlesztésében, az együttműködések elősegítésében, a figyelemfelkeltésben és a kutatás-fejlesztésben (Dornfeld 2016). A hazánkban működő Nemzeti Kibervédelmi Intézet részeként operáló Kormányzati Eseménykezelő Központ, valamint a Nemzeti Elektronikus Információbiztonsági Hatóság honlapján riasztásokat ad ki az új fenyegetések és sérülékenységek kapcsán, valamint szabadon elérhető ajánlásokkal és tanácsokkal, tudatosító anyagokkal vesz részt a bűnmegelőzésben.

9.3. Együttműködés a magánszektorral

Az együttműködésnek és koordinációnak a kormányzati szerveken kívül a magánszektorral is nagy jelentősége van. Hiszen a biztonság kialakításában, a jogellenes cselekmények felderítésében az IT-iparág és az internetszolgáltatók is fontos szerepet játszanak. Különösen igaz ez a nyugati világban, amely partnerként kezeli ezeket a szereplőket a kiberbiztonságban. Ennek a szabályozási modellnek az elnevezése a *minden érdekelt fél bevonása,* ahol nagy tér jut a kölcsönös előnyökkel járó együttműködésnek (Dornfeld 2016). Ezen együttműködés kialakításának alapja az, hogy az állam működésének biztosításához elengedhetetlen a kritikus infrastruktúra védelmének biztosítása, ám ezek nagy része magántulajdonban van (Carr 2016). Az ENSZ-felmérésben vizsgált 35 ország mintegy fele rendelkezett már kialakított együttműködési programmal, míg harmadukban nem létezett ilyen és előkészítés alatt sem állt (UNODC 2013, 231.).

A magánszektorral történő együttműködésnek öt elsődleges modellje alakult ki: 1. non-profit globális információmegosztás, 2. osztott közösségi szintű információmegosztás, 3. központi közösségi szintű információmegosztás, 4. zárt kormányzat, 5. informális együttműködés (UNODC 2013, 232.). Más szerzők aszerint tesznek különbséget, hogy van-e az együttműködésben olyan fél, amely hierarchikusan a többiek felett áll. Ezek alapján különbséget tesznek horizontális és hierarchikus együttműködések között (Carr 2016, 54.). A horizontális vagy informális együttműködés elsősorban az angolszász országokra jellemző megoldás, ahol a felek egyenrangú partnerekként vesznek részt, nem jogszabályi kötelezettség, hanem felismert közös érdekek alapján. Az Egyesült Királyság

[7] Europol EC3. Elérhető: www.anacom.pt/streaming/Benoit_Godart.pdf?contentId=1176117&field=ATTACHED_FILE (A letöltés dátuma: 2018. 06. 01.)

[8] Europol. Elérhető: www.europol.europa.eu/newsroom/news/cybercrime-prevention-%E2%80%93-unified-message-towards-online-criminals (A letöltés dátuma: 2018. 06. 01.)

kiberbiztonsági stratégiája például „közös kihívás"-t fogalmaz meg, ahol szükséges „a magánszektor, az egyének és a kormányzat" együttműködése (CARR 2016, 55.). Linder ezzel szemben hat különböző modellt határoz meg, és a neoliberális, illetve neokonzervatív ideológiákhoz köti ezeket. Így például az egyik által felállított modell az „együttműködés mint menedzsmentreform", amely szerint a kormányzati tisztviselők utánozni kezdik partnereiket, és a szigorú bürokratikus szabályalkotás helyett vállalkozói és rugalmas módon kezdenek el működni (CARR 2016, 55–56.). Ennek érdekessége az, hogy jelen esetben a kormányzati szervek idomulnak a magánszektor működéséhez, és nem fordítva. Ennek jelentősége, hogy informális együttműködés – hiába alapul az közös érdeken (DAHABIYEH 2015, 2–4.) – kialakításában nehézséget jelent az, hogy az üzleti élet szereplői gyakran bizalmatlanok az állammal szemben, az állami szervek eljárását túl merevnek tartják. Jól összefoglalja ezt az a vélekedés, hogy „ha az egyetlen eszközöd a kalapács, az egész világ szögnek tűnik" (WOLF 2001). Az együttműködések túlnyomó többsége informális, általában csak a kritikus infrastruktúrát szolgáltatók esetén léteznek kormányzati döntésen vagy jogszabályon alapuló együttműködések (UNODC 2013, 232.). Az együttműködés legtipikusabban információcserére és segítségnyújtásra terjed ki, de hasonlóan gyakori a tudatosság növelése és a jó gyakorlatok cseréje. Jóval kevésbé jellemző a technikai megoldások kidolgozásába, illetve a nemzetközi együttműködésbe történő bevonás, és szinte elenyésző a politikák kialakításában van részvétel (UNODC 2013, 233.).

A Világgazdasági Fórum 2016-os ajánlása öt pontban tartalmaz javaslatokat az együttműködésre.[9] Az első ezek közül az állandó és biztonságos *információs csatornák kialakítása,* valós idejű információmegosztás a CERT-ekkel, valamint a technikai megelőzés eszközeinek és a tapasztalatoknak, illetve a jó gyakorlatoknak a megosztása. Az ilyen szintű információcsere szükségessége összefügg azzal a problémával, hogy nem mindig egyértelmű egy-egy esetben eldönteni, hogy valamilyen technikai hiba vagy pedig kibertámadás történt-e (CARR 2016, 58.). Ráadásul a látencia is igen jelentős a kiberbűnözés esetén, ami vagy abból ered, hogy nem ismerik fel a támadásokat az áldozatok, vagy abból, hogy a közvélemény szemében való bizalomvesztéstől, illetve az üzleti titkaik kitudódásától való félelmükben nem jelentik be azokat (DORNFELD 2015, 29.). Mivel a magánszektor szereplőitől begyűjtött adatok potenciálisan piaci versenytársaikhoz is eljuthatnak, ezért kellő körültekintéssel kell eljárni, és csak olyan információkat megosztani, amelyek nem sértenek üzleti titkot. Ilyen módon csökkenthető a bizalmatlanság a hatóságokkal szemben (BRENNER–CLARKE 2005, 684.). A második javaslat a globális, illetve *regionális szintű együttműködési platformok* felállítását szorgalmazza, ami összefügg a kiberbűnözés mint probléma globális, határokon átnyúló jellegével. Ilyen például az INTERPOL égisze alatt működő Globális Innovációs Komplexum (*Global Complex for Innovation,* IGCI).[10] Hasonló együttműködés létezik az Interpol és a bankkártya-szolgáltatók között, ami a csalás visszaszorítását szolgálja (LI 2007). A negyedik javaslat a korábban már említett bizalmatlansággal összefüggésben a *bizalomépítést,* a *párbeszédet* és a *kapacitásépítést* emeli ki.

[9] World Economic Forum Recommendations for Public-Private Partnership against Cybercrime. January 2016. 6–10.

[10] Interpol. Elérhető: www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation/Implementation (A letöltés dátuma: 2019. 06. 10.)

9.4. Oktatás, tudatosság kialakítása

Az ENSZ Bűnmegelőzési Iránymutatásai kiemeli a közoktatás és a tudatosságnövelés fontosságát. A viktimizációs veszélyek ismerete és a védelmi intézkedések szélesebb körű ismertetése alapvető fontosságú a sikeres bűnmegelőzéshez (UNODC 2013, 234.). A kiberbűnözés viktimizációja erősebben jelentkezik a fejletlenebb országokban, ami azt mutatja, hogy itt még nagyobb szükség van a megfelelő megelőzésre, elsősorban a tudatosság növelésén keresztül.[11] Ennek eszközrendszere meglehetősen széles lehet, internetes figyelemfelhívó kampányoktól kezdve, kiberbiztonsági napok szervezésén keresztül egészen az akadémiai szféra és az oktatás bevonásáig. A kampányokat tipikusan állami szervek készítik nemzeti szinten, de léteznek regionális szintű és techcégek, illetve nonprofit civil csoportok által kezdeményezett események is. Erre lehet példa a Google tevékenysége (UNODC 2013, 236.).

A megfelelő figyelemfelhívó kampány kialakítása meglehetősen nehéz lehet. Egy 2011-es felmérés szerint sok ilyenhez egyáltalán nem kapcsolódik utólagos értékelés, és azt is nehéz eldönteni, hogyan lehet minél költséghatékonyabb módon a megfelelő hatást elérni. Hasonlóan komoly probléma a technikai oldalon, hogy további tréningek és képzések nélkül csak korlátozott hatást képesek elérni. A felmérés szerint a leghatékonyabbak az egyszerű, egy adott csoportot célzó kampányok (UNODC 2013, 236.). A felmérések szerint mára a legtöbb internetfelhasználó az alapvető óvintézkedéseket megteszi internetezés közben.[12] A figyelemfelhívásnak és tudatosításnak így inkább valamely kifejezett veszélyre kell vonatkoznia, például a zsarolóvírusokra vagy a botnetekre, nem kizárólag általánosságokra. Továbbá fontos azt is észben tartani, hogy a javasolt biztonsági megoldások ne legyenek túl bonyolultak, mert ez csökkentheti a felhasználók hajlandóságát, hogy alkalmazzák azokat.[13] Például a gyakorlati javaslatok ellenére meglehetősen valószínűtlen, hogy egy átlagos felhasználó minden szolgáltatáshoz külön jelszót fog használni, ezeket rendszeresen cseréli, és anélkül emlékszik rájuk, hogy bárhová felírná őket. A veszélyekkel kapcsolatos oktatást minél hamarabb szükséges elkezdeni, ugyanis a fiatalok hatványozottan kitettek az interneten található veszélyeknek. Ennek első lépése a köznevelés, ahol szükséges a tanárok továbbképzése is, hogy ők maguk is tisztában legyenek a veszélyekkel, illetve a rájuk adható jó válaszokkal. Ennek céljait jelentősen segítheti az is, ha állandó kapcsolat alakul ki a helyi rendőrség és az iskolák között, így egy gyakorlati tapasztalatokkal is rendelkező előadó tud az oktatási tevékenységen részt venni.

Az akadémiai szféra szerepe változó lehet a megelőzés terén, így például részt vehetnek az oktatásban és a szakemberek képzésében, a jogszabályok és vonatkozó politikák, illetve a technikai standardok és megoldások kidolgozásában. Az egyetemeken gyakran találhatók specializált kutatóintézmények és kiberbűnözési szakemberek is. A kiberbűnözés elleni küzdelemhez felhasználható tudásanyag számos tudományos diszciplínában megtalálható,

---

[11] Comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector. UNODC/CCPCJ/EG.4/2013/2. 3.

[12] Comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector. UNODC/CCPCJ/EG.4/2013/2. 12.

[13] Comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector. UNODC/CCPCJ/EG.4/2013/2. 12.

így többek között a számítástechnikában, a jogban, a kriminológiában és a szociológiában. Az elmúlt évtizedekben egyre nőtt az ezen témákkal foglalkozó folyóiratok és kutatások száma, és az elméleti tudást a gyakorlatban is fel lehet használni (UNODC 2013, 236–237.).

Brenner javaslata a jelenlegi rendszer helyett egy *osztott rendészeti stratégia* létrehozása, ahol nem a rendőrség, hanem az állampolgárok elsődleges feladata a kibertér biztonságának őrzése. Az ő elképzelése szerint a rendőrség feladata ebben a rendszerben az elrettentés és megelőzés lenne, míg a felhasználókat jogszabályok köteleznék bizonyos magatartásokra, így például az illegális tartalmak jelentésére vagy bizonyos szoftverek telepítésére (CHANG 2017). Chang is a lakosság növekvő szerepét emeli ki, felhívva arra a figyelmet, hogy mivel a legtöbb rendszer ugyanolyan zárt forráskódú szoftvereket használ, egy sebezhetőség felfedezése láncreakciót indíthat el (WALL 2008). Jól mutatja ennek potenciális veszélyét a *WannaCry* zsarolóvírus futótűzszerű elterjedése is (NAGY–MEZEI 2017).

9.5. Technológiai eszközök a bűnmegelőzés szolgálatában

A technológia bűnmegelőzési célú felhasználása nem új keletű gondolat, így a kiberbűncselekmények prevenciója terén is hamar felmerült alkalmazása. Ennek elméleti alapja szorosan kapcsolódik a szituációs bűnmegelőzéshez, amelynek lényege szerint a bűnözés azáltal csökkenthető, ha nehezebbé tesszük a bűncselekmények elkövetését, csökkentjük a várható előnyöket vagy növeljük az elkövető kockázatát. Ez a fajta hozzáállás népszerű állami szinten is, így például Nagy-Britannia kibertérrel kapcsolatos politikájában is, ahol az állami kezdeményezések a fejlesztőket a bűnözésre való lehetőségek csökkentésére ösztönzik. Az elmúlt évtizedben két egymástól elkülöníthető modell alakult ki a szakirodalomban: a rendszerek bűnmentessé tétele, illetve a bűnmegelőzés beépítése a rendszerbe.

9.5.1. Modellek

A rendszerek bűnmentessé tétele azon az elképzelésen alapszik, hogy a lehetőségét is meg kell szüntetni a rendszer jogellenes használatának. Ilyen megoldás lehet például, ha egy vállalkozás kizárja a közvetlen bankkártyás fizetés lehetőségét, és csak letéti fizetési rendszerek (például PayPal) közbeiktatásával enged fizetni, ami jelentősen csökkenti a bankkártyás csalások lehetőségét. Hasonló megoldás, ha egy információs rendszer tervezésekor a biztonsági beállítások alapállapotban bekapcsoltak. Ennek a megközelítésnek ugyanakkor sok buktatója van, így például az, hogy a tervezési szakaszban nem határozható meg előre, mennyire sikerült a bűnözési lehetőségeket kizárni, valamint, hogy a mindennapi használatot túlságosan nehezítő védelem esetén az átlagfelhasználók hajlamosak kikapcsolni a védelmi funkciókat, mivel a funkcionalitás fontosabb számukra (WALL 2008, 188.).

A másik megoldás a bűnmegelőzés rendszerbe építése, amelyek közül a legismertebb a felhasználónév-jelszó kombináció, ami szükséges a védett rendszerekbe történő belépéshez. A használható eszközök között kap helyet az adatbányászás is, ami az összegyűjtött és tárolt forgalmi adatok elemzését jelenti, mivel ezek tartalmazzák az összes internetes tranzakciót. Ezzel a technikával számos fontos információ kinyerhető, és a *kockázati társadalom* rendfenntartásának egyik alapköve lehet, ahogy a rendvédelmi szervek közötti

kapcsolatoknak is egyre fontosabb részét képezi az információmegosztás. Az információközvetítés bűnmegelőzésben betöltött szerepét az Egyesült Államokban is felismerték, ahol a 9/11-es terrortámadást követően javasolták az összes fontos nemzeti adatbázis egyesítését (Wall 2008, 189.). Ez nemcsak a kibertérben, de azon kívül is igen hasznos lehet, így például a 2016-os nizzai kamionos terrortámadást is meg lehetett volna előzni, ha megfelelően használják és összevetik a francia listákkal a Schengeni Információs Rendszert.[14] A bűnözéskontroll másik módja lehet a szoftveres bűnmegelőzés beépítése, anélkül, hogy az a hardware-t érintené, ezáltal automatizált, aktív rendfenntartó eszközöket létrehozni. Ilyen lehet például egy olyan honlap létrehozása, ami külsőre valósnak tűnik, és látszólag illegális tartalmakkal van feltöltve, ám ehelyett egy rendőrségi figyelmeztetés fogadja a látogatókat (Wall 2008, 190.). Gyakorlati példaként hozható az Europol *Police2Peer* programja, amelynek részeként a *peer2peer* fájlcserélő rendszereken folyó gyermekpornográfiaterjesztés ellen léptek fel. A rendőrök látszólag gyermekpornográf tartalmú fájlokat tettek közzé, ám ezek a valóságban egy rendőrségi figyelmeztetést tartalmaztak az azt letöltők számára.[15] Ezek a fajta tartalmak azonban ellenkező hatást is elérhetnek: vicces kedvű felhasználók látszólag ártalmatlan címek mögé rejthetik a rendőrségi figyelmeztetésre mutató linket, ami az egyszerű felhasználókban pánikot okozhat. Rosszabb esetben a bűnelkövetők dolga egyszerűsödhet, ha például egy fiatalkorúnak, akitől meztelen képet csaltak ki, megmutatnak egy olyan figyelmeztetést, hogy az ilyen képek készítése bűncselekmény, így további szexuális szolgáltatásokat zsarolhatnak ki belőle. Katyal is azon az állásponton van, hogy a kód megfelelő felhasználása a bűnmegelőzés céljait segítheti elő. Véleménye szerint ehhez az offline bűnmegelőzési eszközökből merítve négy alapelv betartására van szükség: 1. természetes megfigyelés lehetőségének megteremtése; 2. területiség érzésének keltése; 3. közösségépítés; 4. a bűncselekmények célpontjainak védelme. Az első pont alapján például amellett érvel, hogy a zárt forráskódú szoftverek biztonságosabbak, mint a nyíltak. A területiségnél az *ellenőrzött pszeudoanonimitás* mellett foglal állást, vagyis az IP-címek logolását javasolja megoldásként, ahol megmarad az anonimitás, de könnyebbé válik a hatóságok dolga (Chang–Grabosky 2008, 537.).

9.5.2. Tartalomszűrés

A megelőzés technikai megoldásai közé sorolható a tartalomszűrés is. Ez nem más, mint a különböző jogsértő tartalmak kiszűrése, majd eltávolítása vagy más módon történő elérhetetlenné tétele. A szűrésnek három szintje különböztethető meg: az elsődleges szint a felhasználói, ahol a számítógépet használó vagy az azt üzemeltető intézmény állítja be a szűrés mértékét; a második szint az internetszolgáltató által alkalmazott szűrés; míg a harmadik szint pedig az állam által előírt tartalom blokkolása (Parti–Marin 2012, 58.).

Az első szinten történő szűrés egyik fontos eszköze a szűrőszoftverek, ahol a felhasználó maga állíthatja be a szűrni kíván tartalmakat. Az elektronikus hírközlésről szóló 2003. évi C. törvény 149/A. § előírja az internet-hozzáférési szolgáltatást nyújtó

[14] EPP. Elérhető: www.eppgroup.eu/news/Five-lessons-learned-from-the-terror-attacks-in-France (A letöltés dátuma: 2018. 11. 12.)

[15] Europol. Elérhető: www.europol.europa.eu/partners-agreements/police2peer (A letöltés dátuma: 2018. 11. 12.)

szolgáltatónak, hogy a kiskorúak védelmét lehetővé tevő, magyar nyelvű, könnyen telepíthető és használható szoftver letöltését ingyenesen elérhetővé kell tenni. A Gyermekvédelmi Internet-kerekasztal kapcsolódó 5/2014. (IV. 23.) sz. ajánlása javaslatokat fogalmaz meg e szoftverek elérhetősége, telepítése és beállítása, a korlátozása módja és a tevékenységek monitorozása, illetve a riasztások kapcsán; továbbá előírja az oktatási intézmények számára a szoftverek alkalmazását.

A harmadik szinten történő tartalomszűrés egyik alapját az Európai Unió a gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről szóló 2011/93/EU irányelve teremti meg, amelynek *A gyermekpornográfiát tartalmazó vagy azt terjesztő weboldalak elleni intézkedések* címet viselő 25. cikke kötelességként írja elő az ilyen weboldalak eltávolítását, illetve az ezekhez való hozzáférés meggátolását. Ennek hazai jogszabályokba történő átültetése a Büntető Törvénykönyv 77. §-ba foglalt elektronikus adat végleges hozzáférhetetlenné tétele intézkedésként, illetve a büntetőeljárási törvény 335. § szerinti elektronikus adat ideiglenes hozzáférhetetlenné tétele kényszerintézkedésként történt meg. A 23/2003. (VI. 24.) BM–IM együttes rendelet alapján a kényszerintézkedés elrendelésére a nyomozó szerv vezetője tesz előterjesztést az ügyészhez, az előterjesztésnek az egyéb releváns adatok mellett tartalmaznia kell az IP-címet IPv4- vagy IPv6-szabvány szerint és az alhálózati maszkot, a domainnevet, az URL-címet, valamint a portszámot. Ugyan a jogintézmény elsődleges célja a már folyamatban lévő bűncselekmények megszakítása, a megelőzés célját is szolgálja az, hogy ezek a tartalmak elérhetetlenné válnak, így más már nem férhet hozzájuk.

9.5.3. Sweetie-projekt

A holland Terre des Hommes gyermekjogi civil szervezet 2013-ban digitális képalkotási technikával létrehozott egy virtuális filippínó kislányt, és négy kutató 10 héten keresztül megszemélyesítette őt. Ezalatt az idő alatt 20 ezren léptek velük kapcsolatba nyílt chatszobákban, és mintegy 1000 elkövetőt tudtak azonosítani 71 különböző országból.[16] Ugyan ezeket az adatokat átadták a joghatósággal rendelkező hatóságoknak, nagyon kevés esetben indult eljárás, elsősorban a kutatók potenciális ráhatása miatt, amit az elkövetők védekezésként felhozhattak volna. A büntetést nehezíti az, hogy Sweetie csak egy „virtuális áldozata" egy bűncselekménynek, valamint, hogy semmiféle szexuálisan explicit dolgot nem tesz (SCHERMER et al. 2016). Mindezen tényezők megnehezítik azt, hogy a begyűjtött adatok alapján ténylegesen eljárás indulhasson. Az első projekt ezek ellenére sikeresnek volt tekinthető, hiszen világméretű médiafigyelmet kapott, és így sikerült a problémát a figyelem középpontjába állítani. Ennek sikerén felbuzdulva a szervezet elindította a Sweetie 2.0 projektjét, ahol már egy kenyai kisfiút és egy másik filippínó lányt személyesítenek meg. A Terre des Hommes dokumentumaiban maga is proaktív eszközként jellemzi Sweetie-t, aminek segítségével még azelőtt avatkozhatnak be, hogy tényleges bűncselekmény történne. Sweetie ugyan nehezen alkalmazható a bűnözők elítéléséhez, a megelőzésben igen fontos szerepet tölt be, ugyanis elbizonytalaníthatja az elkövetőket, akik sosem tudhatják,

[16] Webcam Child Sex Tourism. Elérhető: www.terredeshommes.org/wp-content/uploads/2013/11/Webcam-child-sex-tourism-terre-des-hommes-NL-nov-2013.pdf (A letöltés dátuma: 2018. 11. 12.)

nem egy virtuális kislánnyal folytatnak-e épp beszélgetést, aki mögött kutatók figyelik tevékenységüket.

9.6. Egyes bűncselekménytípusok megelőzésének kérdései

9.6.1. Agresszió és online megfélemlítés

Az online megfélemlítés *(cyberbullying)* a kutatások fókuszába kerülő egyik új jelenség, aminek sokrétűsége nehézzé teszi a megelőzést. Így például a szándékos, célzott bántalmazást célzó eszközök nem feltétlenül járnak sikerrel olyan esetben, ha valaki hirtelen felindulásból válaszol így egy provokációra. Ugyanígy a bosszúból történő elkövetést célzó eszközök hatástalanok lehetnek azzal szemben, aki csak szórakozásból, trollkodásból végzi a tevékenységét. A különböző motivációkkal és megjelenési formákkal foglalkozik az agressziókutatás, amelynek a kibertérben történő agressziónál nagy jelentősége van. A kutatások tanulsága szerint az online zaklatás elkövetőit legtöbbször a kikapcsolódás igénye, az unaloműzés, a bosszú, illetve a mások feletti hatalom érzete vezérli. A motivációk tanulmányozása és feltárása hasznos tapasztalatokat jelent a jelenség megelőzéséhez, illetve a beavatkozáshoz (Runions et al. 2016, 75.).

A *cyberbullying* ellen nem jelenthet megoldást, ha kikapcsoljuk az áldozat elektronikus eszközeit, és megfosztjuk az internethozzáféréstől, hiszen ezzel tulajdonképpen őt büntetjük meg. A bántalmazás során jelentősége van a családon belüli érzelmi kapcsolatoknak is, a felmérések szerint ugyanis az érzelmi támogatás mérsékelte az online zaklatás negatív következményeit, és csökkentette az ismétlődés veszélyét is. Rajtuk kívül azonban fontos az egészségügyi, iskolai dolgozók bevonása a megelőzésbe, illetve a kortársak, akik egymást támogatva védőhálót nyújthatnak az ilyen próbálkozások ellen. Az érintetteken túl a szemlélőknek is fel kell ismerniük, hogy a bántalmazás sikeréhez az is elegendő, ha passzívak maradnak, és nem sietnek a bántalmazott segítségére (Zsila–Ujhelyi–Demetrovics 2015, 57–58.). Magyarország Digitális Gyermekvédelmi Stratégiája a büntetőeljárás helyett az alternatív vitarendezési mechanizmusokat helyezi előtérbe, és előbbit kizárólag utolsó megoldásként kívánja alkalmazni. Az online megfélemlítésre adott válaszok közül a legnépszerűbbek azok, amelyek valamilyen módon megbirkóznak vele (úgynevezett megküzdési stratégiák). Ilyen például a bántalmazó tiltólistára helyezése/blokkolása, az online név vagy telefonszám megváltoztatása. Léteznek azonban rossz megoldások is a helyzet kezelésére, így például, ha valaki maga is megfélemlítéssel válaszol. Arra azonban már ritkábban, utolsó lehetőségként kerül sor, hogy ezeket az incidenseket szülőkkel, tanárokkal közöljék, ami az életkori sajátosságokon túl abból is ered, hogy úgy érzik, ők nincsenek tisztában a probléma mértékével (Slonje–Smith–Frisén 2012, 5.).

Az online megfélemlítés kezelésének legjobb módja az iskolai megelőzés, illetve beavatkozás. Ilyen például, ha ráébresztjük az elkövetőt, hogy milyen következményekkel járnak tettei az áldozatra nézve. Ennél a bűncselekménynél különösen nagy jelentősége van a tudatosításnak és a felelősségteljes internethasználat oktatásának (Slonje–Smith–Frisén 2012, 6.). A megfelelő szemléletmódot nemcsak az érintettekkel, de a szülőkkel, tanárokkal és a szélesebb társadalommal is meg kell ismertetni. Hazánkban 2015-ben került megrendezésre a Magyar Országos Cyberbullying Konferencia (MOCK), ahol a tudományos

élet képviselői mellett a Nemzeti Média- és Hírközlési Hatóság és a Nemzeti Adatvédelmi és Információszabadság Hatóság tagjai is részt vettek.

9.6.2. Szexuális devianciák

A szexuális vágyak kiélése a kibertérben elkövetett bűnözés másik jelentős csoportja. Az új információs technológiák fundamentálisan eltérő módokon teszik lehetővé a gyermekek és nők kizsákmányolását. A kulturális befolyásuk révén ezek a technológiák jelentősen kiterjesztik az erőszak elfogadásának a mértékét, és normalizálnak olyan tevékenységeket, amelyek korábban elfogadhatatlanok voltak (MALTZAHN 2006, 7.).

A *groominghoz* és a gyermekkel történő *sextinghez* hasonló tevékenységeket nagyon nehéz kiszűrni, és fellépni ellenük. Ugyanígy problémás a gyermekpornográfia terjesztésének megakadályozása, amely szinte robbanásszerű növekedésnek indult az új technológiák nyújtotta lehetőségeknek köszönhetően (DORNFELD–MEZEI 2017, 32.). Számos szegényebb országban, így például a már említett Fülöp-szigeteken elterjedt az a gyakorlat, hogy a szülők maguk kényszerítik a gyermekeket, hogy élőben streameljenek szexuális tevékenységeket. A helyi hatóságok sokáig nem léptek ez ellen fel, míg végül 2012-ben megszületett a kiberbűncselekmények megelőzéséről szóló törvény, ami fellép a *kiberszex* és a gyermekpornográfia ellen is. A fellépés nemcsak a gyermekeket kényszerítő felnőttek, de a szexkamera-turisták ellen is megtörtént, ami alapvető fontosságú. Ha a keresleti oldalt nem érik behatások, a jelenség sem szűnik meg, csak más, a problémára kevésbé érzékeny országokba kerül át. Mindemellett jelentős tudatosítási erőfeszítésekre is sor került az iskolákban, ahol a kiberszex veszélyeire hívták fel a fiatalok figyelmét.[17]

A Fülöp-szigeteken történt változás egyfajta modellprogramnak is tekinthető, amely a hasonló helyzetű országokban alkalmazható. Az Európai Bűnmegelőzési Hálózat által Romániában folytatott kutatás európai környezetben is a tudatosítás fontosságát jelzi.[18] A tapasztalatok szerint egyrészt meg kell ismertetni a fiatalokkal a jelenséget, és lehetővé tenni azt, hogy jelentsék, másrészt fel kell hívni a figyelmüket, hogy a szexuális tartalmú képek maradandó károkat képesek okozni. Fontos azonban figyelembe venni, hogy az elkövetők egy kisebb köre az, aki a gyakorlatban is részt vesz a gyermekpornográf anyagok elkészítésében, a többiek csak a fogyasztásukkal generálják az igényt rá. A fogyasztás első időszakában még csak érdeklődőkről, később letöltőkről, gyűjtőkről, majd legvégül előállítókról beszélhetünk. A sikeres fellépéshez elengedhetetlen az, hogy ez a folyamat ne érje el az utolsó fázisát, és pontosan e beavatkozás miatt volt fontos például a korábban már említett holland Sweetie-projekt.

---

17 Terre des Hommes: *Children of the Webcam. Updated Report on Webcam Child Sex Tourism.* Elérhető: www.savesweetienow.org/sites/default/files/2017-03/HR%2017021%20TdH%20Report%20Webcam%20-Manilla.pdf (A letöltés dátuma: 2018. 06. 10.)

18 EUCPN. Elérhető: https://eucpn.org/document/prevention-and-investigation-child-pornography-cases-internet-partnership-romanian-police (A letöltés dátuma: 2018. 11. 12.)