DOI: 10.38146/BSZ-AJIA.2025.v73.i3.pp593-608

Crowdsourcing – lehetőségek és korlátok nemzetbiztonsági szemmel

Crowdsourcing – opportunities and limitations from national security perspective

Dobák Imre
Dr., PhD, egyetemi docens, intézetvezető
Nemzeti Közszolgálati Egyetem,
Nemzetbiztonsági Intézet
dobak.imre@uni-nke.hu

Bérczi Péter
doktorandusz
Nemzeti Közszolgálati Egyetem,
Hadtudományi Doktori Iskola
bereczki.peter@stud.uni-nke.hu

Absztrakt

Cél: A biztonságunkat érintő környezet folyamatos változásával, a technológiai fejlődés és a globális összekapcsoltság gyorsuló hatásával, felértékelődnek azok az innovatív megoldások, amelyek a társadalom tagjait is bevonva járulhatnak hozzá a biztonság növeléséhez. Ezek között jelennek meg a crowdsourcing modellre épülő megoldások, amelyek a társadalom különböző csoportjait megszólítva, a közösségi együttműködés előnyeit felhasználva lehetnek eredményesek a biztonságot szolgálaló tevékenységek egy-egy területén. A módszer nem új, azonban a kibertér lehetőségei előtérbe hozták a társadalom tagjainak a megszólíthatóságát és az ehhez kapcsolódó kutatási irányokat.

A módszer előnyei közé tartozik a gyorsaság, költséghatékonyság és a humán erőforrások bővítése, ugyanakkor felmerülnek kihívások is, mint az adatbiztonság, az adatok hitelessége és az adatok manipulálása. A tanulmány célja, hogy ráirányítsa a figyelmet a crowdsourcing modell biztonsághoz kapcsolódó alkalmazhatóságára, rávilágítson a crowdsourcing modell biztonsági célú alkalmazásánál megjelenő sajátos szempontokra, és hangsúlyozza a téma további kutatásának fontosságát.

Módszertan: A tanulmány kutatási módszertanának a szerzők a nemzetközi szakirodalmak elemzését választották, a témakör általános szakirodalmi forrásainak vizsgálatát követően áttérve a biztonsági és nemzetbiztonsági irányultságú

A szerzők a kéziratot magyar nyelven nyújtották be. Benyújtás: 2025. 02. 02. Átdolgozás: 2025. 02. 18. Elfogadás: 2025. 02. 20.

alkalmazási példák és szempontok vizsgálatára. A cél nem csupán az esettanulmányok bemutatása volt, hanem a crowdsourcing előnyeinek, hátrányainak és azok kezelésére javasolt megoldásoknak a feltárása.
Megállapítások: A nemzetközi gyakorlati példák és szakirodalmi források alapján jól látható, hogy a crowdsourcing módszerre épülő megoldások fokozatos teret kapnak a biztonsági gondolkodásban. Számos irányban, többek között a kiberbiztonság, a biztonsági eseményekhez kapcsolódó információgyűjtés, vagy akár egyes szakértői képességek és kapacitások becsatornázása terén már most is jelen van mindennapjainkban. Az azonosítható előnyök (humánerőforrás- és költséghatékonyság, gyorsaság) mellett ugyanakkor számos hátrány, illetve korlát [a résztvevők (adat)biztonságát érintő kérdések, vagy akár az adatok hitelessége, manipulálhatósága, szennyezhetősége] és a módszer alkalmazását nehezítő tényező is megjelenik, amelyek még komplexebbé teszik a témakör tudományos célú vizsgálatát.
Érték: A magyar nyelvű, biztonsági kérdésköröket tárgyaló szakirodalomban szűkösek a módszer vizsgálatára irányuló eddigi források. A tanulmánnyal a szerzők a témakör felszínre hozását szeretnék elérni, és a témakörhöz kapcsolódó további tudományos gondolkodást és szakmai diskurzust elősegíteni.

Kulcsszavak: nemzetbiztonság, crowdsourcing, információgyűjtés, kibertér

Abstract

Aim: In the contemporary context of a constantly evolving security environment, the accelerating impact of technological advances and global interconnectivity, innovative solutions that can enhance security by engaging members of society are becoming increasingly valuable. Solutions based on the crowdsourcing model are one such example. These solutions can be effective in specific areas of security-related activities by mobilising diverse groups within society and leveraging community collaboration. The method is not a recent innovation; however, the possibilities of cyberspace have brought to the fore the accessibility of members of society and the related research directions. The advantages of this method include such benefits as speed, cost-effectiveness and the broadening of human resources. However, challenges such as data security, data authenticity and data manipulation must also be considered. The aim of this paper is to draw attention to the security-related applicability of the crowdsourcing model, to highlight the specific aspects of the crowdsourcing model for security purposes, and to emphasise the importance of further research on the topic.
Methodology: For the research methodology of the study, the authors have chosen to analyse the international literature, after examining the general literature

on the subject, moving on to examine security and national security-oriented application examples and aspects. The aim was not only to present case studies, but also to explore the advantages and disadvantages of crowdsourcing and the solutions proposed to address them.
Findings: A review of international examples and literature reveals that crowdsourcing solutions are gradually gaining ground in security thinking. It is already present in our daily lives in a number of areas, including cybersecurity, information gathering related to security incidents, and the channelling of specific expertise and capacities. However, alongside the advantages (human resources, cost-effectiveness, speed) that are clearly identifiable, there are also a number of drawbacks and limitations (the (data) security of the participants, or even the authenticity, manipulability and contamination of the data) and factors that make the application of the method more difficult, which makes the scientific study of the subject even more complex.
Value: In the Hungarian-language literature on security issues, there is a scarcity of resources on the method. With this study, the authors aim to bring the topic to the fore and to promote further scientific reflection and professional discourse on the subject.

Keywords: national security, crowdsourcing, information gathering, cyberspace

Bevezetés

Napjainkban a biztonságunkat érintő környezet jelentős változáson megy keresztül, amelyen belül a technológiai fejlődés, valamint a kibertér biztosította globális összekapcsoltság számos kihívással is szembesíti a társadalmat. Ezek a komplex kihívások gyors és hatékony válaszokat igényelnek a biztonságért felelős szervektől, így azok folyamatosan keresik az új, a biztonság szolgálatába állítható megoldásokat. Felértékelődik az online tér, a technikai környezet nyújtotta innovatív megoldások és eszközök jelentősége, amelyek lehetővé teszik a társadalom civil szereplőinek szélesebb körben történő bevonását a biztonságot érintő tevékenységek támogatásába. Ilyen formálódó lehetőségként tekinthetünk az online térben, a crowdsourcing elvére épülő új megoldásokra, amely során a résztvevők információikkal, szakértelmükkel, résztevékenységek ellátásával járulhatnak hozzá egy közösségi eredmény létrehozásához, és akár proaktív módon segíthetik a biztonság növelését.

A crowdsourcing kifejezés talán sokak számára ismeretlen, azonban modellként történő alkalmazásával szinte minden nap találkozhatunk. Mögöttes értelmezésére,

a crowd, mint tömeg és az outsourcing, mint kiszervezés kifejezések adhatnak némi kiinduló alapot, utalva arra, hogy bizonyos tevékenységeket, részfolyamatokat a humán erőforrások közötti megosztással látnak el, ahol a résztvevők egy-egy részelemmel járulhatnak hozzá a kumulált „közösségi" eredmény létrehozásához. A modell alkalmazása során a tömeg tagjai képességeik és lehetőségeik révén, különböző módokon (például online tér felületei és eszközei) csatornázzák be eredményeiket, információikat, ahol a folyamat végén a közösen létrehozott eredmény tekinthető végterméknek.

A közösség erejének felhasználása rendkívül szerteágazó irányokban figyelhető meg, a szakértői típusú feladatok ellátásától kezdve, akár az egy-egy témakörre koncentráló tevékenységig. Gyakorlati alkalmazásait tekintve szinte minden tudományterületen jelen van, akár a műszaki, akár a társadalomtudományok területein. Módszerként itt említhetőek meg többek között a crowdfundig (közösségi finanszírozás), a crowdsourcing intelligence (közösségi forrásokból történő információgyűjtés), a technikai (Crowd-IoT) jellegű felhasználási irány, a crowdtesting (szoftvertesztelés), a crowdmaping (térkép készítés, illetve frissítés közösségi erőforrások segítségével), vagy akár a módszer jövőbeli eseményekre irányuló prediktív (crowdsourcing forecast) alkalmazhatóságának kutatásai példái is.

A corwdsourcing elvére épülő gyakorlati alkalmazásokra számos történelmi példát láthatunk, főként a gazdasági-üzleti és informatikai élet területeiről. Jelentőségét igazán azonban az online tér mutatta meg, hiszen meghatározott célok érdekében tömegek érhetőek el rövid időn belül. Az egyéni szinteken rendelkezésre álló infokommunikációs eszközök emellett lehetővé tették, hogy a résztvevők ne csak információkat fogadjanak, hanem információikkal, szakértelmükkel, adataikkal, tevékenységükkel részt is vegyenek a munkafolyamatokban. A biztonság témakörére helyezve a hangsúlyt, gondolhatunk egy-egy kritikus biztonsági eseményre (például terrortámadás), ahol az online tér tagjai rövid időn belül a közösségi felületeken teszik közzé információikat, amelyek hozzájárulhatnak a hatóságok munkájának sikeréhez. Az alkalmazási példák sokszínűségét jól jelezheti akár a Google Street View (utcaképek) készítése is, ahol a résztvevők munkájának (elosztott módon történő létrehozása) eredményeként aktuális és egyre pontosabb térképi felületek születhetnek, vagy akár a forgalmat is figyelembe vevő online navigációs megoldások. A crowdsourcing módszer „célirányosítására" létrehozott platformok az információk hasznosulását még hatékonyabbá tehetik, hiszen az eredmény nem az adott egyedi információ (például egy forgalmi dugónál nem az információt közlő személye fontos), hanem már az összesített eredmény szintjén mutatkozhat meg.

Jól látható, hogy az alkalmazás sikere gyakran a módszer adott feladathoz történő célirányos implementálásában rejlik és nem kizárólag egységes sablonok

alkalmazásában. Eltérő célokkal, megjelenési módokkal és platformokkal találkozhatunk például egy, az önkéntesek részvételével zajló biztonsági incidensekhez (például földrengés, árvíz) kapcsolódó adatgyűjtési folyamat, valamint akár egy, a résztvevők szakértelmét felhasználó (például kiberbiztonsághoz kapcsolódó sérülékenységeket jelző) megoldás során. Mindezek a résztvevők eltérő típusú hozzájárulására építenek, amely mellett egy-egy crowdsourcingra épülő projekt időbelisége vagy akár térbelisége (például egy földrajzi térben jól értelmezhető természeti katasztrófa kapcsán a pontosabb információval rendelkező helyi lakossági közösségi felületen megosztott információi) is tovább színezik a kérdéskört.

A módszer előnyeit keresve az outsourcing (kiszervezés) irányába indulhatunk el, és gyakran a humán erőforrás növelésének lehetőségét, a költséghatékonyságot, vagy akár az adott tevékenység gyorsabb végrehajtásának lehetőségét lehet kiemelni. A crowdsourcing esetében mindezeket az online tér és közösségei nyújtotta előnyök még inkább felerősíthetik, hiszen lehetővé teszik, hogy térbeli és időbeli akadályokon túllépve, infokommunikációs eszközeik révén széles tömegek (közösségek) válhassanak egy adott feladat részeseivé. Fontosnak tartjuk ugyanakkor hangsúlyozni, hogy a jól látható előnyök (Schenk & Guittard, 2011) mellett számos korlát és a módszer alkalmazását nehezítő tényező is megjelenik. Gondolhatunk magának a platformnak a kibertámadásokkal szembeni ellenállóképességére, biztonságára, a résztvevők adatainak biztonságára, vagy akár az általuk közölt adatok hitelességére, a vétlen vagy akár szándékos adatszennyezésre, megtévesztő információk közlésére. Mindezek különösen a minél pontosabb és hiteles adatokat igénylő megoldásoknál (például aktuális forgalmat figyelembe vevő navigációs alkalmazások), valamint a biztonsághoz kapcsolódó crowdsourcing alkalmazásoknál válnak kiemelten fontossá és kezelendővé.

Jelen tanulmány, a crowdsourcing általános alkalmazási irányain túllépve, a módszer nemzetközi forrásokban látható biztonsági célú alkalmazási példáin keresztül kívánja felhívni a figyelmet a téma fontosságára. Miközben egyre jelentősebb számú nemzetközi kutatás foglalkozik a témával, a hazai biztonsági, akár nemzetbiztonsági szemléletű szakirodalom rendkívül szűkösnek tekinthető. A tanulmány értelemszerűen csak bepillantást adhat a témakörbe, ugyanakkor illeszkedik egy szélesebb vizsgálati környezetbe is, ahol távlati kutatási célként annak feltérképezése és vizsgálata merül fel, hogy a módszer hogyan és milyen területeken, milyen előnyök és korlátok mellett segítheti a (nemzet) biztonságért felelős szervek munkáját.

Módszertan és szakirodalmi előzmények

A nemzetközi szakirodalmakban jól látható az elméleti módszertan, és azok az alapelemek, amelyek körülölelik a crowdsourcing elméletét. Gondoljunk egyszerűen a résztvevők bevonására, a közös cél/feladat nyílt definiálására, és ehhez kapcsolódóan a „résztvevők" motivációjának, vagy akár adatbiztonságának kérdéseire. Mindezek nélkül a crowdsourcing folyamat el sem indulhat. Kulcselemként definiálható továbbá a feladathoz illesztett megfelelő koordináló, feladatelosztó, adatgyűjtő platformok létrehozása, amelyek ugyanakkor önmaguk is kibertámadások célpontjai lehetnek. Mindezek a crowdsourcing módszer megjelenési irányaihoz igazodva rendkívül sokfélék lehetnek, a mobilkommunikációs eszközöktől kezdve, az önálló internetes weboldalak létrehozásáig. Külön területként értelmezhető a keletkező eredmények gyűjtésének és magának az összesített eredmények elemzésének a módszertana. Ezek mögött további fontos részirányok, így például a nagy tömegű adatok feldolgozhatósága, vagy akár az adatminőség (hitelesség vagy az adatszennyezés) kérdései láthatóak.

A tanulmány kutatási módszertanának a nemzetközi szakirodalmi források feldolgozását választotta, amely egyben jelzi is a nemzetközi színtéren látható alkalmazási megoldások sokszínűségét. A relevánsnak ítélt szakirodalmakból kiindulva, a módszer általános megközelítésétől haladtunk a biztonság általánosabb, majd a nemzetbiztonsági célú vizsgálati irány felé. Ennek megfelelően az általános szakirodalmi áttekintést követően a módszer biztonsági célú kutatásaihoz kapcsolódó források és a nemzetközi színtéren látható példák vizsgálata képezte a tanulmány alapját. Ezek tanulmányba történő beemelése során célunk nem azok részletes ismertetése, hanem a crowdsourcing mint megközelítés sajátos szempontjainak a feltárása volt.

A szakirodalmak a crowdsourcing fogalmát szinte egységesen J. Howe-hoz kötik, aki azt az üzleti-gazdasági folyamatok mentén közelítette meg (Howe, 2006). Alkalmazási irányai azonban napjainkra már jelentősen kitágultak (Brabham, 2013), így a kezdeti fogalom fejlődésére és a felölelt tevékenységek vizsgálatára is összetett szakirodalmi kutatásokat láthatunk (Hossain & Kauranen, 2015). Ezek eredményei jól jelzik az alkalmazási irányok sokszínűségét a menedzsmenttől kezdve az egyre összetettebb technológiai környezetet igénylő okos városok kérdésköréig. Garrigos-Simon és Narangajavana-Kaosiri (2024) közzétett tanulmányukban a témakörben keletkezett minőségi publikációk számának elmúlt évtizedben megfigyelhető jelentős emelkedéséről számoltak be, amely előrevetíti a terület körüli kutatások egymásra épülő további fejlődését, multidiszciplináris jellegét.

Napjainkra a módszer lényegében egy önkéntes részvételen alapuló, főként online felületekhez kötött tevékenységgé formálódott. Elosztott problémamegoldó és termelési modell, amelyben a hálózatba kapcsolt emberek együttműködnek egy feladat elvégzésében (Vukovic et al., 2009), amely használhatóságát a heterogenitás és a források nagy száma adja (Estellés-Arolas & González-Ladrón-de-Guevara, 2012). Mivel napjainkra az internethez kapcsolódó mobilkommunikációs eszközök már rendkívül széles körben rendelkezésre állnak, felértékelődtek a közösségi felületek biztosította lehetőségek, amelyek vizsgálatára számos nemzetközi tanulmány is irányul (Spiliotopoulou et al., 2014). Ezek jelentős része már a modell mögöttes elemeivel, a résztvevő tömeg viselkedésének vizsgálatával, vagy akár az előnyök és hátrányok feltárásával foglalkozik (Shen et al., 2014; Bakici, 2020). Az üzleti világban a crowdsourcing gyakran szolgál innovációs ötletek gyűjtésére, míg a tudományos közösségben is fontos szerepet játszhat problémák megoldásában (Franzoni & Sauermann, 2014). A szakirodalmak között jól látható irányként találkozhatunk az adatvédelem és etikai kérdéskörök vizsgálatával is (Yang et al., 2015; Shmueli et al., 2021; Ren et al., 2022; Feng et al., 2017), így például Xia és McKernan tanulmányukban a crowdsourcing adatvédelmi kihívásait és fenyegetéseit vizsgálva rámutatnak, hogy a crowdsourcing platformok adatvédelmi szempontból számos kockázatot hordozhatnak magukban (Xia & McKernan, 2020).

A crowdsourcing helye és szerepe a biztonsági gondolkodásban

Az elmúlt évtizedben több, a nemzetbiztonsági témakörére fókuszáló nemzetközi tanulmány is született (Gradecki & Curry, 2017; Hui, 2015). Herhkovitz például munkájában rávilágít arra, hogy a crowdsourcing eszköz lehet a nemzetbiztonsági fenyegetések kezelésében is. Részletesen elemzi, hogyan lehet a tömegeket bevonni a nemzetbiztonságot érintő információk gyűjtésébe, amely különösen hasznos lehet a dinamikusan változó biztonsági helyzetekben (Herhkovitz, 2020). Más tanulmányok a módszer előnyeit és kockázatait vizsgálva ismertetik, hogy mindez hogyan segítheti a bűnüldöző szervek munkáját, kitérve annak előnyeire, ugyanakkor kockázataira is. Ide sorolható a már említett közösségi média és más online platformok biztosította környezet vizsgálata, feltárva a tömegek által gyűjtött információk és adatok biztonsági fenyegetések azonosításához és kezeléséhez történő hozzájárulását (Hui, 2015).

Ugyanakkor fejlődő kutatási területként ágaznak el a kiberbiztonság összetett témaköréhez kapcsolódó tanulmányok (Khandpur et al., 2017), többek között a crowdsourcing módszerre épülő bug bounty programok sajátosságainak és

előnyeinek vizsgálata (lásd Sridhar & Ng, 2021). Újabb irányként találkozhatunk a crowdsourcing katasztrófahelyzetekhez és egyéb konfliktusos időszakokhoz kapcsolódó biztonsági célú felhasználhatóságának területével (Xu et al., 2016; Harrison & Johnson, 2019; Havas et al., 2017; Liu, 2014). A nemzetközi fogalmi definiálásokon túllépve, közös elemként látható, hogy a módszer egyik alapvető kritériuma a nyíltság, a megoldandó feladat pontos ismerete és közzététele, valamint a tömeges részvétel és a kollektív problémamegoldás. A szükséges nyíltság ugyanakkor jelzi a crowdsourcing nemzetbiztonsági, vagy védelmi célra történő felhasználhatóságának nehézségeit és összetettségét is.

A crowdsourcing megközelítés nemzetbiztonsági célú lehetséges felhasználása specifikusabb szemléletet kíván, mint a módszer alkalmazhatóságának egyéb területei. Számos, közvetlen biztonsági fókuszú terület azonosítható (Dobák, 2025). Az első ilyen jól azonosítható alkalmazási terület a kiberbiztonság, ahol többek között az egyéni és szervezeti biztonság tudatosságát növelő awareness tevékenység, vagy akár a sérülékenységek és fenyegetések feltárása (Cybersecurity Threat Intelligence – CTI), megosztása során láthatjuk megjelenési példáit. Mindezek ugyanakkor proaktív módon segíthetik a jövőbeli fenyegetésekkel kapcsolatos ismeretek bővülését is. A nemzetközi példák alapján jelen vannak ugyanakkor a támadói oldalról is a szolgálatba állított crowdsourcingra épülő megoldások, ahol a kibertérben megbújó felületek mögött a kibertámadásokhoz csatlakozó elszórt humán és szakmai képességek koncentrálódhatnak.

Nemzetbiztonsági alkalmazási lehetőségként azonosítható a modell alkalmazásával a biztonságot érintő folyamatok és események előrejelzés-szerű vizsgálata, vagy akár a szétszórt humán erőforrásokra épülő előrejelző rendszerek (például radikalizáció) létjogosultsága. A szakirodalmi forrásokban leginkább azonban a különböző biztonsági eseményekhez köthető információgyűjtés és megosztás, a szakértői képességek felhasználása, vagy akár digitális bizonyítékok begyűjtésének példái láthatóak. Gondoljunk az orosz–ukrán háború kibertérben zajló eseményeire, ahol az ukrán fél oldalán találkozhatunk többek között az orosz katonai aktivitások információs jelzését, akár digitális bizonyítékok gyűjtését támogató alkalmazásokkal. A folyamat részeként, a kezdetben a közösségi felületeken még széles körben megjelenő, a nyílt információgyűjtés (Open Source Intelligence – OSINT) számára tömeges forrást jelentő (valós és dezinformációs) információk idővel a zártabb, crowdsourcing modelljét alkalmazó internetes felületek irányába mozdultak el. Az erre a célra létrehozott platformok mögött meghúzódó tömegesen összegyűjtött adatok ugyanakkor felvetették a másik fél számára azok kibertámadási célpontként történő felértékelődését is. Példaként emeljük ki, hogy a lakosság biztonságtudatosságának elvére építve dolgozta ki az ukrán lakosok támogatására az Ukrán Stratégiai Kommunikációs Központ

(Ukrainian Center for Strategic Communication) az ukrán civilek támogatására létrehozott Dovidka.info weblapot is, amely a crowdsourcing több aspektusát is alkalmazza. Egyrészt célja a civilek biztonságtudatosságának növelése, de a tömegeket mint információforrást is felhasználja. Olyan védelmi tanácsokkal látják el a lakosságot, melyek segítenek a megszállás alatt álló területeken elkerülni a civilekkel szembeni erőszak fokozódását, valamint az agresszor kibertevékenységével kapcsolatos védekezési formákat is megosztanak. Emellett a civilek információgyűjtő tevékenységének biztonságos és hatékony támogatását is elősegíti (külön listázzák azokat a chatbotokat, melyeken keresztül biztonságosan lehet az ellenségről adatokat szolgáltatni – https://dovidka.info/). A szolgáltatott eredmények aztán bárki számára elérhetővé tehetőek, melynek a nemzetbiztonsági szervezeteken kívül bárki hasznát veheti, aki kutatni, elemezni és értékelni akarja az adott témát. Ilyen felület a Scribblemap Ukraine (URL1), melyen bárki láthatja a frontvonal aktuális elhelyezkedését.

Sajátosságok és korlátok

A szakirodalmak alapján a biztonság és a nemzetbiztonság szempontjait figyelembe véve a crowdsourcing modell előremutató lehetőségei mellett annak nehézségei és korlátai is kirajzolódnak.

A modell előnyei között láthatók:

- Gyors reakcióidő (a tömeges részvétel és megfelelő platformok esetén gyors információszerzés, értékelés és gyors reagálás lehetősége, akár azonnali válaszadás).
- Az eredmények pontosságának növekedése (a nagyobb mennyiségű és több forrásból származó adat növelheti az összesített eredmény pontosságát).
- Erőforrások hatékony felhasználása [humán és egyéb erőforrások (költség) hatékony felhasználása].
- Széles körű részvétel (az egyének szintjén rendelkezésre álló szakértelem, nézőpontok és innováció pozitívumainak becsatornázása).
- A társadalom és a hatóságok közötti bizalom erősítése (a társadalom önkéntes bevonása a közös érdekeken alapuló, a közösség biztonságát szolgáló folyamatokba).
- Feladatspecifikus megoldások kialakíthatósága (adott biztonsági feladathoz térben és időben igazodó, célzott megoldások kialakíthatósága).
- Az eredményként megjelenő közösségi tudás felhasználása (végeredményként – széles körű részvétel esetén – az egyének szintjén megjelenő információ, tudás, szakértelem, tapasztalat együttes eredményének megjelenése).

A modell korlátai között láthatók:

- Adatvédelem (a résztvevők adatainak védelme, anonimitásuk biztosítása a folyamat során, adatszivárgás elkerülése).
- Téves, pontatlan, valamint megtévesztő adatok megjelenése [vétlen vagy szándékos (például megtévesztés, adatszennyezés) okra visszavezethető téves adatok megjelenése, amelyek akár téves eredményekhez és döntésekhez vezethetnek].
- Az alkalmazás hitelessége, a megoldásba vetett bizalom fenntartása (a tömeges részvétel elérése érdekében a résztvevők adatainak, közreműködésének, hozzájárulásának védelme, amely sérülése bizalomvesztéshez vezethet).
- A gyűjtött és tömegesen rendelkezésre álló adatok sérülékenysége (más szereplők, például üzleti szereplők, ellenérdekelt entitások, hackerek irányából az adathalmazok iránti érdeklődés egyéb felhasználás érdekében).
- Résztvevők alacsony száma (a részvételi motiváció alacsony szintje, amely miatt az alkalmazás kiüresedhet, téves eredmények születhetnek; az önkéntesség mellett akár egyéb motiváló eszközök beépítésének szükségessége).
- A tömegesen megjelenő adatok minőségének meghatározása, szakértése, feldolgozása (a részvétel koncentrálása az adott feladatban releváns információt, szakértelmet biztosító résztvevői kör irányába, ellenkező esetben a gyűjtött adatok minősége sérül, illetve értéktelen lesz).
- Sérülékeny infrastruktúra (platformok biztonsága, amelyek az adatok megszerzése, manipulálása szándékával például kibertámadások célpontjaivá válhatnak).

A bizalmasság kérdése kapcsán a nemzetközi színtérre kitekintve általánosságban megfogalmazható, hogy a nemzetbiztonsági területen az információs igények alapvetően szenzitív jellegűek. Bizonyos esetekben azonban a társadalom széles körének nyílt támogatását élvező biztonsági eseményekhez kapcsolódva a nyíltan megfogalmazható információs igények is teret nyerhetnek crowdsourcingra épülő felületeken. A külső tömeges források bevonásával járó tevékenységeknél azonban számolni kell az ellenérdekű felek dezinformációs szándékával, adatmanipulálásával, vagyis az adatgyűjtés megbízhatósága és így a felhasználhatóság nagy mértékben függ a források megbízhatóságától. Ennek egyik eleme az adatszolgáltatók száma. Széles adatforrási kör esetén statisztikai szempontból elhanyagolható lesz a szolgáltatott adatot nyújtók adatmanipulációs tevékenysége a számosság elve alapján (Estellés-Arolas & González-Ladrón-de-Guevara, 2012). De amint szűkítjük az adatszolgáltatók körét, úgy nő az adatok pontatlansága, megbízhatósága.

A célirányosan, szakértőként bevont, kis számú forrás esetében már egyértelmű, hogy csak az adatszolgáltató személy, vagy kisebb csoport motivációján múlik, hogy milyen mértékben szolgáltat valós adatot az együttműködés során. A megbízhatóság másik eleme maga a gyűjtött adat, amely típusa jelentős különbséget mutathat a megbízhatóság szempontjából. Az okoseszközökről vagy az azokkal előállított objektumokról (képek, leiratok, posztok stb.) gyűjtött metaadatok manipulált mivoltának jóval kisebb a valószínűsége, mint az adatszolgáltató által szándékosan közétett tartalmaknál (Acker, 2018), valamint a metaadat önmagában is alkalmas lehet a manipulált és hamisított tartalmak kiszűrésére (Wittau & Seifert, 2024).

Az önkéntes adatszolgáltatás másik kérdése a személyes és egyéb érzékeny adatok védelme. Tömeges adatgyűjtésnél vagy adatszolgáltatásnál előfordulhat, hogy olyan információk is megjelennek, melyek valamilyen személyes adatot tartalmaznak. A személyes adatokon túl olyan adatok, audiovizuális információk is felmerülhetnek, melyek sérthetik akár az adatszolgáltatót, akár azt, akire az információ vonatkozik. A vallási, a faji, vagy akár a szexuális identitáshoz tartozó adatok is kiemelten érzékenyek. Előfordulhatnak olyan jellegű kérdések is az adatgyűjtés során, melyek alkalmasak lehetnek az adatszolgáltató beazonosítására. Annak érdekében, hogy a crowdsourcing hosszú távon hatékony eszköz lehessen, garantálni kell a résztvevők anonimitását és azt, hogy a közétett információk nem sértenek senkit és nem ütköznek jogszabályba. Az adatvédelem ezen aspektusa többrétű és egy online közösségnél egyrészt védheti a forrást, másrészt nem ad teret az olyan jellegű tevékenységeknek, mint például az „internetes trollkodás". (A trollkodás alatt azt a tevékenységet értjük, mely során a közösség egy tagja manipulatív vagy provokatív céllal, vélt vagy valós ellenvéleményt fogalmaz meg egy téma kapcsán. Ez a tevékenység lehet egy gyerekes személyiség szórakozása, de akár egy ellenérdekű fél hibrid eszköztárának egyik eleme is (Latvian Institute of International Affairs & Riga Stradins University, 2016), ami hátrányosan befolyásolhatja az érintett közösség véleményét is. A közösség „hivatásos trollokon" keresztül történő befolyásolása már az információs hadviselés egyik eleme, melynek célja lehet akár politikai, akár társadalmi destabilizálás okozása (McCuen, 2008).

A védelmi célú alkalmazásoknál – így az előzőekben leírtak miatt – főként a katasztrófahelyzetek kezelése során, vagy akár a terrorizmus elleni harc és biztonságot érintő egyéb események kapcsán találkozunk a megoldással, mivel ezeken a területeken jól azonosíthatóak a társadalom tagjainak közreműködését igénylő nyílt biztonsági célok és érdekek, így egységesebb képet mutat a társadalom motivációja is (Lamprou & Antonopoulos, 2021). A terrorizmus elleni harchoz kapcsolódó jól ismert – a crowdsourcing módszer előnyeire és

hátrányaira is rávilágító – széles körben ismert példa a Boston Marathon (2013) alatt elkövetett robbantás, amely után a Reddit internetes közössége nyújtott segítséget a hatóságok felderítő munkájához (Nhan et al., 2017). Az üzemeltetők és a segítséget kérő rendvédelmi szervezetek moderálásának hiányában a közösség azonban túlterjeszkedett és aktívan belefolyt az elkövetők felkutatásába. További érdekes irányként látható, hogy a szervezett bűnözés elleni harcban is hasznos információforrásként működhetnek a lakóközösségek, akik az információmegosztással jelentős mértékben tudják korlátozni a lakóhelyükön tevékenykedő „csoportok" aktivitását (Estellés-Arolas, 2022), ezzel is segítve a rendészeti és nemzetbiztonsági szervek munkáját.

Összefoglalás

A civil társadalom és a gazdasági élet egyre több szegmensét szövik át a crowdsourcingre épülő megoldások, profitot termelve a módszerben rejlő lehetőségek felhasználásával. Ennek okai között látható, hogy az üzleti szereplők költséghatékonyságot szolgáló gondolkodása jól hasznosítja a tömegek által szolgáltatott adatokat, legyen szó termékfejlesztésről, trendek vizsgálatáról, vagy egy mélytanuló hálózat betanításáról.

Ugyanakkor a biztonsági ágazat zártabb gondolkodása ellenére a nemzetközi színtéren látható esetek azt mutatják, hogy a modell alkalmazása teret nyert a biztonsági szférában is. A tanulmányban felvetett néhány, már most is látható alkalmazási irány (többek között a kiberbiztonság, a döntéshozatal információkkal történő támogatása, sajátos szakértői ismeretek becsatornázása) jelzi a tágabban értelmezett nemzetbiztonságot szolgáló innovatív megoldások fejlődésének irányait.

A módszer előnyei mellett jól láthatóak azok a gyakorlati alkalmazási példák is, amelyek a módszer biztonsági célú alkalmazhatóságának korlátaira és sajátos szempontjaira is rávilágítanak. Amellett, hogy segítheti a gyors és hatékony információszerzést és adatfeldolgozást, kihívások jelennek meg a résztvevők biztonsága, motiválása, a pontos és hiteles információk kiszűrése, vagy akár a nagy számú résztvevő információinak kezelése terén.

A szakirodalmakban megjelenő példák többségében a társadalom irányába széles körben megfogalmazható és általuk támogatott biztonsági tevékenységekhez köthető felhasználási irányokat mutatnak. Ennek okai a részvételi hajlandóságra vezethetőek vissza, hiszen motivált, önkéntes egyéni részvétel nélkül elmaradhatnak a résztvevők, akik nélkül a crowdsourcing módszer alkalmazása kiüresedik.

Információs társadalmunkban és a mesterséges intelligencia térhódításának világában a biztonsági ágazat azonban nem mondhat le azokról az előnyökről, amelyek a társadalom tagjainak bevonásával gyorsabb és hatékonyabb megoldásokat eredményezhetnek a biztonságot érintő összetett fenyegetések valamely területén. Amellett, hogy növekedhet a szervezetek munkájának hatékonysága, a civil szereplők bevonása révén a biztonsági intézkedések szélesebb társadalmi támogatottságot nyerhetnek, ami tovább erősíti a közösségek ellenálló képességét a biztonsági kihívásokkal szemben.

Felhasznált irodalom

Acker, A. (2018). *Data craft: The manipulation of social media metadata*. Data & Society Research Institute. https://datasociety.net/wp-content/uploads/2018/11/DS_Data_Craft_Manipulation_of_Social_Media_Metadata.pdf

Bakici, T. (2020). Comparison of crowdsourcing platforms from social-psychological and motivational perspectives. *International Journal of Information Management, 52*, 102097. https://doi.org/10.1016/j.ijinfomgt.2020.102121

Brabham, D. C. (2013). Crowdsourcing: A model for leveraging online communities. In A. Delwiche & J. J. Henderson (Eds.), *The participatory cultures handbook* (pp. 120–129). Routledge.

Dobák, I. (2025). Crowdsourcing for security in the age of hybrid threats. *Security and Defence Quarterly.* https://doi.org/10.35467/sdq/197309

Estellés-Arolas, E. (2022). Using crowdsourcing for a safer society: When the crowd rules. *European Journal of Criminology, 19*(4), 692–711. https://doi.org/10.1177/1477370820916439

Estellés-Arolas, E. & González-Ladrón-de-Guevara, F. (2012). Towards an integrated crowdsourcing definition. *Journal of Information Science, 38*(2), 189–200. https://doi.org/10.1177/0165551512437638

Feng, W., Yan, Z., Zhang, H., & Zeng, K. (2017). A survey on security, privacy, and trust in mobile crowdsourcing. *IEEE Internet of Things Journal.* https://ieeexplore.ieee.org/document/8080202

Franzoni, C. & Sauermann, H. (2014). Crowd science: The organization of scientific research in open collaborative projects. *Research Policy, 43*(1), 1–20. https://doi.org/10.1016/j.respol.2013.07.005

Garrigos-Simon, F. J. & Narangajavana-Kaosiri, Y. (2024). Crowdsourcing: A systematic literature review and future research agenda. *European Journal of Studies in Management and Business, 30*(1), 1–26. https://doi.org/10.32038/mbrq.2024.30.01

Gradecki, J. & Curry, D. (2017). Crowd-sourced intelligence agency: Prototyping counterveillance. *Big Data & Society, 4*(1), 1–13. https://doi.org/10.1177/2053951717693259

Harrison, S. & Johnson, P. (2019). Challenges in the adoption of crisis crowdsourcing and social media in Canadian emergency management. *Government Information Quarterly, 36*(3), 501–509. https://doi.org/10.1016/j.giq.2018.09.009

Havas, C., Resch, B., Francalanci, C., Pernici, B., & Scalia, G. (2017). E2mc: Improving emergency management service practice through social media and crowdsourcing analysis in near real time. *Sensors, 17*(12), 2766. https://doi.org/10.3390/s17122766

Herhkovitz, S. (2020). Crowdsourced intelligence (Crosint): Using crowds for national security. *The International Journal of Intelligence, Security, and Public Affairs, 22*(1), 42–55. https://doi.org/10.1080/23800992.2020.1744824

Hossain, M. & Kauranen, I. (2015). Crowdsourcing: A comprehensive literature review. *Strategic Outsourcing: An International Journal, 8*(1), 2–22. https://doi.org/10.1108/SO-12-2014-0029

Howe, J. (2006, June 1). The rise of crowdsourcing. *Wired.* https://www.wired.com/2006/06/crowds/

Hui, J. Y. (2015). *Crowdsourcing for national security.* S. Rajaratnam School of International Studies. http://www.jstor.org/stable/resrep05853

Khandpur, R. P., Ji, T., Jan, S., Wang, G., & Lu, C. T. (2017). Crowdsourcing cybersecurity: Cyber attack detection using social media. In *Proceedings of the 2017 ACM on Web Science Conference* (pp. 263–272). https://doi.org/10.1145/3132847.3132866

Lamprou, E. & Antonopoulos, N. (2021). Crowdsourcing as a tool against misinformation: The role of social media and user-generated content in overturning misinformation during the Greek Covid-19 pandemic. In *Adapt to Survive: The Role of Social Media, Sharing and Communication to Ameliorate This World* (pp. 13–23). Communication Institute of Greece. https://coming.gr/wp-content/uploads/2021/12/1_1_2021_Adapt-to-survive_Book_conf-proceedings_COMinG.pdf

Latvian Institute of International Affairs, & Riga Stradins University. (2016). *Internet trolling as a hybrid warfare tool: The case of Latvia*. NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/publications/internet-trolling-as-a-hybrid-warfare-tool-the-case-of-latvia/160

Liu, S. B. (2014). Crisis crowdsourcing framework: Designing strategic configurations of crowdsourcing for the emergency management domain. *Computer Supported Cooperative Work (CSCW), 23*(4–6), 389–443. https://doi.org/10.1007/s10606-014-9204-3

McCuen, J. J. (2008). Hybrid wars. *Military Review, 88*(2), 107–113.

Nhan, J., Huey, L., & Broll, R. (2017). Digilantism: An analysis of crowdsourcing and the Boston Marathon bombings. *British Journal of Criminology, 57*(2), 341–361. https://doi.org/10.1093/bjc/azv118

Ren, Y., Liu, W., Liu, A., Wang, T., & Li, A. (2022). A privacy-protected intelligent crowdsourcing application of IoT based on the reinforcement learning. *Future Generation Computer Systems, 125*, 1–12. https://doi.org/10.1016/j.future.2021.03.011

Schenk, E. & Guittard, C. (2011). Towards a characterization of crowdsourcing practices. *Journal of Innovation Economics & Management, 7*(1), 93–107. https://doi.org/10.3917/jie.007.0093

Shen, X. L., Lee, M. K. O., & Cheung, C. M. K. (2014). Exploring online social behavior in crowdsourcing communities: A relationship management perspective. *Computers in Human Behavior, 40*, 144–151. https://doi.org/10.1016/j.chb.2014.07.048

Shmueli, B., Fell, J., Ray, S., & Ku, L. W. (2021). Beyond fair pay: Ethical implications of NLP crowdsourcing. *arXiv preprint* arXiv:2104.10097. https://doi.org/10.18653/v1/2021.naacl-main.295

Spiliotopoulou, L., Charalabidis, Y., & Loukis, E. N. (2014). A framework for advanced social media exploitation in government for crowdsourcing. *Transforming Government: People, Process and Policy, 8*(4), 545–568. https://doi.org/10.1108/TG-01-2014-0002

Sridhar, K. & Ng, M. (2021). Hacking for good: Leveraging HackerOne data to develop an economic model of bug bounties. *Journal of Cybersecurity, 7*(1), tyab007. https://doi.org/10.1093/cybsec/tyab007

Vukovic, M., Lopez, M., & Laredo, J. (2009, November). PeopleCloud for the globally integrated enterprise. In *Service-Oriented Computing. ICSOC/ServiceWave 2009 Workshops* (pp. 109–114). Springer. https://doi.org/10.1007/978-3-642-16132-2_10

Wittau, J. & Seifert, R. (2024). Metadata analysis of retracted fake papers in Naunyn-Schmiedeberg's Archives of Pharmacology. *Naunyn-Schmiedeberg's Archives of Pharmacology, 397*(6), 3995–4011. https://doi.org/10.1007/s00210-023-02850-6

Xia, H. & McKernan, B. (2020). Privacy in crowdsourcing: A review of the threats and challenges. *Computer Supported Cooperative Work (CSCW), 29*, 263–301. https://doi.org/10.1007/s10606-020-09374-0

Xu, Z., Liu, Y., Yen, N. Y., Mei, L., & Luo, X. (2016). Crowdsourcing based description of urban emergency events using social media big data. *IEEE Transactions on Big Data, 2*(3), 324–335. https://ieeexplore.ieee.org/document/7381652

Yang, K., Zhang, K., Ren, J., & Shen, X. (2015). Security and privacy in mobile crowdsourcing networks: Challenges and opportunities. *IEEE Communications Magazine, 53*(8), 75–81. https://doi.org/10.1109/MCOM.2015.7180511

A cikkben szereplő online hivatkozás

URL1: *Ukraine War Map.* https://www.scribblemaps.com/maps/view/Ukraine-War-Map/uwa

A cikk APA szabály szerinti hivatkozása

Dobák I. & Bérczi P. (2025). Crowdsourcing – lehetőségek és korlátok nemzetbiztonsági szemmel. *Belügyi Szemle*, *73*(3), 593–608. https://doi.org/10.38146/BSZ-AJIA.2025.v73.i3.pp593-608

Nyilatkozatok

Összeférhetetlenség

A szerzők nem jelentettek összeférhetetlenséget.

Finanszírozás

A szerzők nem kaptak pénzügyi támogatást a kutatáshoz, a szerzőséghez és/vagy a cikk publikálásához.

Etikai nyilatkozat

Jelen cikkhez nem kapcsolódik adatkészlet.

Levelező szerző

A cikk levelező szerzője Dobák Imre, aki a dobak.imre@uni-nke.hu e-mail címen érhető el.