Magyar Rendészet 2026/3. 269–275.
DOI: 10.32577/mr.2026.3.17

RECENZIÓ

Recenzió Orbók Ákos *Az okos város kiberbiztonsága*[1] című tanulmányáról

Review of Ákos Orbók's Study Titled „Cybersecurity in the Smart City"

HARANGOZÓ Valentin[2]

Bevezetés: Az okosvárosok fejlődése, valamint az információs és kommunikációs technológiák integrációja alapvetően alakítja át a modern városi környezet működését. A digitalizáció következtében létrejövő kiberfizikai rendszerek ugyanakkor új típusú biztonsági kihívásokat teremtenek, amelyek a rendészettudomány, a közlekedésbiztonság és a kiberbiztonság területén egyaránt jelentkeznek. E folyamatok vizsgálata különösen aktuális az elektromobilitási járművek gyors terjedése miatt.

Cél: A recenzió célja Orbók Ákos *Az okos város kiberbiztonsága* című tanulmányának átfogó, kritikai elemzése, fókuszálva az urbanizációs és digitalizációs folyamatok rendészettudományi és közlekedésbiztonsági kihívásaira. A tanulmány célja továbbá, hogy a recenzált mű elméleti megállapításait a szerző az elektromobilitási eszközök kiberbiztonságát vizsgáló empirikus kutatások eredményeivel, valamint a legújabb nemzetközi és hazai szakirodalommal szintetizálja.

Módszertan: A munka a leíró és elemző szakirodalom-feldolgozás módszertanára épül. Az elméleti állítások validálása és kontextualizálása érdekében a recenzió beépíti a szerző korábbi, a technológiaelfogadási hajlandóságot és az e-rollerek *firmware* sérülékenységét vizsgáló kutatásainak adatait, kiegészítve azt a nemzetközi kiberbiztonsági és a hazai „okosrendőrség" paradigmák tapasztalataival.

Megállapítások: Orbók tanulmánya kiváló elméleti alapot nyújt az okosvárosok sérülékenységének megéréséhez, rámutatva, hogy a kiberfizikai rendszerekben az IT-biztonság hiányosságai azonnali fizikai kockázatot generálnak. Ezt

[1] Orbók Ákos (2018): Az okos város kiberbiztonsága. In Sallai Gyula (szerk.): *Az okos város (Smart City).* Budapest: Dialóg Campus, 187–201. Online: https://real.mtak.hu/88490/1/Web_PDF_Smart_City.pdf

[2] R. főhadnagy, főelőadó, információbiztonsági felelős, Somogy Vármegyei Rendőr-főkapitányság Rendészeti Igazgatóság Közlekedésrendészeti Osztály; doktori hallgató, Nemzeti Közszolgálati Egyetem Rendészettudományi Doktori Iskola, e-mail: harangozovalentin1986@gmail.com

az elméleti keretet a gyakorlati mikromobilitási tesztek és a nemzetközi szakirodalom maradéktalanul igazolják, ugyanis a költséghatékony, de alacsony biztonsági szintű IoT-eszközök könnyedén manipulálhatók, ami új típusú közlekedésrendészeti és kiberbiztonsági fenyegetéseket teremt.

Érték: A recenzió hozzájárul a rendészettudományi diskurzushoz azáltal, hogy hidat képez az okosvárosok elméleti kiberbiztonsági koncepciói és a mindennapi közlekedésrendészeti gyakorlat között, rávilágítva a felhasználói biztonságtudatosság elengedhetetlen szerepére az elektromobilitás korában.

Kulcsszavak: könyvismertetés, okosváros, kiberbiztonság, elektromobilitás, közlekedésrendészet

Introduction: The development of smart cities and the integration of information and communication technologies are fundamentally transforming the functioning of the modern urban environment. At the same time, the cyber-physical systems emerging as a result of digitaliSation are creating new types of security challenges that arise in the fields of law enforcement, transportation safety, and cybersecurity. Examining these processes is particularly relevant given the rapid proliferation of electric vehicles.

Objective: The objective of this review is to provide a comprehensive, critical analysis of Ákos Orbók's study titled "Cybersecurity in the Smart City", focusing on the challenges posed by urbanisation and digitalisation processes in the fields of criminology and traffic safety. The study also aims to synthesise the theoretical findings of the reviewed work with the results of empirical research examining the cybersecurity of electric mobility devices, as well as with the latest international and domestic literature.

Methodology: The work is based on a methodology of descriptive and analytical literature review. To validate and contextualise the theoretical claims, the review incorporates data from the author's previous research examining technology acceptance and firmware vulnerabilities in e-scooters, supplementing it with insights from international cybersecurity paradigms and the domestic "smart policing" paradigm.

Findings: Orbók's study provides an excellent theoretical foundation for understanding the vulnerabilities of smart cities, highlighting that IT security gaps in cyber-physical systems generate immediate physical risks. This theoretical framework is fully corroborated by practical micromobility tests and the international literature, as cost-effective but low-security IoT devices can be easily manipulated, creating new types of traffic safety and cybersecurity threats.

Value: This review contributes to the discourse in the field of law enforcement by bridging the gap between theoretical cybersecurity concepts for smart cities and everyday traffic enforcement practices, highlighting the indispensable role of user security awareness in the age of electromobility.

Keywords: book review, smart city, cybersecurity, electromobility, traffic policing

A mű témája, célja és aktualitása

A 21. század urbanizációs folyamatainak egyik legmeghatározóbb paradigmaváltása az okosvárosok *(smart city)* koncepciójának megjelenése és fizikai valósággá válása. Ahogy a fizikai életterünk egyre szorosabban összefonódik a kibertérrel, úgy a hagyományos rendészeti, biztonsági és szabályozási mechanizmusok is korábban nem látott kihívásokkal szembesülnek. Ezt a komplex, technológiai és társadalmi metszéspontot vizsgálja Orbók Ákos *Az okos város kiberbiztonsága* című hiánypótló tanulmánya.

A mű célja, hogy feltérképezze azokat a kiberbiztonsági kihívásokat, amelyek az okosvárosok működését alapjaiban határozzák meg, kiindulva abból az alapvetésből, hogy minden olyan feladat, amelyet a dolgok internete (*internet of things,* IoT) vagy a mesterséges intelligencia hajt végre, immár a kibertérben zajlik. Az aktualitás vitathatatlan, hiszen a szenzorok, okosmérők, intelligens közlekedésirányítási rendszerek és az elektromobilitási eszközök expanziója olyan hálózati ökoszisztémát hozott létre, ahol a digitális sebezhetőségek azonnali, a fizikai térben manifesztálódó károkat képesek okozni. Orbók tanulmánya arra vállalkozik, hogy a kiberbiztonság alapfogalmainak tisztázásától eljusson a konkrét, okosvárosi kulcsterületeket érintő fenyegetések rendszerezéséig, különös tekintettel az infokommunikációs infrastruktúrára, az energetikára, valamint a közlekedésre.

A mű felépítése és fogalmi keretei

Orbók írása logikus és átgondoltan felépített struktúrát követ, a fogalmi alapozástól halad a specifikus kockázatelemzés felé. A szerző rögtön a bevezető részben tisztázza a kibertér fogalmát, visszanyúlva William Gibson *Burning Chrome* című novellájához, majd kiterjeszti azt minden olyan eszközre, amely elektromágneses hullámokat használ kommunikációra vagy adatforgalomra.

Ezt követően a rendészettudomány és a mérnöki tudományok határterületén gyakran összemosódó fogalmak egy rendkívül fontos differenciálását végzi el, ugyanis elválasztja a safety (biztonság mint veszélytelenség, üzembiztonság) és a security (biztonság mint védettség, sértetlenség) fogalmát. Ez a megkülönböztetés közlekedésrendészeti szempontból is kardinális. Egy jármű esetében a fékrendszer mechanikai megbízhatósága (safety) hagyományos mérnöki kérdés, azonban ha ezt a fékrendszert egy elektronikus vezérlőegységen (ECU) keresztül külső, illetéktelen beavatkozás éri (security), az azonnal safety kockázattá, azaz közvetlen balesetveszéllyé alakul.

A tanulmány rámutat arra a sajnálatos piaci anomáliára, hogy a gyártók elsősorban az üzembiztonságra *(safety)* fókuszálnak, miközben például a kiberbiztonságot másodlagosként kezelik. Orbók rávilágít ennek gazdasági mozgatórugójára: egy meghibásodás garanciális időn belül közvetlenül a gyártót károsítja meg, így az üzemeltetés biztonsága prioritást élvez a tervezéskor. A szerző hangsúlyozza továbbá, hogy a biztonság szubjektív állapot; nincs teljes biztonság, csupán tudatos kockázatvállalás létezik. A biztonsági intézkedéseket ráadásul észszerű határokon belül kell tartani, hiszen egy bizonyos ponton túl már a használhatóság rovására mennek, és teljesen kontraproduktívvá válhatnak.

Az elméleti keretalkotás során a mű definiálja az IT-biztonság alapkövetelményeit is, úgymint az adatok és rendszerelemek bizalmasságát, sértetlenségét és rendelkezésre állását. Ezt a hármast szokták az angol kezdőbetűik alapján CIA-elvnek nevezni (Muha–Krasznay 2014). A kiberbiztonság megteremtése a szerző szerint összehangolt folyamat, amelynek elengedhetetlen elemei:

- az információ, a hálózati és az alkalmazásbiztonság garantálása;
- a működési biztonság és a folyamatos üzem biztosítása (vészhelyreállítás);
- a végfelhasználók biztonsági oktatása és tudatosítása.

Ez a komplex és többrétegű megközelítés az IoT-eszközök esetében hatványozottan fontos. Orbók kiemeli, hogy az IoT-eszközök vonatkozásában ma már nem az egyes eszközök biztonságával kell foglalkozni, hanem a hálózatba kapcsolt eszközök rendszerét külön entitásként kell vizsgálni. Ebben a kiterjedt ökoszisztémában így fontos alapvetés, hogy a teljes infrastruktúra biztonsága egyenlő a mindenkori leggyengébb láncszem biztonsági szintjével.

Aszimmetrikus fenyegetések és a kibertér

A szerző a kiberbiztonsági kihívásokat a motivációk és az elkövetői kör alapján négy fő kategóriába sorolja: kiberbűnözés, kiberhadviselés, kiberterrorizmus és hacktivizmus. Orbók rámutat, hogy a kiberbűnözés szinte kizárólagos motivációja a pénzszerzés, amely azért rendkívül vonzó az elkövetők számára, mert a virtuális jelenlét miatt csekély a fizikai lebukás veszélye, a célpontok pedig alig védekeznek. Bár a rendészet számára a kiberbűnözés és a nehezen kiszámítható hacktivizmus (például az Anonymous mozgalom) jelent mindennapos kihívást, a tanulmány a kiberhadviselést is kiemeli mint a hadviselés új, ötödik színterét. Ezen a téren a legnagyobb veszély az anonimitás: aránylag kis befektetéssel lehet hatalmas infrastrukturális károkat okozni anélkül, hogy a támadó kiléte egyértelműen bizonyítható lenne.

Rendkívül fontos a szerző megállapítása a *social engineering* (pszichológiai manipuláció) kapcsán, miszerint az információs rendszer leggyengébb eleme maga az ember. Ez a módszer nem logikai úton támad, hanem befolyásolással, megtévesztéssel veszi rá a felhasználót, hogy akár egy teljesen zárt rendszerbe is bejuttassa a kártékony kódot. A tanulmány a hírhedt iráni urándúsítók elleni Stuxnet-támadást hozza fel példaként, ahol az internettől fizikailag elzárt rendszert is képesek voltak kompromittálni.

Az okosvárosokban a humán faktor sebezhetősége drámai méreteket ölthet, hiszen a felhasználók gyakran úgy használnak komplex kiberfizikai rendszereket (például megosztott rollerek, okosotthon-vezérlők), hogy a háttérben zajló adatcsere biztonsági kockázataival egyáltalán nincsenek tisztában. Az emberek többsége kifejezetten az okoseszközök által nyújtott változatos és kényelmi szolgáltatások miatt választja ezeket a technológiákat, miközben a fenyegetéseket nem értik, és a kényelem oltárán a biztonsági intézkedéseket hajlamosak elhanyagolni.

Okosmobilitás és kiberbiztonsági reflexiók

A tanulmány legfontosabb része az okosváros kulcsterületeinek kiberbiztonsági elemzése, különös tekintettel a közlekedésre. Orbók helytállóan rögzíti, hogy az autonóm és intelligens járművek elterjedésével az internet vagy más hálózati technológia használata elengedhetetlenné válik, ezáltal a járművek fokozottan ki lesznek téve a kibertér rosszindulatú felhasználóinak.

Ezt az elméleti keretrendszert a nemzetközi szakirodalom, valamint a mikromobilitási eszközök kiberbiztonságát vizsgáló empirikus kutatások is alátámasztják és gyakorlati kontextusba helyezik. A Texasi Egyetem (UTSA) kutatói átfogó tanulmányukban rávilágítottak arra, hogy a mikromobilitási ökoszisztéma sebezhetőségei nemcsak az adatvédelmet, hanem a felhasználók fizikai épségét is veszélyeztetik. A kutatás rámutatott, hogy a Bluetooth Low Energy (BLE) protokoll sérülékenységein, illetve a GPS-adatok manipulálásán *(spoofing)* keresztül a támadók akár távolról is átvehetik az irányítást a járművek felett (Vinayaga-Sureshkanth et al. 2020). Hasonló megállapításra jutott az NCC Group is, ugyanis vizsgálataik során bizonyították, hogy az elavult alkalmazásbiztonság és a titkosítás hiánya miatt a támadók akár mozgás közben is blokkolhatják a fékrendszert, vagy szoftveresen megnövelhetik a jármű sebességét (NCC Group 2022).

Orbók Ákos elméleti aggodalmait – miszerint az IoT-eszközök logikai sebezhetőségei közvetlen fizikai *(safety)* kockázatot jelentenek – a mikromobilitási eszközökön végzett empirikus vizsgálatok is validálják. Egy széles körben elterjedt elektromos roller biztonsági tesztelése során bebizonyosodott, hogy a jármű Bluetooth modulján keresztül a vezérlőrendszer harmadik féltől származó alkalmazásokkal pillanatok alatt manipulálható, aminek következtében a gyári biztonsági korlátozások megkerülhetővé és felülírhatóvá válnak (Harangozó 2025). Ez a gyakorlati példa tökéletesen alátámasztja Orbók azon felvetését, hogy az ilyen típusú kibertámadások és manipulációk az elektromobilitás területén azonnali és kiemelten súlyos közlekedésbiztonsági veszélyeket idéznek elő.

Továbbá Orbók megjegyzi, hogy az okosváros polgárainak aktív és tudatos részvételére van szükség a rendszer fenntarthatóságához. A szerző a felhasználói magatartás vizsgálatakor három fő területet emel ki: a biztonságtudatosságot, a racionális energiafelhasználást, valamint a társadalmi részvételt. Úgy véli, az okosváros működésének alapfeltétele, hogy a polgárok részt vegyenek a döntéshozatalban és a fejlesztési irányok kijelölésében, ehhez azonban megfelelő informáltságra van szükségük, hogy tisztában lehessenek döntéseik következményeivel. Emellett a korlátozott erőforrások miatt a fenntartható jövőt végső soron a felhasználók racionális döntései fogják biztosítani. A legkritikusabb pont azonban a biztonságtudatosság, ezért hangsúlyozza, hogy a logikai védelem nem helyettesítheti az embert, aki a rendszer leggyengébb láncszeme marad, így a jövőben is a felhasználó tehet a legtöbbet a saját és környezete biztonságáért.

Pozitívumok, kritikai megjegyzések és rendészeti aspektusok

Orbók Ákos tanulmánya egyértelműen hiánypótló, hiába a megjelenése évekre visszanyúló, a megállapításai továbbra is aktuálisak. A tanulmány fő erőssége a logikai felépítés,

a precíz fogalomhasználat és a rendszerszintű látásmód. A tanulmány nemcsak analizál, hanem fontos figyelmeztetést is megfogalmaz. Egyértelművé teszi, hogy az okostechnológiák implementációja nem tekinthető pusztán egyszerű informatikai beszerzésnek, hanem határozottan kritikusinfrastruktúra-fejlesztésként kell kezelni. Ezzel az átfogó megközelítéssel a tanulmány stabil, tudományos iránytűként szolgál a terület jövőbeli kutatói és a szakemberek számára egyaránt.

Kritikai megjegyzésként megfogalmazható, hogy a tanulmány elsősorban elméleti megközelítést alkalmaz, és viszonylag kevés empirikus példát vagy esettanulmányt tartalmaz. Bár érthető, hogy egy alapozó könyvfejezet nem mehet bele mély technikai részletekbe, a tanulmány értékét jelentősen növelhette volna néhány konkrét, műszaki-empirikus esettanulmány. Ugyanakkor épp ez az elméleti alapozás ad lehetőséget arra, hogy a későbbi kutatók – a gyakorlati megvalósítás során – az ő elméleti keretrendszerét empirikus adatokkal töltsék meg.

A rendészet számára az okosváros nemcsak fenyegetést, hanem óriási lehetőséget is jelent. Berki Antal és Nyitrai Endre *Mesterséges intelligencia gyakorlati alkalmazásának lehetőségei – okos város, okos rendőrség* című munkájukban kiemelik, hogy egy okosvárosi stratégia kialakításában elengedhetetlen az „okosrendőrség" aktív jelenléte, ennek hiánya magának az okosvárosnak az üzemeltetését és biztonságát is megingathatja (Berki–Nyitrai 2021). Simon Béla szintén hangsúlyozza, hogy mivel a kibertér határokon átívelő környezet, a kiberbűnözés és a biztonsági incidensek elleni fellépéshez a rendészeti szervek folyamatos információmegosztására és specializált együttműködésére van szükség (Simon 2018). Orbók Ákos tanulmánya kiválóan rezonál ezekkel a hazai rendészettudományi törekvésekkel, és éppen ezért nem csupán mérnökök, de rendvédelmi vezetők és közlekedésrendészeti szakemberek számára is fontos a tanulmány.

Összegzés

Orbók Ákos *Az okos város kiberbiztonsága* című tanulmánya rendkívül érdekes és aktuális témát dolgoz fel, és számos elgondolkodtató kérdést vet fel. Ahogy azt a bemutatott hazai és a nemzetközi kutatási eredmények is megerősítették, a kiberbiztonsági rések azonnali közlekedésbiztonsági és társadalmi kihívásokhoz is vezethetnek. A jövő okosvárosa csak akkor maradhat élhető és biztonságos, ha a technológiai innovációt szigorú rendészeti és kiberbiztonsági kontroll kíséri. Ehhez a felismeréshez Orbók tanulmánya stabil, kellő alapot szolgáltató tudományos iránytűként szolgál.

Felhasznált irodalom

Berki Antal – Nyitrai Endre (2021): Mesterséges intelligencia gyakorlati alkalmazásának lehetőségei – okos város, okos rendőrség. *Rendőrségi Tanulmányok,* 4(3), 4–47. Online: https://doi.org/10.53304/RT.2021.3.1

Harangozó Valentin (2025): Kiberbiztonság a városi mobilitásban, fókuszban az e-rollerek, 2. rész. *Hadmérnök,* 20(1), 121–137. Online: https://doi.org/10.32567/hm.2025.1.7

Muha Lajos – Krasznay Csaba (2014): *Az elektronikus információs rendszerek biztonságának menedzselése*. Budapest: Nemzeti Közszolgálati Egyetem. Online: https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/9975/Teljes%20sz%c3%b6veg%21?sequence=2&isAllowed=y

NCC Group (2022): *Putting the Brakes on E-Scooter Security Flaws with Which?* Online: www.nccgroup.com/newsroom/putting-the-brakes-on-e-scooter-security-flaws-with-which

Simon Béla (2018): A rendészeti szervek együttműködése a kiberbűnözés ellen. *Nemzetbiztonsági Szemle,* 6(1), 36–58. Online: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1510/828

Vinayaga-Sureshkanth, Nisha et al. (2020): Security and Privacy Challenges in Upcoming Intelligent Urban Micromobility Transportation Systems. *AutoSec '20: Proceedings of the Second ACM Workshop on Automotive and Aerial Vehicle Security,* 31–35. Online: https://doi.org/10.1145/3375706.3380559