Magyar Rendészet 2026/1. 27–43.
DOI: 10.32577/MR.2026.1.2

RENDÉSZETTUDOMÁNY

A digitális forenzika és kiberbiztonság újgenerációs fejlesztései

Tapasztalatok a National Forensic Sciences University tanulmányútjáról[1]

Next-Generation Developments in Digital Forensics and Cybersecurity

Insights from a Study Visit to the National Forensic Sciences University

BEZERÉDI Imre[2]

Bevezetés: A 21. század első negyedében a digitális technológia rohamos terjedése gyökeresen átalakította a bűnözés természetét és módszereit. Az így keletkező új típusú fenyegetések – mindenekelőtt a kiberbűncselekmények, az illegális *dark web* platformok és a kriptovaluták bűnügyi célú alkalmazása – olyan összetett kihívásokat jelentenek, amelyek hatékony kezeléséhez a bűnüldöző szerveknek interdiszciplináris szemléletre, folyamatos szakmai megújulásra és innovatív technológiai eszközökre van szükségük.

Célkitűzések: A tanulmány célja összefoglalni azokat a szakmai tapasztalatokat, amelyeket a Nemzeti Közszolgálati Egyetem Rendészettudományi Karának oktatói a National Forensic Sciences University (NFSU) által Gandhinagarban, 2025. szeptember 27. és október 4. között szervezett továbbképzésen szereztek. A szerző különös figyelmet fordít annak vizsgálatára, hogy az indiai

[1] A szerző, utazótársaival közösen köszönetét fejezi ki prof. Naveen Kumar Chaudhary igazgatónak és a National Forensic Sciences University valamennyi oktatójának és munkatársának a vendéglátásért és a szakmai tapasztalatok megosztásáért. Külön köszönet illeti prof. Akshat Mehta dékánt, prof. Parag Rughani professzort, prof. Digvijaysinh Rathod dékánt, dr. Hema Acharya asszisztens igazgatót, valamint dr. Nilay Mistry, dr. Ramya Shah, Mr. Kritarth Jhala, dr. Vishal Parmar, prof. Pooja Anuja és dr. Shubham Pandey oktatókat az értékes előadásokért és a részletes technikai bemutatókért. A tanulmányút megvalósulását a Nemzeti Közszolgálati Egyetem és az indiai National Forensic Sciences University közötti kétoldalú együttműködési megállapodás tette lehetővé, amely remélhetőleg hosszú távú szakmai kapcsolat alapjait rakja le a két intézmény között.

[2] Alezredes, tagozatparancsnok-helyettes, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Rendészeti Kiképzési és Nevelési Intézet Rendvédelmi Tagozat, e-mail: bezeredi.imre@uni-nke.hu

digitális forenzikai és kiberbiztonsági modell mely elemei ültethetők át a magyar rendészeti gyakorlatba, figyelembe véve a hazai jogszabályi környezetet, az elérhető technológiai infrastruktúrát és a szervezeti kultúra sajátosságait.

Módszertan: A kutatás módszertani alapját a továbbképzési program keretében gyűjtött közvetlen, empirikus tapasztalatok rendszeres feldolgozása képezi. A részt vevő megfigyelés, az NFSU oktatóival folytatott szakmai konzultációk, valamint az előadásokon és laboratóriumi bemutatókon szerzett ismeretek együttesen tették lehetővé a forenzikus tudományok, a kiberbiztonság és a kriminológia legfrissebb trendjeit bemutató tartalmak mélyreható elemzését, s egyúttal megteremtették az összehasonlító értékelés alapját is.

Eredmények: A tanulmányút során megismert technológiai megoldások a rendészeti innováció számos területét ölelik fel: a mesterséges intelligencia prediktív rendészetben való alkalmazásától a *dark web* és kriptovaluta-ügyek nyomozásán, a mobilforenzika módszerein és a bűnügyi helyszínek háromdimenziós dokumentációján át az agytérképezésig és a poligráfalapú vizsgálati eljárásokig. Az indiai technológiai önállóság modellje – különösen a *Make in India* és a *Make for India* kezdeményezések tapasztalatai – releváns tanulságokkal szolgálhat a hazai fejlesztések tervezéséhez. A képzés megállapításai szerint a PowerShell-használat korlátozása, a Faraday-táskák rendszeresítése, az OSINT-eszközök integrációja, valamint az AI prediktív rendészeti alkalmazása mind számottevő fejlesztési potenciált hordoz.

Konklúzió: A tanulmányút összességében megerősítette, hogy a digitális forenzika és a kiberbiztonság területén a magyar rendészeti rendszernek jelentős fejlődési lehetőségei vannak, amelyek kiaknázásához stratégiai szemléletű tervezés, interdiszciplináris együttműködés és célzott technológiai beruházások szükségesek. A technológiai önállóságra törekvés stratégiai prioritásnak tekintendő; az etikus AI-alkalmazás és a nyílt forráskódú eszközök előnyben részesítése hosszú távon fenntarthatóbb és rugalmasabb megoldást kínál. Az NFSU-val kialakítható jövőbeli partnerség – közös kutatási projektek, hallgatócsere-programok és forenzikus eszközök együttes fejlesztése révén – mindkét intézmény számára kölcsönös előnyökkel kecsegtet.

Kulcsszavak: digitális forenzika, kiberbiztonság, mesterséges intelligencia, prediktív rendészet, NFSU

Introduction: The rapid expansion of digital technologies in the first quarter of the twenty-first century has fundamentally reshaped the nature and methods of criminal activity. The resulting threats – above all the exponential growth of cybercrimes, the proliferation of illegal activities on dark web platforms, and the increasingly widespread criminal exploitation of cryptocurrencies – pose complex challenges that can only be addressed through interdisciplinary approaches, sustained professional development, and the deployment of innovative technological solutions by law enforcement agencies.

Objectives: This study aims to document and analyse the professional experiences gathered by faculty members of the Faculty of Law Enforcement, Ludovika University of Public Service, during the specialised training programme organised by the National Forensic Sciences University (NFSU) in Gandhinagar from 27 September to 4 October 2025. Particular attention is given to identifying which elements of the Indian digital forensics and cybersecurity model could be meaningfully transposed to Hungarian law enforcement practice, taking into account the domestic regulatory framework, the available technological infrastructure, and the specificities of organisational culture.

Methodology: The research draws on systematic analysis of first-hand empirical experiences gathered throughout the training programme. Participatory observation, professional consultations with NFSU faculty, and insights from lectures and laboratory demonstrations collectively enabled an in-depth examination of cutting-edge developments in forensic sciences, cybersecurity, and criminology. This approach simultaneously provided the analytical foundation for a comparative assessment of the Indian model's applicability within the Hungarian law enforcement context.

Results: The study visit brought to light technological solutions spanning multiple domains of law enforcement innovation: from the application of artificial intelligence in predictive policing and the investigation of *dark web* and cryptocurrency-related crimes, through mobile forensics methodologies and three-dimensional crime scene documentation, to brain mapping and polygraph-based examination techniques. India's model of technological self-reliance – in particular the *Make in India* and *Make for India* initiatives – offers instructive lessons for planning domestic developments. The training's key findings indicate that restricting PowerShell usage, introducing Faraday bags, integrating OSINT tools, and deploying AI for predictive policing each hold considerable development potential for Hungarian law enforcement.

Conclusion: The study visit confirmed that Hungarian law enforcement has substantial room for advancement in digital forensics and cybersecurity, the realisation of which requires strategic planning, interdisciplinary collaboration, and targeted technological investment. Pursuing technological self-reliance should be treated as a strategic priority; favouring ethical AI applications and open-source tools offers a more sustainable and adaptable long-term solution. Future partnership with NFSU – through joint research projects, student exchange programmes, and collaborative development of forensic tools – holds the promise of mutual benefit for both institutions.

Keywords: digital forensics, cybersecurity, artificial intelligence, predictive policing, NFSU

Bevezetés

A 21. század első negyedének digitális forradalmával párhuzamosan a bűncselekmények természete és módszertana is gyökeres átalakuláson ment keresztül. Ez szükségessé teszi a bűnüldöző szervek és igazságügyi intézmények folyamatos megújulását, technológiai fejlesztését és nemzetközi együttműködésének elmélyítését. A kibertérben elkövetett bűncselekmények exponenciális növekedése, a *dark web* által facilitált illegális tevékenységek elterjedése, valamint a kriptovaluták bűnügyi felhasználásának növekedése olyan kihívásokat generál, amelyek megoldása interdiszciplináris megközelítést és innovatív technológiai eszközök alkalmazását igényli. Ebben a kontextusban különösen jelentős az olyan vezető forenzikus intézmények szerepe, mint a National Forensic Sciences University, amely 2009-es alapítása óta világszinten is élenjáró szerepet tölt be a forenzikus tudományok oktatásában, kutatásában és gyakorlati alkalmazásában (Patel et al. 2024).

Az indiai Gudzsarát állam kormányának kezdeményezésére Narendra Modi főminiszter víziójaként létrejött egyetem egyedülálló akadémiai környezetet teremtett. Az intézmény teljes mértékben a kriminalisztikai és forenzikus tudományoknak szenteli működését. Ezzel világszinten is elsőként hozott létre olyan integrált oktatási-kutatási platformot, amely a társadalom aktuális biztonsági igényeire adott válaszként folyamatosan bővíti programkínálatát és technológiai infrastruktúráját. A korszerű technológiákat alkalmazó, egyre összetettebb bűncselekmények számának növekedése miatt az állam felismerte a forenzikus tudományok és technológiák fejlesztésének stratégiai szükségességét, így az egyetem létrejötte olyan akadémiai környezetet teremtett, amely világszinten is kiemelkedő eredményeket ért el a kutatás-fejlesztés területén, különösen a bűnügyi nyomozások, fizikai és digitális biztonság innovációs megoldásainak kidolgozásában.[3]

Jelen tanulmány célja, hogy bemutassa azokat a tapasztalatokat, amelyeket magyar rendészeti oktatók és kutatók szereztek a 2025. szeptember 27. és október 4. között megrendezett továbbképzési programon. A program a kiberbiztonság, digitális forenzika, kriminológia és kriminalisztika témaköreit ölelte fel. Hangsúlyt fektetünk az indiai modell azon elemzésére, amelyek adaptálhatók lehetnek a magyar rendészeti gyakorlatban, figyelembe véve a hazai jogszabályi környezetet, technológiai infrastruktúrát és szervezeti kultúrát. A tanulmány részletesen bemutatja az előadások során megismert technológiai innovációkat, módszertani megközelítéseket és gyakorlati alkalmazásokat, amelyek olyan területeket érintenek, mint a mesterséges intelligencia alkalmazása a prediktív rendészetben, a *dark web* és kriptovaluta-bűnözés nyomozása, a mobilforenzika kihívásai, a bűnügyi helyszínek háromdimenziós dokumentációja, valamint az agytérképezés és poligráfalapú vizsgálati technikák használata a bűnügyi nyomozásokban.

[3] Az egyetem jelenlegi struktúrájáról és működéséről az NFSU képviselői által a tanulmányút során tartott bevezető előadásokban szerezhettünk információkat.

A National Forensic Sciences University mint innovatív oktatási és kutatási központ

A National Forensic Sciences University története és fejlődése paradigmatikus példája annak, hogyan válhat egy regionális kezdeményezés nemzetközi jelentőségű intézménynyé, ha megfelelő szakmai támogatást, politikai akaratot és stratégiai vízióval rendelkező vezetést kap egy olyan terület fejlesztésére, amely a modern társadalmak biztonsága szempontjából kritikus. Alapítását követően az egyetem gyors fejlődésnek indult; kezdetben három intézetben mindössze négy képzést kínált, mára azonban több mint negyven, nemzetközileg is elismert programot működtet, köztük olyan úttörő szakokat, mint például a forenzikus fogászat, belbiztonság és terrorizmusellenes tanulmányok, valamint digitális forenzika, amelyek a társadalom aktuális igényeire válaszul jöttek létre és rövid időn belül nagy presztízst szereztek mind az indiai, mind a nemzetközi szakmai közösségben, ahogyan azt prof. dr. Akshat Mehta professzor, dékán az első előadásában ismertette.

Az egyetem 2020 októberében az addigi tudományos és oktatási eredményei elismeréseként az India Kormánya által elfogadott *NFSU Act, 2020* révén Institution of National Importance státuszt, központi egyetemi besorolást kapott. A státusz lehetővé teszi az intézmény számára, hogy saját tantervet dolgozzon ki, akkreditációs jogkörrel rendelkezzen, és nemzetközi együttműködéseket kössön anélkül, hogy minden egyes lépéshez államigazgatási jóváhagyást kellene kérnie. Az NFSU az évek során UGC[4]-elismerést és NAAC[5]-akkreditációt is szerzett, továbbá jelentős eredményeket ért el a kutatás-fejlesztés területén, különösen a bűnügyi nyomozások, fizikai és digitális biztonság innovációs megoldásainak kidolgozásában, amely munkát több kiválósági központ létrehozásával támogatja, mint például a Ballistics Research Centre and Testing Range, a Cyber Defence Centre, az International Centre for Forensic Narcotics és az International Centre for Humanitarian Forensics egységek (Kumar et al. 2025).

Az egyetem jelenleg több indiai campuson működik, amelyek közül a legfontosabbak Gandhinagar, Delhi, Goa, Tripura, Bhopal, Dharwad, Pune, Manipur és Guwahati, valamint nemzetközi helyszíneken is aktív, például Ugandában, ahol a helyi rendészeti és igazságügyi szervekkel együttműködve forenzikus képzéseket nyújt afrikai szakemberek számára. Az intézmény célja, hogy a közeljövőben további globális akadémiai központokat hozzon létre, ezzel elősegítve a forenzikus tudományok nemzetközi szintű oktatási integrációját, ami különösen fontos a transznacionális bűnözés elleni hatékony fellépés és a nemzetközi jogi együttműködés szempontjából, hiszen a különböző országok forenzikus szakembereinek közös szakmai nyelvre és módszertani alapokra van szükségük a hatékony együttműködéshez, amint azt az előadások során többször hangsúlyozták.

Az NFSU küldetése, hogy világszínvonalú képzést és kutatást biztosítson a forenzikus tudományok területén, előmozdítva a tudományos gondolkodást, a bűnüldözés hatékonyságát és a társadalmi biztonságot. Ez összhangban van Leonardo da Vinci

[4] UGC (University Grants Commission) – India felsőoktatási akkreditációs bizottsága, amely a központi egyetemek minőségbiztosításáért felel.

[5] NAAC (National Assessment and Accreditation Council) – Nemzeti Értékelési és Akkreditációs Tanács, amely ötfokú skálán (A++, A+, A, B+, B) minősíti az indiai felsőoktatási intézményeket.

gondolatával, miszerint „To develop a complete mind: Study the science of art; study the art of science. Learn how to see. Realize everything connects to everything else."[6] Ez a holisztikus szemlélet tükröződik az egyetem oktatási filozófiájában is, amely szerint a forenzikus szakembernek nemcsak technikai tudással, hanem széles körű kulturális, társadalmi és pszichológiai ismeretekkel is rendelkeznie kell ahhoz, hogy hatékonyan tudjon dolgozni a modern bűnüldözés összetett környezetében. Ezt a megközelítést prof. dr. Akshat Mehta professzor az egyetem küldetését bemutató előadásában részletesen kifejtette.

A továbbképzési program előadásai és főbb tapasztalatai

A 2025. szeptember 27. és október 4. között megrendezett továbbképzési programon a résztvevők számos előadást hallgattak meg az NFSU vezető kutatóitól és oktatóitól. Az előadások a digitális forenzika, kiberbiztonság és kapcsolódó területek legújabb fejlesztéseit mutatták be, betekintést nyújtva az indiai gyakorlatba és a nemzetközileg is élenjáró kutatási eredményekbe. Az alábbiakban az egyes előadások főbb tartalmát és a magyar rendészeti gyakorlat szempontjából releváns tanulságokat foglaljuk össze.

Mesterséges intelligencia és digitális forenzika a kiberbiztonság szolgálatában

A mesterséges intelligencia és gépi tanulás gyakorlati alkalmazásai a kiberbiztonságban olyan paradigmaváltást jelentenek, ami alapvetően megváltoztatja a bűnüldöző szervek képességeit a kiberfenyegetések észlelésében, elemzésében és elhárításában, miközben új etikai és jogi kérdéseket is felvet a technológia alkalmazásának határait és felelősségét illetően. A prof. Parag Rughani előadása során bemutatott valós incidensek az AI-rendszerek veszélyeit illusztrálták; különösen figyelemre méltó volt a 2018-ban történt Tesla tesztjármű balesete, amely teljes önvezető funkcióban okozott súlyos sérüléseket, valamint az Uber önvezető autójának tragikus esete, amikor a szoftver nem ismerte fel a gyalogosokat, és egy nő meghalt. Az esetek világosan mutatják, hogy az AI-technológia még nem ért el arra a megbízhatósági szintre, amely lehetővé tenné a kritikus helyzetekben való autonóm döntéshozatalt emberi felügyelet nélkül.

Prof. Rughani, az NFSU vezető kutatója a digitális forenzika területén, különösen a memóriaforenzika és automatizált forenzikai eszközök terén ért el jelentős eredményeket (Rughani–Rughani 2017; Gogia–Rughani 2024a). Az előadó kitért az AI három fő kategóriába sorolható tanulási módjaira is. Felügyelt tanulás esetében valaki vagy valami tanítja a rendszert, hasonlóan ahhoz, ahogy a gyerek a szülőtől tanul. A felügyelet nélküli tanulás esetén a rendszer saját tapasztalataiból tanul anélkül, hogy előre meghatározott címkékkel vagy kategóriákkal dolgozna. A megerősítéses tanulás pedig jutalmazás és büntetés rendszerén keresztül működik, hasonlóan ahhoz, ahogy az állatok és emberek tanulnak viselkedésük következményeiből. Ezeket a módszereket alkalmazzák

[6] Leonardo da Vinci gondolatát az egyetem oktatási filozófiájának bemutatása során ismertették az előadók.

például arcfelismerésnél, ahol a rendszer megtanulja felismerni az emberi arcokat különböző megvilágítási körülmények között és különböző szögekből, vagy bűnügyi helyszín rekonstrukciójánál, ahol a rendszer képes azonosítani a különböző bizonyítékok közötti összefüggéseket és rekonstruálni az események lehetséges menetét. Az előadás során különös hangsúlyt kapott a fájlrendszer-forenzika legújabb fejlesztése is, amelyet prof. Rughani kutatócsoportja dolgozott ki az exFAT fájlrendszer elemzésére, és amely kritikus fontosságú a modern digitális eszközök vizsgálatában (Gogia–Rughani 2024b).

Az előadás rendkívül fontos részét a *metaverse-ben* elkövetett bűncselekmények vizsgálata képezte, amely új jogi és etikai területet nyit meg a bűnüldözés számára. 2024-ben az Interpol egy olyan esetet vizsgált, amikor egy nő azt jelentette, hogy a virtuális világban az avatárját csoportosan megerőszakolták, és ez új jogi kérdéseket vetett fel, mivel nem a valós emberrel történt valami, hanem csak a virtuális képmásával, azonban az áldozat pszichológiai traumája ugyanolyan valóságos volt, mint egy fizikai térben történt támadás esetén. Az Interpol speciális munkacsoportot alakított, mert felismerték, hogy az emberek pszichológiailag valósnak érzik a virtuális világban történteket, és a virtuális térben történő bántalmazás ugyanolyan súlyos mentális egészségügyi következményekkel járhat, mint a fizikai térben történő, ami paradigmaváltást igényel a jogrendszerek és bűnüldöző szervek részéről.[7]

Az AI-biztonsági incidensek közül különösen aggasztó volt a sakkozó robotra vonatkozó eset. A robot eltörte egy gyerek ujját, mert az objektumfelismerő rendszere kudarcot vallott, és a gyerek ujját sakkfiguraként azonosította. Hasonlóan sokkoló volt az az elméleti forgatókönyv, hogy valaki az önvezető autó algoritmusát módosíthatná úgy, hogy egy konkrét ember vagy bizonyos típusú emberek esetében ne fékezzen le. Mindezek azt mutatják, hogy az AI-alapú rendszereket lehet káros céllal manipulálni, és hogy a technológia fejlesztői és alkalmazói számára elengedhetetlen az etikai megfontolások beépítése a tervezési folyamatba.

Az MI-alapú megoldások adaptálása a magyar rendészeti gyakorlatban többféle kihívást is jelent. Jogi szempontból a GDPR és a magyar adatvédelmi szabályozás szigorú korlátokat szab az automatizált döntéshozatalnak, különösen olyan érzékeny területeken, mint az arcfelismerés vagy a prediktív rendészet. Szervezeti oldalról jelentős kapacitásfejlesztésre lenne szükség mind a technológiai infrastruktúra, mind a szakemberképzés terén. Etikai kérdésként merül fel az MI-rendszerek átláthatatlansága és a hibalehetőségek kezelése – az előadásban bemutatott esetek (Tesla- és Uber-balesetek, sakkozó robot) világosan illusztrálták, hogy a technológia még nem érett a kritikus döntések önálló meghozatalára. Az alkalmazás előfeltétele a magyar rendészeti rendszerben az átfogó etikai és jogi keret kidolgozása, valamint pilotprojektek indítása kontrollált környezetben.

[7] Az esetet dr. Rughani előadása során ismertette, az Interpol Virtual Policing Programme keretében folytatott vizsgálat részleteként.

A kiberbiztonság gyakorlati aspektusai és az indiai függetlenségi törekvések

Prof. Digvijaysinh Rathod, aki 21 éves tapasztalattal rendelkezik a kiberbiztonság terén, az egyetem Kibervédelmi Kiválósági Központjáról beszélt, amely már négy éve működik, és közvetlenül az indiai kormányt védi a kiberfenyegetésekkel szemben. A központ emellett oktatási és kutatási tevékenységet is folytat, hozzájárulva a kiberbiztonság legújabb kihívásainak kezeléséhez. A központ három fő területen működik: hagyományos IT-biztonság, amely a szokásos számítógépes hálózatok és rendszerek védelmét foglalja magában; ipari vezérlőrendszerek biztonsága, amelyek az erőműveket és kritikus infrastruktúrákat irányítják, és amelyek kompromittálása katasztrofális következményekkel járhat; valamint az 5G-hálózatok biztonsága, amely különösen fontos, mivel az 5G összekapcsolja az internetet és az ipari rendszereket, létrehozva a dolgok ipari internete (*industrial internet of things,* IIoT) ökoszisztémát, amely új típusú sebezhetőségeket idéz elő.

Az előadó nagy hangsúlyt fektetett India *Make in India* és *Make for India* programok keretében megvalósuló technológiai függetlenségi törekvéseire, hogy az ország saját technológiákat fejlesszen, és csökkentse az amerikai és izraeli technológiai függőséget, ami kritikus nemzetbiztonsági kérdés egy geopolitikai feszültségek kereszttüzében álló országban. Különösen fontos ez, mert sok indiai tehetség az USA-ban dolgozik, és az amerikai kormányzat olyan szigorú vízumszabályokat vezetett be, amelyek meggátolják az indiai szakemberek visszatérését; a *brain drain* jelenség hosszú távon veszélyezteti India technológiai fejlődését és innovációs kapacitását.

Az előadás legfontosabb része egy valós támadási szimulációról szólt, amelyet egy nagy energiaelosztó üzemnél végeztek teljesen offenzív jelleggel. A cél a rendszer sebezhetőségeinek feltárása és a védelmi képességek fejlesztése volt. A biztonsági csapat egyetlen IP-címből kiindulva 19 nap alatt 7676 kritikus rendszert kompromittált. Ez magában foglalta az e-mail-szervereket, a tartománykiszolgálókat (*domain* szervereket) és végül a programozható logikai vezérlőket (*programmable logic controller,* PLC) is, amelyek az energiaelosztást közvetlenül vezérlik. Ezzel demonstrálták, hogy egy motivált és szakképzett támadó képes lehet teljesen átvenni egy kritikus infrastruktúra irányítását. Az előadó részletesen bemutatta a támadás lépéseit, amely passzív információgyűjtéssel indult, keresőmotorok (Shodan és Censys, valamint Google Dorking) segítségével azonosítva a sebezhetőségeket a nyilvánosan elérhető információkból, majd PowerShell-t használtak a laterális mozgáshoz, amivel sikerült *admin* jogosultságokat szerezniük a rendszerben.

A fő tanulság az volt, hogy a megfelelő hálózati szegmentáció, amely zónákra és csatornákra osztja a hálózatot, megakadályozza, hogy egy kompromittált rendszerről könnyedén át lehessen ugrani más rendszerekre, valamint az első védelmi vonal az ilyen típusú támadások ellen a PowerShell szigorú korlátozása lenne. Az előadó hangsúlyozta, hogy soha nem szabad *admin* jogosultságokkal futtatni a PowerShellt normál felhasználói környezetben, mert ez lehetővé teszi a támadók számára, hogy az egyik gépről a másikra ugorjanak anélkül, hogy észlelni lehetne. A PowerShell rendkívül hatékony eszköz a Windows-rendszerek adminisztrációjához, de ugyanilyen hatékony eszköz a támadók kezében is a laterális mozgáshoz és a jogosultságok eszkalációjához.

Az indiai *Make in India* és *Make for India* programok inspirálók lehetnek Magyarország számára is a technológiai függetlenség csökkentése terén. A PowerShell szigorú korlátozásának módszere azonnal implementálható lenne a magyar rendészeti és közigazgatási IT-rendszerekben, minimális költséggel, de jelentős biztonsági előnyökkel. A hálózati szegmentáció szükségessége meghatározó a magyar kritikus infrastruktúrák védelmében. Ugyanakkor figyelembe kell venni, hogy India lakosságszáma és gazdasági mérete lehetővé teszi a nagy volumenű saját fejlesztéseket, ami Magyarországnak jóval nehezebb feladat. Reálisabb cél lehet a regionális együttműködés erősítése (V4-, EU-szintű projektek) és a nyílt forráskódú megoldások előnyben részesítése.

Forenzikus tudomány a drogellenes nyomozásban és a nemzetközi együttműködés szükségessége

Prof. Aastha Pandey átfogó képet nyújtott a forenzikus tudomány szerepéről a kábítószerekkel kapcsolatos bűncselekmények nyomozásában, amely az indiai kontextusban különösen összetett kihívást jelent az ország földrajzi elhelyezkedése és a szomszédos országok drogtermelése miatt. Az 1985-ben hatályba lépett indiai NDPS (Narcotic Drugs and Psychotropic Substances) törvény szigorúan szabályozza a drogok kezelését, előállítását, terjesztését és fogyasztását, azonban a kihívások nagyok, különösen a szintetikus drogok térhódítása és a nemzetközi drogcsempészet bonyolult hálózatai miatt.

Az előadó nemzetközi összehasonlításokat mutatott be, amelyek segítségével kontextusba helyezte az indiai drogpolitikát más országok megközelítésével szemben. Magyarországon *zero tolerance* politika van érvényben a tiltott szerekkel kapcsolatban, az alkohol azonban teljesen legális. Ez utóbbi jelentős társadalmi problémákat okoz, beleértve az alkoholizmus társadalmi és gazdasági költségeit, a közlekedési baleseteket és az egészségügyi problémákat. Hasonlóképpen, India is minden drogot tiltólistán kezel. Ugyanakkor bizonyos hagyományos szerek, mint például a kannabisz használata kulturális és vallási kontextusban összetett jogi kérdéseket vet fel, ami különbséget jelent a magyar gyakorlathoz képest. A forenzikus laboratórium több kritikus feladatot végez a drogokkal kapcsolatos nyomozások során: először is azonosítja, hogy egy adott anyag valóban kábítószer-e, ami kvalitatív analízist jelent különböző spektroszkópiai és kromatográfiai módszerekkel; másodszor meghatározza a mennyiséget, ami kvantitatív analízis és kritikus a jogi eljárások szempontjából, mivel a birtokolt drog mennyisége határozza meg a büntetés mértékét; harmadszor megállapítja a forrást, vagyis képesek azonosítani, hogy a drog Afganisztánból, Bangladesből vagy más forrásból származik-e, amely információ kritikus a nemzetközi bűnügyi együttműködés és a forrásoldali fellépés szempontjából.

Az előadó kiemelte a dizájnerdrogok növekvő problémáját, amelyeket úgy terveznek, hogy megkerüljék a jogszabályokat azzal, hogy kémiailag kissé eltérnek a tiltott anyagoktól, azonban hasonló vagy akár erősebb pszichoaktív hatással rendelkeznek, mint a már jegyzékbe vett anyagok. Ezek a szerek rendkívül gyorsan változnak és fejlődnek, amint egy adott vegyületet betiltanak, a bűnözők kissé módosított változatot állítanak elő, amely még nem szerepel a tiltott anyagok listáján; folyamatos macska-egér játék jön létre a jogalkotók és a droggyártók között. Az egyetem laboratóriuma ISO 17025 és ISO 9001

tanúsítvánnyal rendelkezik, ami nemzetközileg elismert standardokat jelent a tesztelési és kalibrálási laboratóriumok kompetenciájára vonatkozóan, és éves szinten száznál több esetet kezel különböző típusú drogokkal kapcsolatban.

A leggyakrabban lefoglalt drogok India területén a kannabisz és az ópium, de az elmúlt években a szintetikus anyagok, különösen a metamfetamin és a mefedron mennyisége jelentősen nőtt. Ez tükrözi a globális trendet, az átállást a hagyományos természetes drogokról a szintetikus anyagokra, amelyek könnyebben előállíthatók, szállíthatók és elrejthetők. Az előadó megemlítette az új kihívásokat is, mint például a hordozható tesztelési eszközök szükségességét, amelyek lehetővé teszik a helyszíni gyorstesztelést anélkül, hogy a mintákat laboratóriumba kellene szállítani, valamint a szennyvíz-epidemiológia módszerét, amely azt jelenti, hogy a szennyvízből mintákat vesznek és elemzik a drogok jelenlétét, ami alapján meg lehet becsülni egy adott terület drogfogyasztási szintjét és trendjeinek alakulását.

A bemutatott forenzikus módszerek nagy része már részben alkalmazásban van Magyarországon is, azonban a szennyvíz-epidemiológia módszere jelentős fejlesztési potenciált kínál a drogfogyasztási trendek feltérképezésére. A dizájnerdrogok gyors változásának problémája Magyarországon is akut, ezért hasznos lenne átvenni az indiai tapasztalatokat a gyors reagálású jogalkotás terén. A nemzetközi együttműködés nélkülözhetetlen, különösen a balkáni útvonal közelsége miatt. Az ISO tanúsítványok beszerzése a magyar forenzikus laboratóriumok számára prioritás kellene hogy legyen a nemzetközi elfogadottság biztosításáért.

A *dark web* és kriptovaluta-alapú bűnözés új dimenziói

Dr. Ramya Shah előadása az indiai digitális pénzügyi rendszer robbanásszerű növekedésével kezdődött, amely paradigmatikus változást hozott az ország gazdasági életében, és amely új típusú bűnözési formák megjelenését is lehetővé tette. Az egységes fizetési rendszeren (*unified payments interface,* UPI) keresztül 2025 májusában 18 milliárd tranzakció történt, közel 2,5 billió indiai rúpia értékben, ez pedig nyilvánvalóan mutatja, hogy a pénzügyi elektronizálódás India teljes gazdaságát áthatotta, és hogy az ország rendkívül gyorsan halad a *cashless* társadalom irányába. Azonban ezzel párhuzamosan a kiberbűncselekmények száma is drámaian nőtt: online csalások, digitális pénzügyi visszaélések és kriptovaluta-alapú bűncselekmények.

Az előadó olyan eseteket említett, mint amikor technikus dolgozók, akik feltételezhetően magasabb szintű digitális műveltséggel rendelkeznek, mint az átlagpopuláció, 15 millió rúpiát (több százezer dollár) veszítettek digitális letartóztatási csalások miatt, amelyek során a bűnözők rendőri vagy kormányzati tisztviselőknek adják ki magukat, és azzal fenyegetik az áldozatokat, hogy ha nem utalnak át azonnal pénzt, letartóztatják őket állítólagos bűncselekmények miatt. Még a tanultabbak is könnyen áldozattá válhatnak tehát, ha nem rendelkeznek megfelelő tudatossággal és felkészültséggel a digitális fenyegetésekkel szemben.

Az előadó szerint a probléma gyökerében az emberi tényező áll, minden technológiai biztonsági rendszer leggyengébb láncszeme. Az IBM kutatásai szerint az adatszivárgások

74%-a emberi hibából történik globálisan, de Indiában ez az arány 95% feletti, ami rendkívül aggasztó statisztika, és rámutat arra, hogy a technológiai védekezés önmagában nem elegendő, szükség van átfogó oktatási és tudatosságnövelő programokra is. Az emberek rendkívül gyenge jelszavakat használnak, a leggyakoribbak az 123456789, az admin@123 és a password, amely jelszavakat egy támadó másodpercek alatt feltörhet egyszerű *brute force* vagy *dictionary attack* módszerekkel.

A felhasználók gyakorta mellőzik az összetett jelszavak használatát a kényelem miatt, ezért inkább egyszerű, könnyen megjegyezhető jelszavakat választanak, ez azonban rendkívül veszélyes biztonsági gyakorlat.

A titkosságot sokan elhanyagolják, nem törlik rendszeresen az e-maileket és a nem kívánt fotókat, ami három fő problémát okoz: a tárhely megtelik, és nem lehet új adatokat tárolni; a számtalan fénykép között nem találják meg azt az egyet, amit keresnek; illetve komoly biztonsági kockázatot jelent. Mire ugyanis a felhasználók – például egy hosszú repülőút során, unalmukban – rászánják magukat az adatok törlésére, gyakran már túl késő, és a feleslegesen tárolt, lényeges információk addigra kiszivárognak vagy kompromittálódnak.

A *dark web* nem mítosz vagy egy technológiailag felkészületlen emberek számára hozzáférhetetlen tér, hanem jól szervezett illegális gazdaság, amely párhuzamos struktúrát alkot a legális internettel, és amely különböző illegális szolgáltatásokat és termékeket kínál. Az előadó szerint az internet szerkezetét sok ember tévedésből képzeli el egyetlen rétegként, a valódi szerkezet három fő rétegből áll: a felületi web a hagyományos keresőmotorokkal elérhető és indexált tartalmakat jelenti; a mély web keresőmotorok által nem indexált, de technológiailag nem rejtett tartalmakat jelenti, mint például a jelszóval védett e-mail-fiók vagy online banki felület; valamint a *dark net,* amely speciális szoftverekkel, mint a Tor böngésző, érhető el, és amely tudatosan rejti el a felhasználók és szolgáltatások azonosságát.

A *dark weben* a drogkereskedelem mellett fegyverek illegális értékesítése, professzionális hackerszolgáltatások bérlése, lopott adatok és dokumentumok vásárlása, valamint terrorfinanszírozás is zajlik, és ökoszisztémát alkot illegális termékekkel és szolgáltatásokkal. Az egyik megdöbbentő eset, amelyet az előadó megosztott, egy 13 éves fiúról szólt, aki 18 bitcoint keresett illegális tevékenységekkel. A fiú YouTube-videókról tanulta meg a szükséges technikákat. Az illegális technológiák megismerése tehát rendkívül egyszerű, és a fiatalok különösen sebezhetők.

A terroristák is átálltak a kriptovalutákra, ami komoly kihívást jelent a nemzetközi terrorellenes erőfeszítések számára. Az előadó kutatásai szerint a terrorista szervezetek 60–65%-a mostanra kriptovalutát használ a finanszírozáshoz, vagyis a hagyományos, banki tranzakciókon alapuló pénzügyi nyomkövetési módszerek kevésbé hatékonyak. Közönséges emberek akaratlanul, tudtuk nélkül is kapcsolódhatnak a terrorfinanszírozáshoz, ha terrorista tevékenységhez kapcsolódó kriptotárcába transzferálnak, mivel a kriptovaluta-tranzakciók pszeudoanonimek, és nehéz nyomon követni a pénz eredetét és célját.

A *dark web* nyomozásának jogi keretei Magyarországon még fejlesztésre szorulnak. Az indiai gyakorlat szerint alkalmazott *gateway* szintű monitorozás komoly adatvédelmi kérdéseket vet fel az európai jogrendszerben. Reálisabb megközelítés lehet a nyílt forrású hírszerzési (*open source intelligence,* OSINT) technikák fejlesztése és a nemzetközi

együttműködés erősítése (Europol-, Interpol-platformokon). A kriptovaluta-nyomkövetés terén érdemes lenne képzési programokat indítani a magyar nyomozók számára, mivel ez a terület gyorsan fejlődik és speciális szakértelmet igényel.

A mobilforenzika kihívásai és a titkosítás evolúciója

A mobilforenzika területén tapasztalható technológiai fejlődés és a titkosítási mechanizmusok folyamatos erősödése rendkívül összetett kihívásokat jelent a forenzikai szakemberek számára, amelyeket Mr. Kritarth Jhala részletes technikai előadása világított meg. A mobilforenzika az egyik legdrágább digitális forenzikai terület, mivel rendkívül sok különféle operációs rendszer és verzió létezik, amelyekhez egyedi adatkinyerési módszereket kell fejleszteni. Az Android operációs rendszernek 16 különböző fő verziója van, az iOS-nek pedig 18, és minden egyes verzióhoz külön forenzikai eszközöket és technikákat kell fejleszteni, mivel a belső fájlrendszer, titkosítási mechanizmusok és biztonsági funkciók verziónként jelentősen változnak.

A titkosítás fejlődése óriási kihívást jelent a forenzikai szakemberek számára. Korábban a teljes eszköztitkosítás rendszerét (*full device encryption,* FDE) használták, ahol az egész eszköz egy mester titkosítási kulccsal volt titkosítva, ami azt jelentette, hogy ha a forenzikai szakembernek sikerült feltörnie vagy megszereznie ezt az egy kulcsot, hozzáférést kapott az összes adathoz. 2019 után azonban az FBE *(file based encryption)* vált általánossá az Android- és iOS-rendszerekben, ami azt jelenti, hogy minden egyes fájl külön titkosítási kulccsal van védve, és ez rendkívüli mértékben megnehezíti a forenzikai elemzést. Ha egy telefonon 1,5 millió fájl van, akkor potenciálisan 1,5 millió különböző titkosítási kulccsal kell megbirkózni, ami gyakorlatilag lehetetlenné teszi a hagyományos *brute force* módszereket.

Az eredeti berendezésgyártók (*original equipment manufacturer,* OEM), mint például a Samsung, Sony és Vivo, a nyílt forráskódú Android operációs rendszerre rátettek egy úgynevezett *wrapper* vagy csomagoló réteget, amely javítja a biztonsági paramétereket, és további védelmi mechanizmusokat ad hozzá: a forenzikai szakembereknek meg kell kerülniük vagy fel kell törniük ezt a további védelmi réteget is, mielőtt hozzáférnének az alapvető operációs rendszerhez. A harmadik féltől származó alkalmazások, mint a WhatsApp Plus vagy más módosított üzenetküldő alkalmazások szintén jelentős problémákat okoznak, mivel ezek nem a hivatalos alkalmazásboltokból származnak, és gyakran extra funkciókat kínálnak, mint például képesség arra, hogy 1500 fős csoportokat kezelhessenek, vagy hogy az üzeneteket törölhessék a fogadótól anélkül, hogy nyom maradna, ami rendkívül megnehezíti a forenzikai vizsgálatot.

Az előadó megemlített egy *app masking* nevű technikát is, ahol egy ártalmatlannak tűnő alkalmazás, például egy számológép titkos alkalmazást rejt. Speciális kód beírása a számológépbe rejtett funkciót nyit meg, például egy titkosított üzenetküldő alkalmazást vagy illegális tartalmakat tároló teret. Indiának csak két városában, Mumbaiban és Hyderabadban működik *gateway* szintű forgalomfigyelés, amely lehetővé teszi, hogy a hatóságok valós időben monitorozzák az internetforgalmat, és automatikusan kiszűrjék az olyan kulcsszavakat tartalmazó kommunikációt, mint a „bomba” vagy

„gyermekpornográfia", ami kritikus lehet terrorista támadások vagy súlyos bűncselekmények megelőzése szempontjából.

Az adat-helyreállítás terén is vannak jelentős korlátok, amelyeket a forenzikai szakembereknek ismerniük kell. A null könyvtár koncepciója fontos ebből a szempontból: egy mobiltelefon vagy pendrive tárhelyének egy bizonyos területét az OEM-gyártó fenntartja illesztőprogramok és rendszerfájlok tárolására, amely terület körülbelül 0,25 és 1,5 GB között van a készülék típusától függően. Amikor adatot törölnek a normál felhasználói felületről, a törölt adatok nyomai ebben a null könyvtárban maradnak, ami lehetővé teszi a forenzikai helyreállítást. Ha azonban valaki a *wipe* vagy *overwrite* műveletet végzi, vagyis az összes bináris 1-est 0-val helyettesíti az adatok teljes területén, az adat végleg helyreállíthatatlan lesz, mivel fizikailag felülírták az eredeti információt.

Indiában 2026-tól újfajta jogszabályok lépnek életbe, amelyek alapvetően megváltoztatják a forenzikai munka jogi kereteit. Bevezették az integrált büntetőjogi rendszert (*integrated criminal justice system,* ICJS), amely teljes mértékben integrálja a rendőrséget, az ügyészséget, a bíróságokat és a laboratóriumokat egyetlen digitális platformon, így lehetővé téve a gyorsabb információcserét és az átláthatóbb eljárásokat. Mandátumrendszert is bevezetnek: csak a felhatalmazott szakértők, mint az NFSU professzorai és az akkreditált forenzikai laboratóriumok munkatársai végezhetnek bíróság előtt elfogadható forenzikai vizsgálatokat, nem pedig magánszolgáltatók vagy nem akkreditált szakemberek, ami javítja a bizonyítékok megbízhatóságát és csökkenti a szakértői vélemények közötti ellentmondásokat.

A mobilforenzika területén bemutatott kihívások Magyarországon is jelentkeznek. A Faraday-táskák kötelező alkalmazása azonnal bevezetendő lenne minden mobilforenzikai eljárás során – ez alacsony költségű, de nagy hatású intézkedés. A fájlalapú titkosítás (FBE) által támasztott kihívások megoldása nemzetközi együttműködést igényel, mivel egyetlen ország sem képes egyedül megfelelni a nagy gyártók (Apple, Samsung stb.) által alkalmazott titkosítási mechanizmusoknak. Az integrált büntetőjogi rendszer (ICJS) típusú platform bevezetése Magyarországon is hasznos lenne, azonban ez jelentős IT-fejlesztési beruházást és jogszabályi változtatásokat igényelne.

Agytérképezés és neurológiai vizsgálati módszerek a nyomozásban

Dr. Vishal Parmar két előadásában a poligráfalapú vizsgálati technikákat és az agytérképezés legújabb módszereit mutatta be, amelyek bár vitatottak bizonyos jogi rendszerekben, Indiában elfogadott és széles körben használt nyomozati eszközök. A poligráf, közismert nevén hazugságdetektor, három fő fiziológiai paramétert mér folyamatosan a vizsgálat során: a pulzust, a légzést, amely magában foglalja a légzési frekvenciát és mélységet; valamint a bőr vezetőképességét, amely a verejtékezés mértékét mutatja.

Az elmélet az, hogy amikor valaki hazudik vagy igazat mond egy számára fontos vagy stresszes kérdésről, ezek a fiziológiai paraméterek megváltoznak, mivel a test autonóm idegrendszere reagál az érzelmi stresszre, és ezek a változások nem kontrollálhatók tudatosan a legtöbb ember számára. Azonban a poligráfnak vannak jelentős korlátai,

amelyeket nem lehet figyelmen kívül hagyni. Nem 100%-os pontosságú, és az eredmények sok különböző faktortól függenek, beleértve a vizsgálatot végző szakember tapasztalatát és képzettségét, a vizsgált személy pszichológiai állapotát, kulturális hátterét és még az időjárási körülményeket is. Az emberek kulturális háttere különösen befolyásolja az eredményeket, mivel különböző kultúrákban az emberek másképp reagálnak a stresszre, és másképp fejezik ki az érzelmeiket.

Az előadás második részében dr. Parmar az agyi elektromos oszcillációs aláírás technológiát (*brain electrical oscillation signature,* BEOS) mutatta be, amely az agy elektromos aktivitásának mérésén alapul, és amelynek célja, hogy megállapítsa, egy személy valóban megtapasztalt-e adott eseményt, vagy csak hallott róla, és rendelkezik fogalmi tudással anélkül, hogy személyesen részt vett volna benne (Parmar 2017). A vizsgálat során a gyanúsítottra egy 32 elektródás EEG-sapkát helyeznek, amely az agy minden területét lefedi, és amely képes mérni az agy elektromos aktivitását milliszekundumos felbontással. A vizsgálat során különböző auditív és vizuális stimulusokat mutatnak be a gyanúsítottnak, és az agy automatikusan reagál ezekre a stimulusokra anélkül, hogy a gyanúsított tudatosan kontrollálni tudná a reakcióit. A technológia képes különbséget tenni a tapasztalati tudás (személyesen megtapasztal) és a fogalmi tudás között (csak hallott valamiről vagy olvasott róla). Az alapvető különbség jól megérthető egy konkrét példán keresztül: ha egy személy valóban kést használt egy gyilkosságban, és a késre vonatkozó stimulusokat mutatnak neki be, az agy aktív reagálása mutatkozik a prefrontális kéregben, amely a memória és a tapasztalati feldolgozás központja. Aki azonban nem követte el a bűncselekményt, csak hallott róla a médiából vagy másoktól, nem mutat ilyen intenzív és specifikus aktivitást ezen az agyi területen.

A BEOS rendkívül pontos az indiai szakemberek szerint: 99,91%-os a pontossága, és ha az eredmény nem eléggé egyértelmű első alkalommal, keresztellenőrzést végeznek különböző típusú stimulusokkal mindaddig, amíg el nem érik a 100%-os bizonyosságot. Az időkeret szintén kritikus a vizsgálat pontossága szempontjából: a vizsgálat nagyon konkrét időpontról vagy időszakról kell hogy szóljon, például 2022 májusának egy meghatározott napjáról, hogy az agy tudja, melyik specifikus eseményre kell emlékeznie, és melyik memóriát kell aktiválnia. A BEOS-t az indiai kormány szabadalmaztatta, és elsősorban magas profilú ügyekben használják, ahol rendkívül fontos a pontos és megbízható eredmény, mint például terrorista merényletekkel vagy politikai gyilkosságokkal kapcsolatos ügyekben.

A BEOS és poligráfmódszerek alkalmazása komoly etikai és jogi kérdéseket vet fel az európai kontextusban. Míg Indiában ezek elfogadott bizonyítékok, az Európai Unióban és Magyarországon szigorúbbak a szabályok. Az Emberi Jogok Európai Bíróságának (EJEB) gyakorlata szerint a neurológiai vizsgálatok eredményei csak kiegészítő jellegűek lehetnek, nem alapjai az ítéletnek. A technológia 99,91%-os pontosságának állítása is kritikus vizsgálatot igényelne független szakértői testület által. A módszer bevezetése előtt átfogó etikai és jogi konzultációra lenne szükség, és csak meghatározott típusú ügyekben (például nemzetbiztonsági kérdések) lehetne reálisan alkalmazható.

A kiberbűnözés nyomozási technikái és IoT-biztonsági kihívások

Dr. Nilay Mistry a kiberbűnözés nyomozásának gyakorlati oldalát mutatta be az NFSU digitális törvényszéki laboratóriumában tartott előadás során, részletesen ismertetve az internet rétegeit – a felszínit, a mélyt és a *dark webet* –, és bemutatva, hogyan használják ezeket a nyomozások során (Mandela et al. 2024). Rávilágított arra, hogy a személyes adatok az interneten gyakorlatilag örökre elérhetők maradnak, és hogy az adatkereskedelem kiterjedt, strukturált rendszeren alapul, és teljes illegális gazdasági szektort képvisel. Kiemelte a szürkepiacon forgalmazott személyes adatok értékét, valamint bemutatta az adatszivárgás, adathalászat és IP-nyomkövetés módszereit, amelyek a modern kiberbűnözés alapvető eszközei.

Gyakorlati példákon keresztül szemléltette a nyílt forrású hírszerzési technikákat, mint például a LinkedIn-adatbányászatot Python- és R-scriptekkel, Twitter-fiókok nyomozását vagy Grabify-alapú IP-geolokalizációt, amelyek demonstrálják, hogy mennyi információ gyűjthető össze nyilvánosan elérhető forrásokból megfelelő eszközökkel és technikákkal. Hangsúlyozta a védekezés fontosságát, mint a domainblokkolás, a PhishTank- és VirusTotal-rendszerek integrálása, valamint az adatbiztonsági tudatosság erősítése szervezeti és egyéni szinten egyaránt.

A dolgok internetének (*internet of things,* IoT) eszközei, biztonsági kihívásai különösen nagy figyelmet kaptak az előadás során. Az IoT-alapú mezőgazdasági rendszerek *(IoT in agriculture,* IoTA) sebezhetőségei kibertámadásoknak és kiberbűncselekményeknek teszik ki őket, miközben a digitális forenzikai vizsgálatok is komoly kihívásokkal néznek szembe ezeken az eszközökön (Rudrakar–Rughani 2022). Az előadó bemutatta, hogy az IoT-eszközök gyakran nem rendelkeznek megfelelő biztonsági mechanizmusokkal, mivel a gyártók elsősorban a funkcionalitásra és a költséghatékonyságra összpontosítanak, nem pedig a biztonságra, ami azt jelenti, hogy ezek az eszközök könnyen kompromittálhatók és *botnetek* részévé válhatnak.

A bemutatott OSINT-technikák nagy része nyílt forráskódú eszközökkel implementálható, így költséghatékony megoldást jelentenek a magyar rendészet számára. Az IoT biztonsági kihívások különösen relevánsak Magyarországon is, ahol a mezőgazdasági szektorban is egyre nagyobb mértékben terjednek az IoT-alapú megoldások. Ajánlott lenne szakmai műhelyek szervezése az OSINT-eszközök gyakorlati alkalmazásáról, valamint pilotprojektek indítása IoT-sebezhetőségi vizsgálatok terén. A PhishTank és VirusTotal típusú rendszerek integrálása a magyar rendészeti informatikai infrastruktúrába szintén prioritást élvezhet.

Következtetések és stratégiai ajánlások

A tanulmányút során szerzett tapasztalatok alapján egyértelműen megállapítható, hogy a digitális forenzika és kiberbiztonság területén jelentős fejlesztési potenciál rejlik a magyar rendészetben, mindez pedig interdiszciplináris megközelítést, nemzetközi együttműködést és jelentős technológiai beruházásokat igényel. A legfontosabb tanulságok között szerepel a PowerShell használatának szigorú korlátozása adminisztrátori

jogosultság nélküli környezetekben: egyszerű, költségmentes intézkedés, de drámaian csökkentheti a laterális mozgás lehetőségét a hálózaton belül, ahogy azt a prof. Rathod által bemutatott valós támadási szimuláció is demonstrálta.

A Faraday-táskák kötelező alkalmazása minden mobilforenzikai eljárás során kritikus fontosságú az elektromágneses szennyeződés megelőzése és a bizonyítékok integritásának megőrzése szempontjából, mivel a mobiltelefonok továbbra is kommunikálhatnak cellatornyokkal és vezeték nélküli hálózatokkal addig, amíg nincsenek megfelelően szigetelve. Az OSINT-technológiák integrálása a modern nyomozásokba elengedhetetlen, mivel a nyílt forráskódú információk rendkívül gazdagok és gyakran gyorsabban hozzáférhetők, mint a hagyományos titkosszolgálati vagy rendőrségi adatbázisok, ahogy azt dr. Mistry előadása is bemutatta.

A mesterséges intelligencia és a prediktív rendészet nem távoli jövőbeli vízió, hanem már ma is működő gyakorlat számos országban, és Magyarországnak is érdemes lenne pilotprojekteket indítani ezeken a területeken, különösen a nagy forgalmú városokban vagy kritikus infrastruktúrák védelmében. A technológiai függetlenség stratégiai fontosságú cél, mivel a külföldi technológiai függőség biztonsági kockázatokat hordoz, és korlátozza az ország manőverezési képességét válsághelyzetekben, ahogy azt az indiai *Make in India* és *Make for India* programok is demonstrálják.

Az etikus AI-használat és a nyílt forráskódú eszközök előnyben részesítése hosszú távon fenntarthatóbb és költséghatékonyabb megoldás, mint a zárt, proprietárius rendszerek használata, amelyek *vendor lock-in-t* hoznak létre, és amelyeknek nincsenek átlátható működési mechanizmusaik. A jövőbeli együttműködési lehetőségek között szerepelhetnek közös kutatási projektek az NFSU-val, hallgatócserék, közös konferenciák szervezése és forenzikus eszközök közös fejlesztése, amelyek mindkét ország számára előnyösek lehetnek, és amelyek elősegítik a tudástranszfert és a legjobb gyakorlatok megosztását (Patel et al. 2024; Kumar et al. 2025).

A költség-haszon elemzés alapján a technológiai fejlesztések több kategóriába sorolhatók: az alacsony költségű megoldások közé tartozik az OWASP ZAP és a PhishTank API használata, valamint a PowerShell biztonsági politika módosítása; a közepes költségű beruházások közé a Faraday-táskák beszerzése és az OSINT-előfizetések; míg a magas költségű fejlesztések között szerepel a 3D LIDAR Faro M70 rendszer VR-integrációval, a BEOS-típusú EEG-rendszer és egy 128 magos feldolgozóegységgel működő Kibervédelmi Központ létrehozása.

Ahogyan az indiai szakemberek hangsúlyozták: „Úgy tanulsz úszni, hogy belépsz a vízbe." A tanulmányút tapasztalatai is azt mutatják, hogy az új technológiák megértése és alkalmazása csak aktív részvétellel, gyakorlati kísérletezéssel és nemzetközi együttműködéssel lehetséges. A National Forensic Sciences University által bemutatott modell olyan inspirációt nyújt, amely adaptálható a magyar kontextusba, figyelembe véve a hazai jogszabályi környezetet, a rendelkezésre álló erőforrásokat és a specifikus nemzeti biztonsági kihívásokat.

Felhasznált irodalom

Gogia, Gaurav – Rughani, Parag (2024a): A Detailed Study of Advancements in Digital Forensics. In Singh, Yashwant et al. (szerk.): *Proceedings of International Conference on Recent Innovations in Computing. ICRIC 2023.* Lecture Notes in Electrical Engineering (Vol. 1194). Singapore: Springer, 333–349. Online: https://doi.org/10.1007/978-981-97-2839-8_23

Gogia, Gaurav – Rughani, Parag (2024b): PAREX: A Novel exFAT Parser for File System Forensics. *Computación y Sistemas,* 28(2), 421–433. Online: https://doi.org/10.13053/CyS-28-2-4804

Kumar, Ahlad et al. szerk. (2025): *Digital Defence: Harnessing the Power of Artificial Intelligence for Cybersecurity and Digital Forensics*. Boca Raton: CRC Press. Online: https://doi.org/10.1201/9781032714813

Mandela, Ngaira et al. (2024): Exploring the Use of Tails Operating System in Cybercrime and Its Impact on Law Enforcement Investigations. *In 11th International Conference on Computing for Sustainable Global Development (INDIACom).* New Delhi, India, 1109–1114. Online: https://doi.org/10.23919/INDIACom61295.2024.10499122

Parmar, Vishal (2017): Brain Electrical Oscillation Signature Profiling (BEOS). *International Journal of Computers in Clinical Practice,* 2(1), 45–58. Online: https://doi.org/10.4018/IJCCP.2017010101

Patel, Sankita J. et al. szerk. (2024): *Information Security, Privacy and Digital Forensics: Select Proceedings of the International Conference, ICISPD 2022.* Lecture Notes in Electrical Engineering (1075). Singapore: Springer, Online: https://doi.org/10.1007/978-981-99-5091-1

Rudrakar, Santoshi – Rughani, Parag (2022): IoT Based Agriculture (IoTA): Architecture, Cyber Attack, Cyber Crime and Digital Forensics Challenges. *Research Square Preprint*. Online: https://doi.org/10.21203/rs.3.rs-2042812/v1

Rughani, Vimal – Rughani, Parag (2017): AUMFOR: Automated Memory Forensics for Malware Analysis. *Asian Journal of Engineering and Applied Technology,* 6(2), 36–39. Online: https://doi.org/10.51983/ajeat-2017.6.2.2781