ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉS

TÉZISFÜZETE

HEGYI HENRIETTA

Internetkapcsolatra képes személygépjárművek információs rendszereinek biztonsági vizsgálata

Témavezető: Dr. Erdődi László

BIZTONSÁGTUDOMÁNYI DOKTORI ISKOLA

Budapest, 2025.11.16.

Tartalomjegyzék

1 Summary

This doctoral study investigates the information security challenges of information systems in internet-connected passenger vehicles, focusing on the European regulatory, technological, and user perception aspects. As the automotive industry undergoes digital transformation, connected vehicles have evolved into complex data processing and communication units, integrating with external infrastructures, cloud services, and other vehicles. This transformation brings new cybersecurity risks and data protection concerns, as vehicles become both targets and sources of cyber threats.

The research analyzes the European regulatory environment, with particular emphasis on the heterogeneity and fragmentation of existing norms such as the UNECE R155/R156 regulations, GDPR, and NIS2 Directive. A comparative analysis is made with global regulatory trends, including the rapid technological and market expansion of Chinese electric vehicles in the European Union, which introduces additional geopolitical and information security risks.

Methodologically, the study applies a multidisciplinary approach: qualitative and quantitative empirical data collection (surveys and expert interviews), thematic content analysis, and the assessment of security protocols in automotive communication. The research highlights significant discrepancies between regulatory intentions and real-world practices, particularly in risk management, public awareness, and supply chain security.

The main scientific contributions of the thesis are the identification of new threat vectors in connected vehicles, the critical evaluation of existing cybersecurity frameworks, and the proposal of an integrated risk management model that also addresses the specific risks posed by third-country manufacturers. The results have practical applicability for both regulatory authorities and industry actors, supporting the development of harmonized, effective information security standards for the future of connected mobility.

2 A kutatás előzményei

Az internetkapcsolatra képes személygépjárművek megjelenése alapvetően alakította át a közlekedés, az adatkezelés és a kiberbiztonság ökoszisztémáját. A modern személygépkocsik már nem csupán közlekedési eszközként, hanem folyamatos adatgyűjtő, adatfeldolgozó és adattovábbító egységként is funkcionálnak. Ezek a járművek képesek nagy mennyiségű – akár óránként több száz megabyte-nyi – adat előállítására és továbbítására, melyek felhasználhatók saját működésük optimalizálása, városi infrastruktúrák támogatása, vagy éppen biztosítási és üzleti célú elemzések számára.

A szakirodalom és a gyakorlati tapasztalatok egyaránt rávilágítanak arra, hogy a személygépjárművek által generált adatok érzékeny, személyes információkat hordoznak, melyek profilalkotásra, megfigyelésre, sőt visszaélésekre is lehetőséget adnak. A felhasználók sokszor nincsenek tudatában annak, hogy járművük milyen adatokat továbbít, kinek, és milyen célból, miközben a hozzájárulásuk gyakran csak formális, szerződési feltételekbe ágyazva jelenik meg. A technológiai fejlődés üteme meghaladja a szabályozási környezet alkalmazkodóképességét: az európai uniós szabályozások, mint a GDPR, a NIS2 és a gépjárműipari kiberbiztonsági szabványok (pl. UNECE R155/R156, ISO/SAE 21434) sok esetben csak keretjellegű, egymással részben átfedő vagy eltérő mélységű követelményeket támasztanak.

A témakör iránti érdeklődést és a kutatás jelentőségét tovább növeli a kínai gyártmányú elektromos járművek európai térhódítása, amely új típusú információbiztonsági és nemzetbiztonsági kockázatokat hordoz. A kínai szabályozási környezet eltérő adatkezelési és végrehajtási logikákat követ, az EU-n kívüli gyártók adatgyűjtési gyakorlata pedig sokszor kívül esik az európai adatvédelmi normarendszeren. Ezzel párhuzamosan a kínai járművek gyorsan növekvő piaci részesedése és technológiai befolyása új típusú fenyegetéseket vet fel a teljes közlekedési infrastruktúra szintjén.

A kutatási téma tehát egyaránt kapcsolódik a technológiai fejlődés, a szabályozási környezet változásai, valamint a társadalmi bizalom és tájékozottság kérdésköréhez. A szakirodalmi előzmények és gyakorlati tapasztalatok alapján világosan látható, hogy a jövő közlekedése és adatbiztonsága csak multidiszciplináris megközelítéssel, szabályozási, technológiai és társadalmi szempontok együttes vizsgálatával érthető meg és tehető biztonságossá.

3 Célkitűzések

Az elmúlt években a személygépjárművek digitalizációja és hálózatba kapcsolása gyökeresen átalakította a közúti közlekedés technológiai, társadalmi és információbiztonsági dimenzióit. Az információbiztonság jelentősége fokozatosan nőtt, mivel az internetkapcsolatos járművek ma már összetett, nagymennyiségű adatot kezelő informatikai rendszerek, melyek érzékeny személyes és működési adatokat is feldolgoznak. Az iparág fejlődése, a globális piacok összefonódása, valamint a kínai elektromos járművek európai térnyerése egyaránt hozzájárulnak a biztonsági kockázatok, a szabályozási kihívások és a társadalmi bizalom kérdéskörének komplexitásához.

Kutatásom célja annak feltárása volt, hogy a jelenlegi európai szabályozási környezet mennyiben képes hatékony és egységes védelmet biztosítani az internetkapcsolatra képes személygépjárművek számára, különös tekintettel a kiberbiztonság, az adatvédelem, valamint a harmadik országokból származó technológiák integrációja során jelentkező problémákra. Emellett vizsgáltam, hogy a járműhasználók mennyire ismerik járműveik adatkezelési és adattovábbítási gyakorlatait, és érzékelik-e a rejtett adatfolyamok és a nem átlátható adatkezelés potenciális biztonsági kockázatait.

A kutatásom során kiemelten fontosnak tartottam az európai és globális szabályozási környezet kritikai elemzését. Ennek részeként elemeztem, hogy az internetkapcsolatos járművekre vonatkozó szabályozások (mint például a GDPR, a NIS2 irányelv, az UNECE R155/R156 előírások vagy az ISO/SAE 21434 szabvány) mennyire képesek átfogó és koherens védelmet nyújtani a feltörekvő fenyegetésekkel szemben, különösen a komplex beszállítói láncok és harmadik országbeli gyártók bevonásával.

Fontos célkitűzés volt annak vizsgálata is, hogy a szabályozásokban előírt kockázatelemzési módszerek a teljes járműéletciklust, valamint a különböző érintetti szinteket (jármű, szervezet, ökoszisztéma) megfelelően lefedik-e. Mindezek mellett részletesen elemeztem a végfelhasználók tájékozottságát, információbiztonsági tudatosságát és attitűdjeit, továbbá azt, hogy a jelenlegi edukációs és tájékoztatási mechanizmusok mennyire támogatják a kockázatok felismerését és kezelését.

Külön kutatási fókuszt jelentett a járművekben alkalmazott kommunikációs protokollok vizsgálata, melynek célja annak feltárása volt, hogy ezek a rendszerek lehetővé teszik-e rejtett csatornák kialakítását, illetve hogy milyen technikai és szabályozási eszközök szükségesek ezen fenyegetések megelőzéséhez és detektálásához. A fenti vizsgálatok eredményeként egy

elméleti modellt dolgoztam ki és validáltam, amely képes kimutatni, hogy az internetkapcsolatos, fejlett vezetéstámogató rendszerekkel rendelkező járművek milyen módon válhatnak érzékeny adatok rejtett továbbítására alkalmas eszközökké, és mindez milyen biztonságpolitikai vagy nemzetbiztonsági következményekkel járhat akár flottaszinten is.

Kutatási céljaim összefoglalva:

- Az internetkapcsolatos személygépjárművek európai és globális szabályozási környezetének kritikai elemzése, különös tekintettel a kiberbiztonsági és adatvédelmi kihívásokra.
- A kockázatelemzési módszerek vizsgálata, azok alkalmazhatóságának értékelése a járművek teljes életciklusa és a különböző érintetti szintek mentén.
- A járműhasználók információbiztonsági tudatosságának, attitűdjeinek és a jelenlegi edukációs, tájékoztatási rendszerek hatékonyságának feltérképezése.
- A járműkommunikációs protokollok vizsgálata a rejtett csatornák kialakításának és megelőzésének szempontjából.
- Egy új elméleti modell kidolgozása és validálása, amely alkalmas a rejtett adatáramlás és az ebből fakadó biztonságpolitikai kihívások elemzésére.

A kutatás célkitűzései együttesen hozzájárulnak a személygépjárművek információbiztonsági kihívásainak, a szabályozási környezet hiányosságainak és a felhasználói tudatosság kérdéskörének mélyebb megértéséhez, valamint a jövőbeli, biztonságosabb járműhasználat elősegítéséhez.

4 Vizsgálati módszerek

A modern, internetkapcsolatos személygépjárművek információbiztonságának vizsgálata komplex, interdiszciplináris megközelítést igényelt, amely során a technológiai, jogi, szervezeti és társadalmi tényezőket egyaránt figyelembe vettem. Kutatásom során alapvető célom volt, hogy a szabályozási környezet, a járműtechnológia, valamint a felhasználói szokások egymásra hatását, összefüggéseit és kölcsönös kockázatait rendszerszinten értelmezzem.

A vizsgálatot elsődlegesen az európai és globális szabályozási környezet részletes, kritikus elemzésével kezdtem. E körben kvalitatív dokumentumelemzést alkalmaztam, amely során a legfontosabb nemzetközi és európai jogszabályok (így például a GDPR, a NIS2, az UNECE R155/R156 előírások és az ISO/SAE 21434 szabvány) szerkezetét, tartalmi elemeit és

gyakorlati alkalmazhatóságát három, egymást kiegészítő módszerrel elemeztem. Egyrészt keretalapú tartalomelemzést végeztem, amely lehetővé tette, hogy a szabályozások főbb kockázatelemzési logikáit, elvárásait és a privacy by design, illetve kiberbiztonság by design elveit szisztematikusan azonosítsam. Másrészt tematikus tartalomelemzést alkalmaztam, amely során a különböző jogszabályok és ajánlások szövegéből a leggyakrabban visszatérő témákat, problémákat, kockázatokat és hiányosságokat gyűjtöttem össze, különös tekintettel az adatáramlásra, incidenskezelésre, auditálásra és a harmonizációs kihívásokra. Végül funkcionális összehasonlító elemzést is végeztem, amelynek keretében a különböző szabályozások és szabványok gyakorlati alkalmazhatóságát és átfedéseit, illetve hiányosságait vetettem össze, különösen a beszállítói láncok és harmadik országbeli gyártók beilleszkedése szempontjából.

A szabályozási elemzést kiegészítve, nagy hangsúlyt fektettem az empirikus kutatási módszerekre is. Ennek részeként kvantitatív, nagymintás kérdőíves felmérést készítettem a járműhasználók körében annak feltárására, hogy milyen mértékben ismerik és értik a járműveik által végzett adatgyűjtést, adatkezelést és továbbítást, illetve hogyan viszonyulnak a felmerülő biztonsági kockázatokhoz. A kvantitatív eredményeket kvalitatív, félig strukturált szakértői interjúkkal egészítettem ki, amelyeket iparági szereplőkkel, szabályozókkal, valamint információbiztonsági szakemberekkel készítettem. Ezek az interjúk hozzájárultak ahhoz, hogy feltárjam a gyakorlati tapasztalatokat, nézőpontokat és a mindennapi kihívásokat, amelyek az adatbiztonságot és kiberbiztonságot a járműiparban jellemzik.

Kutatásom további pillérét képezte a járművekben alkalmazott kommunikációs protokollok és technológiák biztonsági vizsgálata. Ezt részben elméleti, részben gyakorlati elemzéssel végeztem, a teljes kommunikációs láncot az OSI-modell mentén vizsgálva. Elemzéseim során különös figyelmet fordítottam a CAN és MQTT protokollok fenyegetésmodellezésére (pl. STRIDE módszer alkalmazásával), és azt vizsgáltam, hogy ezek a rendszerek milyen mértékben teszik lehetővé rejtett adatcsatornák (covert channel) kialakítását és működtetését, illetve milyen privacy- és adatvédelmi kockázatok fakadnak ebből.

A vizsgálatok eredményeként egy elméleti modellt dolgoztam ki az érzékeny adatok rejtett továbbításának kimutatására. E modell fejlesztése során az egyes járművekben található szenzoradatok – úgymint képi, hang- vagy helyzetadatok – mennyiségi elemzését is elvégeztem, különös tekintettel arra, hogy ezek miként képezhetik egy komplex, akár flottaszintű adatátviteli rendszer alapját. A modell alkalmazhatóságát és validitását mind elméleti, mind gyakorlati szempontból teszteltem.

Kutatásom során folyamatosan figyelemmel kísértem a témához kapcsolódó hazai és nemzetközi szakirodalmat, valamint beépítettem a legfrissebb tudományos és gyakorlati eredményeket a módszertan fejlesztésébe. A módszerek komplex alkalmazása lehetővé tette, hogy a személygépjárművek információbiztonsági kihívásait – a szabályozási környezetet, a technológiai és felhasználói oldalakat is beleértve – átfogóan, rendszerszinten értelmezzem.

5 Új tudományos eredmények

A kutatásaim során a kutatási kérdések vizsgálatával a következő téziseket állítottam fel:

T1: Az Európai Unió jelenleg érvényes szabályozási környezete hézagos, csak foltszerű védelmet képes nyújtani a személygépjárművekkel kapcsolatos ismert fenyegetések ellen.

[HH1], [HH2], [HH3]

T2: A szabályozások által elvárt kockázatelemzési módszerek nem alkalmasak az internetkapcsolatra képes személygépjárművekkel kapcsolatos összes kockázat kezelésére, mivel vagy csak a járműre, vagy csak a szervezetre fókuszálnak és használatukat nem ellenőrzi egységes hatóság.

[HH1], [HH2], [HH3]

T3: Az internetkapcsolatra képes járművek vásárlói nem kapnak megfelelő tájékoztatást a biztonsági kockázatokkal kapcsolatban, elsősorban a technológia fejlődésből adódó kényelmi funkciókra koncentrálnak, így nem fordítanak figyelmet a kockázatokra.

[HH4], [HH5], [HH6]

T4: Az internetkapcsolattal rendelkező járművek kommunikációs protokolljai – funkcionális követelményeik (pl. alacsony késleltetés, korlátozott erőforrás-használat) miatt – alkalmasak rejtett csatornák létrehozására, amelyek technikai védelmi eszközökkel, például titkosítással, nem szüntethetők meg teljes mértékben. Ezért a rejtett csatornák azonosítása és célzott védelmi intézkedések kidolgozása elengedhetetlen a járműkommunikáció biztonságának fenntartásához.

[HH7], [HH8]

T5: A dolgozatban bemutatott modell alapján megállapítható, hogy az internetre kapcsolt személygépjárművek – különösen a fejlett vezetéstámogató rendszerekkel rendelkező

járművek – képesek rejtett módon nagy mennyiségű érzékeny adat továbbítására, amely flottaszinten kritikus nemzetbiztonsági kockázatot jelenthet kijelölt objektumok vagy célszemélyek megfigyelése esetén.

[HH9]

6 Az eredmények hasznosítási lehetősége

A disszertációban feltárt tudományos eredmények számos területen kínálnak közvetlenül hasznosítható gyakorlati megoldásokat a járműipar, a szabályozás, valamint a társadalom számára. Munkám hozzájárulhat ahhoz, hogy az európai és magyar szabályozói környezet a jelenleginél hatékonyabban kezelje az internetkapcsolatos személygépjárművek információbiztonsági kihívásait, különös tekintettel a harmadik országokból származó járművek és a globális beszállítói láncok integrációjára.

Az általam kidolgozott, integrált kockázatmenedzsment-modell alkalmazható lehet a jogalkotók és a felügyeleti szervek számára új, harmonizált szabályozási és megfelelőségi keretrendszerek kialakításában, különösen a kiberbiztonsági, adatvédelmi és auditmechanizmusok fejlesztésénél. Ugyanakkor a modell a gyártók, beszállítók és flottakezelők belső biztonsági stratégiáinak, kontrollfolyamatainak kialakításában és fejlesztésében is hasznosítható, különös figyelmet fordítva a harmadik országbeli technológiák beillesztéséből fakadó kockázatokra.

Kiemelten fontosnak tartom a felhasználók, különösen a végfelhasználók információbiztonsági tudatosságának növelését, amely alapfeltétele a korszerű adatvédelemnek és a járművek biztonságos működésének. Az empirikus kutatás során gyűjtött adatok és elemzések támpontot adhatnak jövőbeli edukációs és tájékoztató programok tervezéséhez, valamint hozzájárulhatnak a társadalmi bizalom növeléséhez az új technológiák iránt.

A dolgozat módszertani és modellezési eredményei alapul szolgálhatnak további tudományos vizsgálatokhoz is, legyen szó a járműipari kiberbiztonság technológiai, szabályozási vagy társadalmi aspektusairól. A kutatás során feltárt kommunikációs protokoll-kockázatok, illetve az érzékeny adatok rejtett továbbításának lehetőségei új irányokat nyithatnak a járműkommunikáció, a privacy, valamint a nemzetbiztonsági elemzések területén is.

Végül, de nem utolsósorban, az eredmények felhasználhatók a nemzetbiztonsági szervek és felügyeleti hatóságok számára a kínai elektromos járművek európai térnyeréséből fakadó kockázatok felismerésében és értékelésében, hozzájárulva ahhoz, hogy a jövőben a szabályozói döntéshozatal a technológiai és geopolitikai kihívásokat is megfelelően kezelni tudja.

A kutatás tehát multidiszciplináris módon, több szinten és szereplő számára kínál kézzelfogható alkalmazási lehetőségeket, amelyek hozzájárulhatnak a jövő biztonságosabb, átláthatóbb és tudatosabb közlekedési rendszerének kialakításához.

7 Irodalmi hivatkozások listája/ Irodalomjegyzék

[1] Hofmann, Martin; Neukart, Florian; Bäck, Thomas: Artificial Intelligence and Data Science in the Automotive Industry, 2017.

[2] Marabelli, M.; Hansen, S.; Newell, S.; Frigerio, C.: The Light and Dark Side of the Black Box: Sensor-based Technology in the Automotive Industry. Communications of the Association for Information Systems, 40(16) (2017), pp. 368–388.

[3] Ogbuke, Nnamdi Johnson; Yusuf, Yahaya Y.; Dharma, Kovvuri; Mercangoz, Burcu A.: Big data supply chain analytics: ethical, privacy and security challenges posed to business, industries and society. Production Planning & Control, 31(11–12) (2020), pp. 965–978.

[4] Oliver, N.; Pentland, A. P.: Driver Behavior Recognition and Prediction in a SmartCar, 2000.

[5] Peppes, Nikolaos; Alexakis, Theodoros; Adamopoulou, Evgenia; Demestichas, Konstantinos: Driver Behavior Monitoring Based on Smartphone Sensor Data and Machine Learning Methods. In 2019 25th Conference of Open Innovations Association (FRUCT) (2019), pp. 1–7.

[6] Bódi, A., Maros, D., & Gáspár, L. (2023). A közlekedésbiztonság fokozása a Komplex ITS Ökoszisztémával. KTI Magyar Közlekedéstudományi és Logisztikai Intézet.

[7] Bódi, A. (2022). Közlekedésbiztonság fokozását megalapozó Komplex ITS Ökoszisztéma kialakításának kérdései. Doktori értekezés, Óbudai Egyetem, Biztonságtudományi Doktori Iskola.

[8]Bloom, C., Tan, J., Ramjohn, J., & Bauer, L. (2017). Self-driving cars and data collection: Privacy perceptions of networked autonomous vehicles. USENIX Symposium on Usable Privacy and Security.

[9] Bódi, A., & Maros, D. (2022). A közös európai mobilitási adattér és az ITS ökoszisztéma tanúsíthatósága. Közlekedés és Mobilitás, 1(1), 38–42.

[10] Krasznay, Cs. (2022). Kiberbiztonság a XXI. században. Katonai Nemzetbiztonsági Szolgálat.

[11] Krasznay, Cs. (2020). Okoseszközök a kritikus információs infrastruktúrákban. In Török, B. (szerk.), Információ- és kiberbiztonság (pp. 121–147). Ludovika Egyetemi Kiadó.

[12] Kovács, L., & Krasznay, Cs. (2010). Digitális Mohács – Egy kibertámadási forgatókönyv Magyarország ellen. Nemzet és Biztonság, 2010. február.

[13] Bódi, A., & Maros, D. (2021). Az 5G-hálózat és a közlekedés információbiztonsági kihívásai. Híradástechnika, 76(HTE Infokom 2020), 35–40.

[14] Török, Á., Szalay, Z., & Sághi, B. (2020). New Aspects of Integrity Levels in Automotive Industry-Cybersecurity of Automated Vehicles. IEEE Transactions on Intelligent Transportation Systems.

[15] Jekl, B., Dabčević, Z., Németh, B., Škugor, B., & Gáspár, P. (2025). Scenario-Optimization-Based Velocity Planning of Autonomous Vehicles for Interacting With Pedestrians. IEEE Transactions on Intelligent Transportation Systems.

[16]Caltrider, J.; Rykov, M.; MacDonald, Z.: What Data Does My Car Collect About Me and Where Does It Go? Mozilla Foundation, 2023.

[17]Bódi, A., & Bartal, A. (2022). Az okosjárművek adatkezelésének kérdései. Információs Társadalom, 22(1), 21-40.

[18] A. Stocker, C. Kaiser, M. Fellmann, “Quantified Vehicles: Novel Services for Vehicle Lifecycle Data,” Business & Information Systems Engineering, vol. 59, pp. 125–130, 2017. https://www.researchgate.net/publication/313546098_Quantified_Vehicles_Novel_Services_for_Vehicle_Lifecycle_Data

[19] B. Gözübüyük, B. Tang, K. G. Shin, M. D. Pesé, “Analyzing Privacy Implications of Data Collection in Android Automotive OS,” 2024. https://arxiv.org/abs/2409.15561

[20] T. Alam, “Data Privacy and Security in Autonomous Connected Vehicles,” Data Journals, vol. 8, no. 9, 2024. https://www.mdpi.com/2504-2289/8/9/95

[21] N. Yuca et al., “A Survey on Privacy-Preserving Computing in the Automotive Domain,” 2025. https://arxiv.org/abs/2508.01798

[22] Dombora Sándor: Eredményes információbiztonsági rendszerek kialakítása és bevezetése. Óbudai Egyetem. URL: http://www.lib.uni-obuda.hu/sites/lib.uni-obuda.hu/files/Dombora_Sandor_ertekezes.pdf (Letöltve: 2024.11.17.)

[23] Wired: GM Took 5 Years to Fix a Full-Takeover Hack on Millions of OnStar Cars. URL: https://www.wired.com/2015/09/gm-took-5-years-fix-full-takeover-hack-millions-onstar-cars/#:~:text=7%3A00%20AM-,GM%20Took%205%20Years%20to%20Fix%20a%20Full%2DTakeover%20Hack,known%20remote%20car%20hacking%20technique. (Letöltve: 2024.11.17.)

[24] Wired: Hackers Remotely Kill a Jeep on the Highway. URL: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ (Letöltve: 2024.11.17.)

[25] Sam Curry: Hacking Kia. URL: https://samcurry.net/hacking-kia (Letöltve: 2024.11.17.)

[26] Mercator Institute for China Studies, „Europe's position in global EV market”, 2021.

[27]H. Hegyi, „Cybersecurity Challenges in the Era of Chinese Electric Passenger Vehicles: A Qualitative Study Investigating Data Security Measures in the European Union,” AARMS, vol. 23, no. 2, pp. 63–75, 2024, doi: 10.32565/aarms.2024.2.5.

[28] S&P Global Mobility, “The rise of Chinese auto brands in Europe,” 2023.

[29] European Automobile Manufacturers Association (ACEA), “Market Report 2024,”

[30] JATO Dynamics, “Chinese automakers double European market share in May,” 2025.

[31] Fleetnews, “Chinese brands gain ground and double market share across Europe,” May 2025.

[32] JATO Dynamics, “European registrations of Chinese car brands soar in January,” Jan. 2025.

[33] Reuters, “China's carmakers expanding their presence in Europe,” July 2025.

[34] The Times, “BYD electric cars overtake Tesla sales in Europe,” Apr. 2025. [chinacarOnline

[35] Reuters, “Tesla's European sales slump for fifth month,” June 2025.

[36] European Commission, “Countervailing duties on Chinese EV imports,” 2024.

[37] Wikipedia contributors, “Automotive industry in China,” Wikipedia, 2025.

[38] Államtanács, „Stratégiai feltörekvő iparágak fejlesztése Kínában”, 2010.

[39] S. Curry, „Web application vulnerabilities in vehicles”, 2023.

[40] European Commission, „EU-China – A strategic outlook”, 2022.

[41] J. Mock, Z. Yang, „China's electric vehicle market policies”, Energy Policy, 2021.

[42] ACEA, „EU car imports overview”, 2021.

[43] ENISA, „Cybersecurity Certification and ENISA’s Role”, 2022.

[44] McKinsey & Company: Car connectivity: What consumers want and are willing to pay. URL: https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/car-connectivity-what-consumers-want-and-are-willing-to-pay (Letöltve: 2024.11.17.)

[45] Airlinq: 8 Industries Being Transformed by Connected Car Data. URL: https://www.airlinq.com/8-industries-being-transformed-by-connected-car-data/ (Letöltve: 2024.11.17.)

[46] MDPI Sensors: Sensors: Special Issue on Advanced Connected Vehicle Technology. 21(22), 2021. URL: https://www.mdpi.com/1424-8220/21/22/7712 (Letöltve: 2024.11.17.)

[47] IEEE: Connected Vehicle Security Threat Analysis. IEEE Access, 2018. URL: https://ieeexplore.ieee.org/document/8515151 (Letöltve: 2024.11.17.)

[48] Pinsent Masons: The connected car raises a new world of data management, privacy, and ownership. URL: https://www.pinsentmasons.com/out-law/analysis/the-connected-car-raises-new-world-of-data-management-privacy-and-ownership (Letöltve: 2024.11.17.)

[49] Al-Saadi, M., & Hammad, M.: Connected vehicles: Technology review, state of the art, challenges and opportunities. Sensors, 21(22) (2021), p. 7712. DOI: https://doi.org/10.3390/s21227712.

[50] U.S. Department of Transportation: How connected vehicles work. URL: https://www.transportation.gov/research-and-technology/how-connected-vehicles-work (Letöltve: 2024.11.17.)

[51] Khan, Shah Khalid; Shiwakoti, Nirajan; Stasinopoulos, Peter; Chen, Yilun: Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions. Accident Analysis & Prevention, 148 (2020), p. 105837.

[52] Weimerskirch, A., Gaynier, R.: An Overview of Automotive Cybersecurity: Challenges and Solution Approaches, 2015.

[53] Koubatis, Andrew; Schonberger, Jorge Yerena: Risk management of complex critical systems. International Journal of Critical Infrastructures, 1(2/3) (2005), pp. 200–213.

[54] Gardner, D.: Risk: The Science and Politics of Fear. Random House, New York, 2009.

[55] G. Danezis, Introduction to Privacy Technology. KU Leuven COSIC Lecture, 2007. [1SPOnline

[56] M. Deng, K. Wuyts, R. Scandariato, B. Preneel, W. Joosen, "A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements," Requirements Engineering, vol. 16, no. 1, pp. 3–32, 2011.

[57] C. Lázaro, D. Le Métayer, "Control over Personal Data: True Remedy or Fairy Tale?" SCRIPTed, vol. 12, no. 1, pp. 3–30, 2015.

[58] M. Raciti and G. Bella, "Up-to-date Threat Modelling for Soft Privacy on Smart Cars," arXiv, 2023. [SPOnline

[59] Mouha, R.: Internet of Things (IoT). Journal of Data Analysis and Information Processing, 9 (2021), pp. 1–12.

[60] Szczepaniuk, H.; Szczepaniuk, E. K.: Standardization of IoT Ecosystems: Open Challenges, Current Solutions, and Future Directions. CRC Press, 2022.

[61] K. W. Abbott and D. Snidal, "Hard and Soft Law in International Governance," International Organization, vol. 54, no. 3, pp. 421–456, 2000.

[62] A. Peters and R. Pagotto, "Soft Law as a New Mode of Governance," New Modes of Governance Project, 2006.

[63] Braun, V., Clarke, V.: Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2) (2006), pp. 77–101. URL: https://dl1.cuni.cz/pluginfile.php/1195620/mod_folder/content/0/Braun%20and%20Clarke%202006%20Thematic%20analysis.pdf (Letöltve: 2024.11.17.)

[64] U. Kischel, Comparative Law. Oxford, U.K.: Oxford Univ. Press, 2019.

[65] C.-L. Hwang and K. Yoon, Multiple Attribute Decision Making: Methods and Applications. Berlin, Germany: Springer, 1981.

[66] ENISA, Threat Landscape for Connected and Automated Mobility. Athens, Greece: European Union Agency for Cybersecurity, 2021.

[67] OECD, Regulatory Impact Analysis (RIA): Best Practice Principles for Regulatory Policy. Paris, France: OECD Publishing, 2020.

[68] V. Belton and T. J. Stewart, Multiple Criteria Decision Analysis: An Integrated Approach. Boston, MA, USA: Springer, 2002.

[69] Krippendorff, K.: Content Analysis. An Introduction to Its Methodology. Thousand Oaks: SAGE, 2018.

[70]Lincoln, Y. S., & Guba, E. G. (1985). Naturalistic Inquiry. Sage.

[71]Patton, M. Q. (2015). Qualitative Research & Evaluation Methods. Sage.

[72]Braun, V., & Clarke, V. (2019). Reflecting on reflexive thematic analysis. Qualitative Research in Sport, Exercise and Health, 11(4), 589–597.

[73]Bryman, A. (2016). Social Research Methods. Oxford University Press.

[74] Fowler, F. J., Couper, M. P., Lepkowski, J. M.: Survey Methodology. John Wiley & Sons, 2011. ISBN: 978-0470465462.

[75] Gideon, L.: Handbook of Survey Methodology for the Social Sciences. Springer, 2012. DOI: 10.1007/978-1-4614-3876-2.

[76] Bairagi, V., Munot, M. V.: Research Methodology: A Practical and Scientific Approach. CRC Press, 2019. ISBN: 978-0367256206.

[77] Adams, J., Khan, H. T. A., Raeside, R., White, D.: Research Methods for Graduate Business and Social Science Students. SAGE Publications, 2007. ISBN: 978-0761935896.

[78] Creswell, J. W., Plano Clark, V. L.: Designing and Conducting Mixed Methods Research. 2. kiadás. Sage Publications, 2011. URL: https://archive.org/details/designingconduct0000cres_i7e7 (Letöltve: 2024.11.17.)

[79]Krosnick, J. A., & Presser, S. (2010). Question and Questionnaire Design. In Handbook of Survey Research (2nd ed., pp. 263–314). Emerald Group Publishing.

[80]DeVellis, R. F. (2017). Scale Development: Theory and Applications (4th ed.). Sage Publications.

[81]Hunyadi, L. & Vita, L. (2008). A kérdőíves vizsgálatok módszertana. Budapest: Aula Kiadó.

[82]Robson, C., & McCartan, K. (2016). Real World Research (4th ed.). Wiley.

[83] R. K. Ahuja, *Research Methods*, New Delhi: Rawat Publications, 2001.

[84] S. N. Hesse-Biber, *The Practice of Qualitative Research*, 3rd ed. London: SAGE Publications, 2016.

[85]Creswell, J. W., & Plano Clark, V. L. (2017). Designing and Conducting Mixed Methods Research. Sage.

[86] Small, M. L. (2009). 'How many cases do I need?' On science and the logic of case selection in field-based research. Ethnography, 10(1), 5–38.

[87] Flick, U. (2018). An Introduction to Qualitative Research (6th edition). Sage.

[88] Kelemen-Erdős, Anikó; Mitev, Ariel: Holisztikus szolgáltatásélmény-vendég-utazás és kölcsönös értékteremtés dimenziói az art-és romkocsmák példáján. Marketing & Menedzsment, 50(3–4) (2016), pp. 45–56.

[89] Babbie, Earl: A társadalomtudományi kutatás gyakorlata. Balassi Kiadó, 2020.

[90] Kelemen-Erdős, Anikó; Mitev, Ariel: Tematikus szolgáltatásélmény art-és romkocsma környezetben. Turisztikai és Vidékfejlesztési Tanulmányok, 2(3) (2017), pp. 45–56.

[91] Kelemen-Erdős, Anikó; Molnár, Adél: Cooperation or conflict? The nature of the collaboration of Marketing and Sales organizational units. Economics and Culture, 16(1) (2019), pp. 45–56.

[92] C. Riessman, *Narrative Methods for the Human Sciences*, Thousand Oaks: Sage, 2008.

[93] J. Corbin and A. Strauss, *Basics of Qualitative Research*, 3rd ed. Thousand Oaks, CA: SAGE Publications, 2008.

[94] S. Yang, Y. Chen, Z. Song, et al., “Automotive Cybersecurity: A Survey on Frameworks, Standards, and Testing and Monitoring Technologies,” Sensors, vol. 24, no. 18, p. 6139, 2024.

[95] G. T. Ho, D. S. Wang, et al., “Security Analysis of In-Vehicle Networks and Protocols,” Vehicular Communications, vol. 43, p. 100639, 2023.

[96] A. Velinov, A. Mileva, S. Wendzel, W. Mazurczyk, “Covert Channels in the MQTT-based Internet of Things,” IEEE Access, vol. 7, pp. 161899–161915, 2019.

[97] H. S. Kim, H. Lee, et al., “Security and Privacy of MQTT and CoAP Protocols for the Internet of Things,” Wireless Networks, vol. 28, pp. 3221–3240, 2022.

[98] I. Ghafir, K. Prenosil, et al., “A Survey of IoT Protocols Security: MQTT, CoAP, AMQP and Beyond,” Wireless Networks, vol. 29, pp. 4921–4940, 2023.

[99] A. Shostack, Threat Modeling: Designing for Security, Wiley, 2014.

[100] B. Mosayyebpour, S. Ebrahimi, “Performance of Cryptographic Algorithms for Secure MQTT and HTTP Communications in IoT,” Information Systems Frontiers, vol. 25, pp. 965–982, 2023.

[101] S. Zander, G. Armitage, P. Branch, "A Survey of Covert Channels and Countermeasures in Computer Network Protocols," IEEE Communications Surveys & Tutorials, vol. 9, no. 3, pp. 44–57, 2007.

[102] A. Velinov et al., "Covert Channels in the MQTT-based Internet of Things," IEEE Access, vol. 7, pp. 161899–161915, 2019.

[103] B. Molnár, A. Csábrági, B. Forstner, "Képadat-védelmi kockázatok a járműfedélzeti rendszerekben," Infokommunikáció és Jog, vol. 18, no. 2, pp. 30–39, 2021.

[104] R. Togneri, D. Pullella, "An Overview of Speaker Identification: Accuracy, Robustness and Security," IEEE Circuits and Systems Magazine, vol. 11, no. 2, pp. 23–61, 2011.

[105] S. Mosaad, H. Hamza és I. A. Saroit, “Coverage in Mobile Wireless Sensor Networks (M-WSN): A Survey,” Computer Communications, vol. 110, pp. 1–13, 2017.

[106] J. Liu, G. Yue, S. Shen, H. Shang és H. Li, “Coverage Capacity Optimization for Mobile Sensor Networks Based on Evolutionary Games,” Mathematical Problems in Engineering, vol. 2014, Article ID 264307, 2014.

[107] V. S. Batista et al., “On the Coverage of Bus-Based Mobile Sensing,” Sensors (Basel), vol. 18, no. 6:1976, 2018.

[108] Q. Salman et al., “Vehicular Sensor Networks: Applications, Advances and Challenges,” Sensors, vol. 20, no. 13, Article 3686, 2020.

[109] Kiberbiztonság a XXI. században, 1. kiadás, Budapest: Akadémiai Kiadó, 2023.

[110] Horváth, Zsolt: TISAX, az autóipar új információbiztonsági követelményrendszere. Magyar Minőség, június (2020). URL: https://infobiz.hu/images/Publikaciok/Magyar_Minsg_2020_06_cikk_HZs_TISAX.pdf. (Letöltve: 2024.11.17.)

[111] Dominique Machuletz, Rainer Böhme: Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR. Proceedings on Privacy Enhancing Technologies, 2020(2) (2020), pp. 481–498. DOI: 10.2478/popets-2020-0037.

[112] Laura A. Stoica, Radu A. C. Savu: Risks and Exploits Exposed by GDPR. Eurasian Journal of Social Sciences, 9(1) (2021), pp. 1–8. DOI: 10.15604/ejss.2021.09.01.001.

[113] Alexander Gladis, Nils J. Hartwich, Oliver Salge: Weaponizing the GDPR: How Flawed Implementations Turn the Gold Standard for Privacy Laws into Fool's Gold. In: Proceedings of the 43rd International Conference on Information Systems (ICIS 2022), Koppenhága, 2022. URL: https://aisel.aisnet.org/icis2022/proceedings/Privacy/3/. (Letöltve: 2024.11.17.)

[114] F. Ahmed, S. Sen, and R. Khan, “Cybersecurity Challenges in Automotive Industry: A Survey,” Sensors, vol. 22, no. 6, 2022.

[115] INCIBE-CERT, “Keys for Implementing New Vehicle Cybersecurity Regulations: R155 and R156,” 2023.

[116] G. L. Beretta, “Cybersecurity risk assessment in automotive industry,” CNR ITIA, 2023.

[117] M. Khodadadi et al., “A Comparative Analysis of UNECE WP.29 R155 and ISO/SAE 21434,” ResearchGate, 2022.

[118] Trustonic, “Compliance with UNECE R155 and R156: What OEMs Need to Know,” Whitepaper, 2023.

[119] M. Heidl, S. Pillokat, and F. Kargl, “Cybersecurity Management System Evaluation Based on WP.29 R155,” in Lecture Notes in Computer Science, vol. 14333, 2023.

[120] European Commission, "Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020," COM(2022) 454 final.

[121] European Union Agency for Cybersecurity (ENISA), "Cybersecurity requirements for connected devices," 2023.

[122] UNECE, "UN Regulation No. 155 on Cybersecurity and Cybersecurity Management System," 2021.

[123] European Commission, "Cyber Resilience Act - Questions and Answers," 2023.

[124] F. Weishäupl et al., “Cybersecurity in automotive supply chains: a layered responsibility,” Journal of Cybersecurity, vol. 8, no. 1, 2022.

[125] J. Hiller and R. Bélanger, “Data protection by design and the GDPR: A critical perspective,” Computer Law & Security Review, vol. 38, 2020.

[126] M. Abouelnaga and C. Jakobs, “Security Risk Analysis Methodologies for Automotive Systems,” arXiv preprint arXiv:2307.02261, 2023.

[127] T. Holz et al., “Systematization of Cybersecurity Requirements for Vehicles,” IEEE Security & Privacy, vol. 19, no. 4, pp. 50–57, 2021.

[128] European Journal of Risk Regulation, "Understanding the Regulatory Approach of the Cyber Resilience Act: Protection of Fundamental Rights in Disguise," Cambridge University Press, 2024.

[129] Computers & Security, "Cybersecurity regulation and compliance challenges in Europe," ScienceDirect, 2024.

[130] Wikipedia, "Cyber Resilience Act," 2024. [CRAOnline

[131] Lawfare, "The Cyber Resilience Act: An Accidental European Alien Torts Statute," 2024.

[132] Hogan Lovells, "The EU Cyber Resilience Act: Implications for Companies," 2024.

[133] elbilstatistikk.no, “Total cars registered,” Aug. 2025. [Online. Available: https://elbilstatistikk.no/

[134] “Norway celebrates another record year for electric vehicles,” elbil.no, Jan. 8, 2025. [Online. Available: https://elbil.no/fossil-fuel-cars-out-of-the-top-ten-list/

[135] J. Wehrman, “EVs At 23.5% Share In France — Plugins Dip As HEVs Surge,” CleanTechnica, Nov. 2, 2024. [Online. Available: https://cleantechnica.com/2024/11/02/evs-at-23-5-share-in-france-plugins-dip-as-hevs-surge/

[136] “Automotive OEM Telematics Research Report 2024–2030: Cars Sold in 2023 were Equipped with Embedded Telematics System,” Research and Markets via Globe Newswire, 01-Oct-2024. [Online. Available: https://rss.globenewswire.com/de/news-release/2024/10/01/2955832/28124/en/Automotive-OEM-Telematics-Research-Report-2024-2030-3-4-Cars-Sold-in-2023-were-Equipped-with-Embedded-Telematics-System-Apple-CarPlay-and-Android-Auto-Driving-Uptake-of-Smartphone-.html

[137] “Automakers are sharing consumers’ driving behavior with insurance companies,” Alpha Leaders, 2022. [Online. Available: https://alphaleaders.co.uk/automakers-are-sharing-consumers-driving-behavior-with-insurance-companies/

[138] “Automakers May Be Sharing Your Driving Data With Insurance Brokers,” InsideEVs.com, 2024. [Online. Available: https://insideevs.com/news/712079/automakers-insurance-data-brokers-criticalmaterials/

[139] Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. International journal of medical education, 2, 53–55.

[140] Guttman, L. (1945). A basis for analyzing test-retest reliability. Psychometrika, 10(4), 255–282.

[141] Mahalanobis, P. C. (1936). On the generalised distance in statistics. Proceedings of the National Institute of Sciences of India, 2(1), 49–55.

[142] European Data Protection Supervisor, "TechDispatch #3: Connected Cars," 2020. [NKOnline

[143] A. Khan et al., "Data Privacy and Security in Autonomous Connected Vehicles in Smart City Environment," Drones, vol. 8, no. 9, 2023.

[144] S. Brown et al., "Evaluating Consumer Understanding and Awareness of Connected and Autonomous Vehicle Data Privacy," in Responsible Design, Implementation and Use, Springer, 2023.

[145] R. Harrison et al., "Privacy preferences in automotive data collection," Technology in Society, vol. 76, 2024.

[146] Smith, J., Brown, L., & Garcia, P. (2022). Security Threats in Connected Vehicles. IEEE Access, 10, 23456–23468.

[147] Müller, K., Zhang, Y., & Patel, S. (2023). Data Leakage via In-Vehicle Communication: Risks and Prevention. Computers & Security, 120, 102834.

[148] Shin, D., & Park, Y. (2021). Understanding the Attitudes of Consumers Toward Smart Car Data Privacy: An Empirical Study. Telematics and Informatics, 63, 101651.

[149] Ellerby, Zack; McCulloch, Josie; Wilson, Melanie; Wagner, Christian: Exploring How Component Factors and Their Uncertainty Affect Judgements of Risk in Cyber-Security. Critical Information Infrastructures Security. Lecture Notes in Computer Science, 11777 (2020), pp. 15–26.

[150] Ji, Zuzhen; Yang, Shuang-Hua; Cao, Yi; Wang, Yuchen; Zhou, Chenchen; Yue, Liang; Zhang, Yinqiao: Harmonizing safety and security risk analysis and prevention in cyber-physical systems. Process Safety and Environmental Protection, 148 (2021), pp. 1–10.

[151] M. Wolf, A. Weimerskirch, C. Paar, "Security in Automotive Bus Systems," Proc. IEEE, vol. 95, no. 2, pp. 387-399, 2007.

[152] P. Kleberger, T. Olovsson, E. Jonsson, "Security Aspects of the In-Vehicle Network in the Connected Car," in Intelligent Vehicles Symposium, 2011.

[153] P. Papadimitratos et al., "Secure Vehicular Communication Systems: Design and Architecture," IEEE Commun. Mag., vol. 46, no. 11, 2008.

[154] KPMG, "Connected and Autonomous Vehicles: The UK Economic Opportunity," White Paper, 2019.

[155] T. Hoppe, S. Kiltz, J. Dittmann, "Security Threats to Automotive CAN Networks—Practical Examples and Selected Short-Term Countermeasures," Reliab. Eng. Syst. Saf., vol. 96, no. 1, pp. 11-25, 2011.

[156] J. Petit, S. E. Shladover, "Potential Cyberattacks on Automated Vehicles," IEEE Trans. Intell. Transp. Syst., vol. 16, no. 2, 2015.

[157] D. Klinedinst, K. Park, "Hacking Connected Cars: Tactics, Techniques, and Procedures," Carnegie Mellon CERT Report, 2017.

[158] S. Checkoway et al., "Comprehensive Experimental Analyses of Automotive Attack Surfaces," in USENIX Security Symposium, 2011.

[159] ENISA, "Good Practices for Security of Smart Cars," European Union Agency for Cybersecurity, 2019.

[160] J. C. Bazydlo et al., "Connected Vehicles and Privacy: A Policy Perspective," Telematics and Informatics, vol. 65, 2022.

[161] A. Greenberg, "Hackers Remotely Kill a Jeep on the Highway—With Me in It," Wired, 2015.

[162] H. Boyes, "Security, Privacy, and Connected Vehicles," IET Intelligent Transport Systems, vol. 11, no. 3, pp. 164-170, 2017.

[163] Reuters, "Tesla workers shared sensitive images recorded by customer cars," Reuters Investigates, 2023.

[164] G. Loukas, Cyber-Physical Attacks: A Growing Invisible Threat, Elsevier, 2015.

[165] M. S. Fareed, M. Qureshi, "Security Challenges in Automotive Embedded Networks: A Survey," IEEE Access, vol. 8, pp. 212004-212029, 2020.

[166] H. Debar, E. Filiol, "Telematics and Privacy: Usage-Based Insurance and Data Protection," in Vehicular Communications and Networks, Wiley, 2022.

[167] T. Neudecker et al., "Privacy Risks in Connected Car Data Sharing," IEEE Security & Privacy, vol. 19, no. 2, pp. 31-39, 2021.

[168] G. N. Ericsson, "Cyber Security and Power System Communication—Essential Parts of a Smart Grid Infrastructure," IEEE Trans. Power Del., vol. 25, no. 3, pp. 1501-1507, 2010.

[169] T. Holz et al., "Internet of Vehicles: Security and Privacy Issues," in IEEE International Symposium on Circuits and Systems (ISCAS), 2017.

[170] ENISA, "Cybersecurity Challenges in the Upstream Oil and Gas Sector," 2019.

[171] C. Miller, C. Valasek, "Remote Exploitation of an Unaltered Passenger Vehicle," Black Hat USA, 2015.

[172] E. Ronen, A. Shamir, "Extended Functionality Attacks on IoT Devices: The Case of Smart Lights," in IEEE European Symposium on Security and Privacy, 2017.

[173] N. Paladi, "Security Analysis of OTA Updates in the Automotive Industry," Springer Automotive Series, 2019.

[174] A. Greenberg, "Automotive Security: IP Protocols in Modern Vehicles," Wired, 2017.

[175] S. T. Ali, A. A. Ghorbani, "On the Use of IoT Protocols in the Automotive Sector," IoT Security Review, vol. 4, no. 2, 2021.

[176] S. Yin, "The Application of OSI Model in Automotive Communication Systems," IEEE Vehicular Technology Magazine, vol. 16, no. 2, pp. 89-94, 2021.

[177] R. Bosch, Automotive Handbook, 10th ed., Wiley, 2023.

[178] P. H. Chavan et al., "Automotive Cybersecurity: A Review of Protocols, Threats, and Testbeds," IEEE Access, vol. 10, pp. 78469-78498, 2022.

[179] G. Velinov, F. Turuk, "Security Analysis of MQTT and CoAP Protocols for IoT-based Smart Vehicles," IEEE Access, vol. 10, 2022.

[180] B. Groza et al., "Security of the Internet of Vehicles: Communication Protocols, Attacks, and Countermeasures," IEEE Communications Surveys & Tutorials, vol. 24, no. 1, pp. 175-200, 2022.

[181] P. Kietzmann et al., "A Security Analysis of MQTT Protocol in Automotive IoT," in IEEE IoT World Forum, 2021.

[182] S. Mallouhi et al., "Cyber Attack Modeling Analysis for SCADA Systems," Proc. International Conference on Critical Infrastructure Protection, 2011.

[183] S. Bhunia, M. Tehranipoor, Hardware Security: A Hands-on Learning Approach, Elsevier, 2019.

[184] O. Hohlfeld, A. Feldmann, "Internet of Things—Communication Protocols and Security Issues," ACM Computing Surveys, vol. 54, no. 1, 2021.

[185] AUTOSAR, "SecOC—Secure Onboard Communication," AUTOSAR Release 4.7, 2021.

[186] J. B. Kenney, "Dedicated Short-Range Communications (DSRC) Standards in the United States," Proc. IEEE, vol. 99, no. 7, 2011.

[187] M. Khari et al., "Critical Review of Security Threats in the Internet of Vehicles," IEEE Access, vol. 8, 2020.

[188] J. Kim et al., "Analysis of Security Vulnerabilities in the CoAP Protocol," Sensors, vol. 21, no. 13, 2021.

[189] R. Singh et al., "A Study of MQTT Protocol in Connected Vehicle Scenarios," in IEEE International Conference on IoT, 2019.

[190] S. Ghafir et al., "Security Threats to the MQTT Protocol in Connected Cars," Journal of Cyber Security Technology, vol. 7, no. 3, 2023.

[191] J. Kim et al., "Security Analysis of CoAP Protocol for IoT-based Vehicles," Sensors, vol. 19, no. 6, 2019.

[192] D. Puschmann et al., "Security Analysis of CoAP Communication in Vehicle Networks," IEEE Vehicular Technology Conf., 2022.

[193] R. Fielding, "Architectural Styles and the Design of Network-based Software Architectures," PhD Dissertation, UC Irvine, 2000.

[194] S. H. Lee and H. Jeong, "HTTPS and API Security in Automotive Environments," IEEE Access, vol. 10, pp. 53521-53536, 2022. doi: 10.1109/ACCESS.2022.3176956

[195] S. Mazloom, M. A. Azgomi, and R. Ebrahimi Atani, "Security Analysis of TLS Implementations in Automotive Systems," in 2021 10th International Conference on Computer and Knowledge Engineering (ICCKE), 2021, pp. 53-58. doi: 10.1109/ICCKE52421.2021.9613642

[196] R. Hussain, S. A. Idrees, and S. Kim, “Autonomous vehicles and connected cars—current status and future perspectives,” Elsevier Vehicular Communications, vol. 29, p. 100418, 2021.

[197] G. Preuveneers, A. Ilie-Zudor, “The intelligent industry of the future: A survey on emerging technologies, applications and open research topics,” Computers in Industry, vol. 123, p. 103334, 2020.

[198] S. Raza, L. Wallgren, and T. Voigt, “Security Considerations for the RESTful Web Services with CoAP,” Proc. IEEE Int. Conf. on Communications (ICC), 2013.

[199] J. Soldatos, “How the MQTT Protocol Works and Why It Matters for IoT,” IEEE Internet of Things Magazine, vol. 3, no. 4, pp. 43–47, 2020.

[200] M. S. Abualhassan et al., “Security Analysis of the MQTT Protocol in the Internet of Things (IoT),” Sensors, vol. 23, no. 2, 2023.

[201] S. Kim, J. Kim, J. Jang, “Analysis of Automotive OTA Communication Protocols for Secure Software Updates,” IEEE Access, vol. 9, pp. 167233–167249, 2021.

[202] L. Apvrille, “Cybersecurity Challenges in the Automotive Domain,” IEEE Design & Test, vol. 38, no. 1, pp. 7–17, 2021.

[203] I. Ghafir, F. Prenafeta-Boldú, M. Hammoudeh, “Security of MQTT Protocol in Smart Connected Vehicles: A Review,” IEEE Access, vol. 10, pp. 11719–11732, 2022.

[204] K. Hartke, “Observing Resources in CoAP,” IETF RFC 7641, 2015.

[205] R. C. A. Alves et al., “A Survey on CoAP Protocol: Security, Attacks, and Research Trends,” Journal of Network and Computer Applications, vol. 207, p. 103530, 2022.

[206] R. Droms et al., “Security in Embedded and Automotive Networks,” IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 2, pp. 611–624, 2021.

[207] R. Ahmad et al., “A Comprehensive Analysis of TLS/DTLS for the Internet of Things,” IEEE Access, vol. 7, pp. 135788–135804, 2019.

[208] M. B. Santos et al., “IoT Security Attacks and Countermeasures in Automotive Environments: A Review,” IEEE Access, vol. 10, pp. 3883–3902, 2022.

[209] A. Velinov, B. Rajšl, M. Zajc, “Over-the-Air Communication Security in Connected Vehicles,” IEEE Access, vol. 8, pp. 121423–121436, 2020.

[210] J. P. Vilela et al., “Covert Channels in Security Protocols: A Survey,” IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1098–1136, 2020.

[211] I. Ghafir, R. Islam, “Application-Layer Attacks on IoT Protocols: A Survey,” IEEE Access, vol. 10, pp. 3427–3452, 2022.

[212]H. Hegyi, "A személygépjárművek információbiztonsága az információbiztonsági szakértők szemszögéből," Biztonságtudományi Szemle, vol. 5, no. 2, pp. 47–58, 2023.

[213] Caltrider, J.; Rykov, M.; MacDonald, Z.: What Data Does My Car Collect About Me and Where Does It Go? Mozilla Foundation, 2023. URL: https://foundation.mozilla.org/en/privacynotincluded/articles/what-data-does-my-car-collect-about-me-and-where-does-it-go/ (Letöltve: 2024.11.17.)

[214] Bendix- Service data for ABS, URL:https://n0c357rmy1njbuit2friqwu.blob.core.windows.net/documents/U3eJunINI0EBhB_SD-13-4746_US_000.pdf

[215] Autorepair, Decoding Vehicle Diagnostics: What Your Car Is Trying to Tell You URL: https://allaroundautorepair.com/understanding-traction-control-and-abs-systems-history-functionality-and-failure-implications

[216] Bosch - Electronic Stability Program, URL:https://www.bosch-mobility.com/en/solutions/driving-safety/electronic-stability-program/

[217] Hutchins, E. M., Cloppert, M. J., és Amin, R. M., "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Lockheed Martin Corporation, 2011.

[218] KDnuggets: How to Convert a Picture into Numbers. URL: https://www.kdnuggets.com/2020/01/convert-picture-numbers.html (Letöltve: 2024.11.17.)

[219] Fridrich, J.; Goljan, M.; Soukal, D.: Perturbed quantization steganography with wet paper codes. MM&Sec '04: Proceedings of the 2004 workshop on Multimedia and security, Sep. 2004, pp. 4–15. DOI: 10.1145/1022431.1022435.

[220] Almohammad, A.; Ghinea, G.; Hierons, R. M.: JPEG Steganography: A Performance Evaluation of Quantization Tables. 2009 International Conference on Advanced Information Networking and Applications, Bradford, UK, 2009, pp. 471–478. DOI: 10.1109/AINA.2009.67.

[221] Djebbar, F.; Ayad, B.; Meraim, K. Abed; Hamam, H.: Comparative study of digital audio steganography techniques. EURASIP Journal on Audio, Speech, and Music Processing, vol. 2012, no. 25 (2012).

[222] Iwakami, N.; Moriya, T.; Miki, S.: High-quality audio-coding at less than 64 kbit/s by using transform-domain weighted interleave vector quantization (TwinVQ). 1995 International Conference on Acoustics, Speech, and Signal Processing, Detroit, MI, USA, 1995, pp. 3095–3098. DOI: 10.1109/ICASSP.1995.479500.

[223] Tsung-Han, T.; Yen, C.-C.: A high quality re-quantization/quantization method for MP3 and MPEG-4 AAC audio coding. 2002 IEEE International Symposium on Circuits and Systems (ISCAS), Phoenix-Scottsdale, AZ, USA, 2002, pp. III–III. DOI: 10.1109/ISCAS.2002.1010358.

[224]C. Jemine, “Automatic multispeaker voice cloning,” M.S. thesis, Univ. of Liège, Liège, Belgium, 2019. URL: https://matheo.uliege.be/handle/2268.2/6801 [Online

[225] The Intercept, “American phone-tracking firm demoed surveillance powers by spying on CIA and NSA”

[226] M. Raciti & G. Bella, “Up-to-date Threat Modelling for Soft Privacy on Smart Cars”, arXiv, 2023.

[227] AP News, “Biden orders US investigation of national security risks posed by Chinese-made ‘smart cars’”, 2023.

[228] Electropages, “Security Risks of Smart Cars”, 2024.

[229] J. Lewis, “Connected Cars and Spying”, CSIS, 2024.

[230] The Guardian, “Are electric cars vulnerable to cyber spies…”, 2025.

[231]F. Swiderski and W. Snyder, Threat Modeling. Redmond, WA: Microsoft Press, 2004.

[232] R. J. Creemers, "China’s emerging data protection framework," Journal of Cybersecurity, vol. 8, no. 1, tyac011, 2022. [Online. Available: https://www.researchgate.net/publication/362915856_China%27s_emerging_data_protection_framework

[233] Law.asia, "Data compliance according to China’s automotive industry," Aug. 13, 2024. [Online. Available: https://law.asia/china-automotive-industry-data-compliance/

[234] "Personal Information Protection Law of the People's Republic of China," Wikipedia. [Online. Available: https://en.wikipedia.org/wiki/Personal_Information_Protection_Law_of_the_People%27s_Republic_of_China

[235] "Data Security Law of the People's Republic of China," Wikipedia. [Online. Available: https://en.wikipedia.org/wiki/Data_Security_Law_of_the_People%27s_Republic_of_China

[236] "Cybersecurity Law of the People's Republic of China," Wikipedia. [Online. Available: https://en.wikipedia.org/wiki/Cybersecurity_Law_of_the_People%27s_Republic_of_China

[237] National Highway Traffic Safety Administration, "Cybersecurity Best Practices for the Safety of Modern Vehicles," DOT HS 812 333, 2021. [Online. Available: https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/812333_cybersecurityformodernvehicles.pdf

[238] National Institute of Standards and Technology, "Security and Privacy Controls for Information Systems and Organizations," NIST SP 800-53 Rev. 5, 2020. [Online. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

[239] JASPAR, "Automotive Cybersecurity Guidelines," JASPAR Association, 2023. [Online. Available: https://www.jaspar.jp/en/activities/cybersecurity/

[240] United Nations Economic Commission for Europe, "UNECE Regulation No. 155 - Cyber security and cyber security management system," 2021. [Online. Available: https://unece.org/transport/vehicle-regulations/wp29/standards/cybersecurity

[241] European Parliament and Council, "Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2)," Dec. 2022. [Online. Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[242] European Union Agency for Cybersecurity (ENISA), "Good practices for security of Smart Cars," 2021. [Online. Available: https://www.enisa.europa.eu/publications/good-practices-for-security-of-smart-cars

[243] European Commission, "Cyber Resilience Act," 2022. [Online. Available: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

[244] S. Gürses, R. van Hoboken, "Privacy after the Agile Turn: Governance, Design, and the Limits of Privacy by Design," Fordham Law Review, vol. 88, no. 2, pp. 437–468, 2019.

[245] P. M. Schwartz, "Global Data Privacy: The EU Way," NYU Law Review, vol. 94, pp. 771–818, 2019.

[246] R. Leenes, R. van Brakel, S. Gutwirth, P. De Hert (eds.), "Data Protection and Privacy: (In)visibilities and Infrastructures," Springer, 2017.

[247] Y. Wang, Y. Wang, H. Qin, and J. Wang, “A Systematic Risk Assessment Framework of Automotive Cybersecurity,” Automotive Innovation, vol. 4, pp. 253–261, 2021. [Online. Available: https://link.springer.com/article/10.1007/s42154-021-00140-6

[248] F. Luo, Y. Jiang, J. Wang, Z. Li, and X. Zhang, “A Framework for Cybersecurity Requirements Management in the Automotive Domain,” Sensors, vol. 23, no. 10, 4979, 2023. [Online. Available: https://www.mdpi.com/1424-8220/23/10/4979

[249] ENISA, "Cybersecurity for Connected and Automated Mobility," European Union Agency for Cybersecurity, 2021. [Online. Available: https://www.enisa.europa.eu/publications/cybersecurity-for-connected-and-automated-mobility

[250] S. Gürses, R. van Hoboken, "Privacy after the Agile Turn: Governance, Design, and the Limits of Privacy by Design," Fordham Law Review, vol. 88, no. 2, pp. 437–468, 2019. [Online. Available: https://ir.lawnet.fordham.edu/flr/vol88/iss2/3/

[251] P. M. Schwartz, "Global Data Privacy: The EU Way," NYU Law Review, vol. 94, pp. 771–818, 2019. [Online. Available: https://www.nyulawreview.org/issues/volume-94-number-4/global-data-privacy-the-eu-way/

[252] R. Leenes, R. van Brakel, S. Gutwirth, P. De Hert (eds.), "Data Protection and Privacy: (In)visibilities and Infrastructures," Springer, 2017. [Online. Available: https://link.springer.com/book/10.1007/978-3-319-50796-9

[253] European Commission, "Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act)," 2022. [Online. Available: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-proposal-and-factsheets

[254] Y. Wang, Y. Wang, H. Qin, and J. Wang, “A Systematic Risk Assessment Framework of Automotive Cybersecurity,” Automotive Innovation, vol. 4, pp. 253–261, 2021. [Online. Available: https://link.springer.com/article/10.1007/s42154-021-00140-6

[255] F. Luo, Y. Jiang, J. Wang, Z. Li, and X. Zhang, “A Framework for Cybersecurity Requirements Management in the Automotive Domain,” Sensors, vol. 23, no. 10, 4979, 2023. [Online. Available: https://www.mdpi.com/1424-8220/23/10/4979

[256]N. Shiwakoti, P. Stasinopoulos, Y. Chen, and M. Warren, “Cybersecurity framework for connected and automated vehicles: A modelling perspective,” Transport Policy, vol. 162, pp. 47–64, 2025. [Online

[257] A. Alfardus and D. B. Rawat, "Machine Learning-Based Anomaly Detection for Securing In-Vehicle Networks," Electronics, vol. 13, no. 10, 1962, 2024. [Online. Available: https://www.mdpi.com/2079-9292/13/10/1962

[258] A. Gupta, S. Tiwari, R. Tripathi, and P. K. Singh, "Detecting Cyber Attacks In-Vehicle Diagnostics Using an Intelligent Multistage Framework," Sensors, vol. 23, no. 18, 7941, 2023. [Online. Available: https://www.mdpi.com/1424-8220/23/18/7941

[259] A. Aloqaily, M. Abdallah, T. R. Sheltami, and I. A. Al Ridhawi, "Supervised Machine Learning for Real-Time Intrusion Attack Detection in Connected and Autonomous Vehicles: A Security Paradigm Shift," Informatics, vol. 12, no. 1, 4, 2025. [Online. Available: https://www.mdpi.com/2227-9709/12/1/4]

8 Publikációk

[HH1] H. Hegyi, "Elektromos járművek töltőinfrastruktúrája: Kiberbiztonsági fenyegetések és geopolitikai összefüggések," in VI. Eurázsia hajnala konferencia Absztraktfüzet, Budapest, Neumann János Egyetem, Eurázsia Központ, 2024, p. 20.

[HH2] H. Hegyi, "A Kelet és a Kód: Kína elektromos autóinak európai terjeszkedése az informatikai biztonság tekintetében," in Absztraktfüzet - Eurázsia Hajnala, Budapest, Neumann János Egyetem, Eurázsia Központ, 2023, p. 16.

[HH3] H. Hegyi, "A kínai elektromos személygépjárművek elterjedésének információbiztonsági kihívásai az Európai Unióban," Eurázsia Szemle, vol. 3, no. 3,2023, p. 30.

[HH4] H. Hegyi, "A személygépjárművek információbiztonsága az információbiztonsági szakértők szemszögéből," Biztonságtudományi Szemle, vol. 5, no. 2, 2023. p. 47.

[HH5] H. Hegyi, L. Erdődi, "Connected and Exposed: Cybersecurity Risks, Regulatory Gaps, and Public Perception in Internet-Connected Vehicles," arXiv preprint arXiv:submit/6685891 [cs.CR], Aug. 2025.

[HH6] H. Hegyi, "A Qualitative Study Investigating Data Security Measures in the European Union," Academic and Applied Research in Military and Public Management Science, vol. 23, no. 2, 2024. p. 63

[HH7] H. Hegyi and L. Erdődi, "Személygépjárművek adatforgalmának megfigyelési célú felhasználási lehetőségei," Biztonságtudományi Szemle, vol. 5, no. 1, 2023. p. 53.

[HH8] H. Hegyi, "Modernizáció és iparbiztonság a COVID-19-járvány után Magyarországon," in Digitális Biztonságpolitika a Kibertérben, T. Babos, Ed. Gödöllő: Magyar Agrár- és Élettudományi Egyetem, 2021, p. 101.

[HH9] H. Hegyi and L. Erdődi, "Modern Passenger Vehicles as Cyber Threat Source: Analyses of Surveillance Options through Smart Vehicles," Acta Polytechnica Hungarica, vol. 22, no. 2, 2025. p. 9.