Milica D. Đekić[*] és **Mester Gyula**[**]

Kiberbiztonság, kiberműveletek vizsgálata

Bevezetés

A kiberműveletek már évtizedekkel ezelőtt kihívást jelentettek az informatikai biztonsági közösség számára.

Gyakorlatilag sokféleképpen lehet incidenst okozni valakinek a kibertérben és ezért fontos, hogy ellenintézkedéseket és vizsgálati eljárásokat dolgozzunk ki és alkalmazzunk.

A kibertérben minden incidenst jelenteni kell, mivel az sokkal súlyosabb bűncselekményekhez vezethet, mint a kiberbűnözés.

A kibertér is olyan vonzó hely, ahol kommunikálni lehet, így világos, hogy miért lehet ilyen szoftvereket és hardvereket használni üzenetküldésre. Ezen túlmenően, ha a kibertérben zajló kampányokról beszélünk, fel kell ismernünk, hogy ezekből a tevékenységekből rengeteg van és ebben az erőfeszítésben csak néhányat fogunk megvitatni.

A modern kiberfenyegetések rendkívül kifinomultak és valódi szakértelemre van szükségük ahhoz, hogy kivizsgálják őket. Ebben a szakaszban elengedhetetlen a nemzetközi együttműködés a hírszerzési ágazatban, mivel a kibertér olyan terület, amely világszerte elérhető.

Továbbá az ilyen környezetek nemzetközileg elismert legjobb gyakorlatot keresnek, mivel a világ egyik részéből származó hackerek bárhol máshol felderíthetők és megbüntethetők.

Más szóval, ha nincs világméretű együttműködés, akkor a világ egyes közösségei hátrányt szenvedhetnek ennek hiányában.

A tanulmány célja, hogy ismertessen néhányat a leggyakoribb kiberműveletek közül és egyértelmű összefüggést állítson fel azok kriminológiai és társadalmi vonatkozásaival.

[*] *Milica D. Đekić, biztonságkutató, Szabadka, Szerbia*

[**] *Dr. Mester Gyula, c. egyetemi tanár, a Magyar Mérnökakadémia rendes tagja, Óbudai Egyetem, Biztonságtudományi Doktori Iskola, Budapest*

Kibertérbeli tevékenységek

Ha a kibertérre, mint ultramodern virtuális környezetre gondolunk, akkor csak egy ilyen környezet egy darabjára gondolunk. Alapvetően a végfelhasználó szemszögéből nézve a kibertér megjeleníthető a kijelzőn, de az igazság ennél sokkal másabb.

Nyilvánvalóan a kibertér magában foglalhatja a virtuális környezetet, mint például az operációs rendszereket, szoftvereket, alkalmazásokat és kütyüket, de gyakorlati értelemben az egész a hardverről és a jelátviteli közegekről szól, amelyek az elektromos jelátvitelt szolgálják [1-5]. Az ilyen jel a vezetékeken keresztül halad és a vezeték nélküli hozzáférési pontokon keresztül terjed tovább, így a hálózat képes kommunikálni a távoli helyekkel.

Más szóval, a digitális világban minden az 1-ekről és a 0-król szól, vagy másképp fogalmazva, az elektronikus feszültségekről. Sok egyezmény szerint a 0 jel 0 V körül van, némi toleranciával felfelé vagy lefelé, míg az 1 jel körülbelül 5 V néhány elfogadott eltéréssel.

A digitális forradalom már a múlt században elkezdődött és még most is jelen van. A kibertérben az a lényeg, hogy nagyon sok információs bitet kezel és nagyon gyorsan dolgozza fel ezeket a csomagokat. Más szóval, a kibertér nem csak a szerverről, az útválasztási útvonalról és a végpontról szól - leginkább a tárolásról, a kommunikációról és a biztonsági mentésről. Mivel így a jelenlegi környezet a kibertér sebezhető a kiberműveletekkel szemben, mint például a fiókkövetés, a kommunikációs streaming, az adathalász támadások, a rosszindulatú programok szabotálása és még sok más. Az a tény, hogy mindannyian megosztjuk a kibertérben, ha bármi történik ott, a felvételek elhagyják ezt a digitális tartományt. Tehát a kibertér nem létezhet az elektromosság nélkül, hasonlóan ahhoz, ahogyan az emberi idegrendszer sem működhet töltés nélkül. A villamosítás a 2. ipari forradalom terméke, és ebben a korszakban felfedeztük hogyan használhatjuk ki a nagyfeszültségű eszközök előnyeit. Másrészt a digitalizáció ideje elhozta számunkra az elektronikát, amely a technológia olyan területe, amely megbirkózik az alacsony feszültségű megoldásokkal.

Ugyanez a helyzet a kibertérrel is. Gyakorlatilag annyira nagyon hasonló az ipar bármelyik ágához. Ezen túlmenően kihívást jelent az ilyen rendszerek fejlesztése és az egész kibertér egyszerűen csak része az olyan kifinomult világnak, amelyben élünk. Az ok,

amiért minden, ami a kibertérben létezik, nyomon követhető, az az, hogy az elektronikus áramkörök elsősorban képesek megjegyezni, hogy mi történt a feszültségükkel és az áramukkal. Bármely beágyazott eszköz, valamint a számítástechnikai egységek mindig is az alaplappal foglalkoznak. Ezek az elemek lefedhetik az ellenállásokat, diódákat, tranzisztorokat, integrált áramköröket, kondenzátorokat és így tovább. Szintén ott vannak a teljes vezetéksorok, amelyek támogathatják az ilyen rendszert, amely a jelcserét végzi [6-11]. A hackereszközök többsége képes utazni a kibertérben és egyszerűen az IP-címmel és néhány port adatával felszerelve bármely online gépet meg tudnak találni. Ezután a kérdés az, hogy milyen szerepet játszik a web egy ilyen esetben. Alapvetően az internet az a világszerte elismert hálózat, amely a TCP/IP protokollokat használja a távoli pontok közötti kommunikáció fenntartására. Ez egyben a kisfeszültségű rendszer a kábelek és a vezetékek segítségével továbbítja az információt egyik pontról a másikra. Továbbá, a jó pont az, ha ezek a kommunikációs közegek emlékeznek arra, hogy mi történt az egész úton keresztül, vagy a számítástechnikai rendszerekre támaszkodnak, amelyek a korrelált eszközök részét képező rengeteg szekvenciált logikai áramkörrel foglalkoznak. Ezenkívül a teljes informatikai infrastruktúra képes az adatcsomagok továbbítására a kommunikációs vonalakon keresztül és teljesen világos, hogy ezek az információ darabok valahol megjegyezve maradnak.

Fiókkövetés

A fiók bármely olyan tartalmi nyilvántartás, amelyet valamilyen számítógépen vagy más eszközön tárolnak. Ez a rekord összefüggésbe hozható az e-mail fiókkal, a közösségi médiaprofillal vagy valamilyen kommunikációs eszközzel, amely az adattárolás kapacitásait használja az ilyen információk viszonylag biztonságos elhelyezése érdekében. Ma lehetséges bármelyik fiók becserkészése, akár aktív, akár időszakos módon. Ez azt jelenti, hogy csak az utasítást kell elküldeni az adott helyre, és megvalósítható lesz egy ilyen mentett tárolás másolatának elkészítése és a kívánt helyre történő átirányítása. A vizsgálat ilyen megállapításokra juthat és ilyen esetben szükséges, hogy minden kritikus fiókot ellenőrizzenek a nyomon követésből. Ez gondos keresésekkel és oly sok esetben ügyes lefoglalásokkal lehetséges, amelyek a fenyegető szereplők megerősítésébe vezetheft-

nek bizonyos közösségek számára. A fiókok nyomon követésének általános módja ma az e-mail profilokon keresztül történik, amelyek a professzionális eszközökön keresztül nyomon követhető a szivárgás valamilyen védelmi szervezetből. Ily módon egyértelmű, hogy egy ilyen szivárgás akkor fordulhat elő, ha van a bennfentes fenyegetés néhány szervezeten belül, amely elsősorban a pénzügyi jövedelem miatt ad engedélyeket az alkalmazások felett. Más szóval, nagy veszélyt jelent a közösségre, mivel ezek a megállapítások olyan terroristák kezébe kerülhetnek, akik megpróbálhatják eltávolítani az embereket és elpusztítani a kritikus infrastruktúrát. Másrészt a fiókkövetés a kémkedés olyan gyakori módszerének tekinthető és ez nem csak az interneten lehetséges, hanem inkább bármilyen távközlési infrastruktúrán keresztül, beleértve a telefonálást is. Elég vonzó a tudat, hogy valamelyik terrorista csoport képes lehallgatni néhány tisztviselő telefonhívásait. A jelenlegi helyzet, amelyet a médiajelentéseken keresztül képviselnek, azt sugallja, hogy a számla-fiók követés riasztó fenyegetést jelent és ezért a világ számos országa kiadta a figyelmeztetéseket arra vonatkozóan, hogy hogyan kell kezelni, valamint, hogy bármilyen megállapítás esetén azonnal jelenteni kell. A hírszerzési keresések időt vesznek igénybe és még a modern rendőrség is megbirkózik a hírszerzés által vezetett ügyekkel, amelyekkel megpróbálják hatékonyabbá és kevésbé költségessé tenni a munkájukat.

Tehát, ha megemlítjük a kibertérben végzett kereséseket, egyértelmű, hogy vannak bizonyos módszerek, amelyek segítségével megtudhatjuk a támadók IP-címét, tartózkodási helyét és egyéb részleteket [12-16].

Kommunikáció csatornázása

Az előző szakaszban a fiókkövetésről beszéltünk, mint a folyamatos biztonságot érintő kihívásról. Másrészt tudnunk kell, hogy az egyes gépeken tárolt adatok nem csak a hackertámadásoknak vannak kitéve. Hasonló a helyzet a kibercsatornákkal is, amelyek lehetőséget adnak arra, hogy az összekapcsolt eszközök teljes hálózatában az információkat egyik pontról a másikra továbbítsák. A kommunikációs csatornán keresztül utazó információ megbirkózik az adatcsomaghoz rendelt két alapvető előtaggal. Ezek a hasznos teher és az útválasztási információ. A hasznos teher a csomagnak azon

része, amely az üzenetet tartalmazza, nyílt szöveges formában van, míg az útválasztási információ szintén nyílt formátumban van és közelebbi információt nyújthat a csomag kézbesítéséről. Ebben az esetben az egyszerű szövegről beszélünk, de a gyakorlatban sok olyan kriptográfiai algoritmust alkalmaznak, amelyek az egyszerű szöveget rejtjelezett szöveggé alakítják át, esetleg többszintű titkosítással. Van még egy elég jó dolog, amit meg kell magyarázni és ez a kommunikációs protokoll. Itt egy rövid szünetet tartunk, meg kell említenünk, hogy bármit használunk a technológiából még az évszázadokkal visszamenőleg is csak azt tudja, amire az ember ráveszi. A gépek nem tudnak gondolkodni, de az élőlények igen. Tehát visszatérünk a régi jó protokollhoz, ami a kicserélt kérdések és válaszok halmaza, csak akkor teszi lehetővé az információátvitelt, ha minden hibátlanul működik. Nos, más szóval ez egyfajta hozzáférés-szabályozás, amely képes eldönteni, hogy a tartalomból mi megy át és mi marad függőben az új lekérdezéshez. Ezután a jó megjegyzés itt az, hogy a kommunikációs csatornát hogyan lehet streamelni. A piacon sok olyan hálózati felügyeleti eszköz van, amely támogathatja a felhasználókat, hogy néhány csomagot megcsapoljanak, valamint a komoly kriptoanalízisre támaszkodva dekódolják az egyszer vett információkat. A kriptoanalízis szakértők kiváló matematikusok és mérnökök egyszerre képesek kezelni minden adatot, amit kapnak.

Adathalász kihívások

Minden kiberbűnöző elsődleges célja a célpont IP-címének megszerzése. Egy ilyen teljesítmény olyannyira kényelmes a hackerek számára, hogy egy oknál fogva biztosíthatja a hozzáférést valaki eszközéhez, sőt az egész hálózathoz. Egyes szakértők szerint az adathalászat és a lándzsás adathalászat összességében az adathalász e-mail küldéséről szól, amely rosszindulatú linket tartalmaz és amelyre kattintva rosszindulatú szoftverek telepíthetők az adott gépre. A gyakorlatban egy ilyen linket nagyon sok csatornán keresztül lehet elküldeni, beleértve az e-mailt, a közösségi médiát, a csevegőeszközöket és még a szöveges üzeneteket is. A helyzet az, hogy minden aktív link, akár rosszindulatú tartalommal rendelkezik, akár nem, potenciálisan veszélyes az áldozatokra nézve, mivel a kiberbűnözőknek, akiknek szükségük van egy ilyen nyomvonalra, hogy sokkal komolyabb műveleteket hajtsanak végre a kibertérben, teljes felvéte-

leket biztosíthatnak. A jó kérdés itt az, hogy hogyan kezdődik az egész adathalász kampány, vagy más szóval, hogy a hackerek hogyan juthatnak a kapcsolatok teljes hálózatának birtokába. Pontosan itt próbálunk foglalkozni azzal, hogy ezek a hackerek okosak és mindenekelőtt nagyon kifinomult készséggel rendelkeznek. Az online környezet rengeteg eszközt kínál arra, hogy kitalálják valakinek az elérhetőségi adatait, de tény, hogy minden adathalász támadás mögött gondosan és részletesen megtervezett és előkészített akciók állnak. A modern média sikeresen végrehajtott adathalász kampányokról számol be, de senki nem mondja ki egyértelműen, hogy ezek a kiberszervezett csoportok hogyan jutottak ilyen kapcsolati gyűrűhöz. Az a tény, hogy a kapcsolatok egy része elérhetőek a weben, mivel a szervezet weboldalán közzéteszik az előtaggal kezdődő elérhetőségi adatokat, az irodát vagy a megkeresést.

Ezután, amint a hackerek birtokába jutnak néhány info@organization.com e-mail címnek, a régi, jó fiókkövetést alkalmazzák és megpróbálják kitalálni az összes elküldött és fogadott üzenetet, amely az adott hivatalos kapcsolathoz érkezik. Tehát sok ügyes kibervédelmi szakember jól ismeri az ilyen trükköt és a valódi e-mail információk helyett a kapcsolatfelvételi űrlapokat kínálják a weboldalaikon [17-22].

A második kihívást jelentő dolog a belső e-mail címekkel vagy más elérhetőségekkel kapcsolatban az, hogy ezek az információk kiszivároghatnak valamelyik szervezetből a bennfentes fenyegetés csatornáin keresztül. A jól kidolgozott rendszer az, hogy néhány vállalkozással a weboldalán közzétett vezetékes telefonon keresztül lépnek kapcsolatba és a közösségi mérnök kedvesen elkéri néhány vezető mobiltelefonját, azt sugallva, hogy ez szükséges néhány üzleti ügylethez. Ez a hacker olyan kedves lesz, hogy a jó modorú ember nem utasíthat vissza egy ilyen szép kérést.

Kiberbiztonság megsértésének problémái

A definíció szerint a kibertámadás bármilyen illegális hozzáférés valamilyen eszközhöz vagy adathoz, amely veszélyeztetheti az egész hálózatot vagy annak egyes tagjait. Más szóval a hackerek behatolhatnak valamely informatikai eszközbe, ott módosíthatnak, ellophatnak néhány adatot vagy törölhetik a teljes tartalmat.

Tehát számos forrás azt sugallja, hogy a kiberbiztonsági jog-

sértés nem arról szól, hogy megtörténhet, hanem arról, hogy hajlandóak vagyunk-e elfogadni egy ilyen eseményt.

Más szóval, mindannyian lehetünk kiberbetörések áldozatai és amire a hackereknek leginkább szükségük van egy ilyen kiberművelet végrehajtásához, az a számítógépek IP-címe.

Látszólag teljesen logikus, hogy az eszköznek online kell lennie, és csak akkor akadályozhatók meg ezek a műveletek, ha úgy döntünk, hogy offline maradunk. Tehát nincs internetkapcsolat - nincs kiberbetörés.

A védelmi közösség bármilyen eszközt leleplezés alá vonhat, akár online, akár offline. Ebben a cikkben a modern kiberbűnözés alvilágáról beszélünk és mivel a definíció olyan szigorú, hogy a betörés csak az interneten lehetséges.

Az iparági óriások többsége kihasználja az ilyen jól fejlett technológia előnyeit, így jutunk el a 4. ipari forradalomhoz, amely elsősorban a webes megoldások előnyeire támaszkodik. Az internet másik nagy előnye, hogy annyira olcsó és bárki biztosíthatja ezt a kiváltságot akár személyes, akár üzleti célokra.

A kibergyakorlattal rendelkező szervezetek tudják, hogyan fedezzenek fel bármilyen, a hálózatukban bekövetkező kiberbiztonsági jogsértést, mivel rengeteg olyan eszköz áll rendelkezésre, amely egyenes választ adhat arra a kérdésre, hogy mikor történt a jogsértés és milyen helyről.

Hogy pontosabbak legyünk, amikor a kibernetikai betörésekről beszélünk, megpróbáljuk elmagyarázni, mi történik, amikor a hacker birtokába kerül egy IP-cím és így ügyesen folytatja a tevékenységét. Más szóval, megpróbáljuk összehasonlítani, hogy mi történik az áldozat képernyőjén és hogyan működik az adott bűncselekményt elkövető kiberbűnöző monitorja.

A gyakorlatban a kiberbűnözők több képernyőt használnak annak érdekében, hogy minél több gépet megfigyelés alá vonjanak. Alapvetően egyszerű, de hatékony eszközökkel boldogulnak a hálózati keresés és megfigyelés során, így valós időben láthatják a képernyőjükön, hogy mit csinál valaki az eszközén [23-29].

Ha csak a kiberbűnözés egyik módjaként a kibernetikai betörésről van szó, a hackerek nem nyúlnak semmihez a szabotázs értelmében, hanem inkább valamiféle kémkedést végeznek, megpróbálva minden érzékeny információt kiszedni, mivel ezeknek a felfedezéseknek megvan az ára a feketepiacon. Tehát ezek a szakem-

berek csak és kizárólag pénzért dolgoznak. Más szóval, a hackerek szeretik az alacsony kockázatú célpontokat, mivel ott minimális az esélye annak, hogy bármilyen következményt, vagy kriminológiai értelemben a büntetést elszenvedjék. A hackerek szó szerint évekig online maradhatnak az informatikai rendszerekkel és senkinek még csak eszébe sem jut megerősíteni, hogy valaki csatlakozott-e az adott hálózathoz. A kiberbiztonsági szakemberek nem részei semmilyen szervezetnek és így a kritikus helyzet a magánszektoron belül van, ahol a kisvállalkozások a nemzet gazdaságának és kereskedelmének hajtóereje és ők is nyitottak bármilyen hacker műveletre.

A sérült adatokat, gépeket és hálózatokat jelenteni kell a bűnüldöző szerveknek, amelyek felajánlhatják a vizsgálatot, amelyet törvényszéki szakértők vezetnek, akik képesek megbecsülni az adott eszköznek és az egész közösségnek okozott teljes kárt.

Az egyetlen dolog, amit a képernyő túloldalán lévő hackernak meg kell tennie ahhoz, hogy ellopja az így bizalmas adatokat, hogy az adatátvitel párbeszédpanelén az OK gombra kattint és minden, amit valaki a hónapok és valószínűleg évek alatt tett, átkerül a bűnöző gépére. Ez nem fikció vagy valaki képzeletének az eredménye.

Ez a kiberbűnözéssel kapcsolatos nyomozás általános forgatókönyve, ezért meg kell próbálnunk csökkenteni az ilyen jellegű hátrányokat, mivel ezek az információk értékesek és nem célszerű, hogy elveszítsük őket.

Összegzés

A modern világ szó szerint túlzsúfolt a korszerű technológiákkal, és bárki bárhol rendelkezhet internetkapcsolattal, mivel olcsó és mindenki számára elérhető. Bemutattunk néhányat a leggyakoribb számítógépes bűncselekmények közül és megpróbáltunk egyfajta tudatosságot is növelni, hogy miért fontos a kiberbiztonság és a kiberműveletek vizsgálata. Az ilyen jellegű bűnözéssel szemben stratégiai megközelítésre van szükségünk. Nagyobb figyelmet kell fordítanunk arra a tényre, hogy a kiberbiztonsági incidensek folyamatosan történnek, de sokuk nem kerül bejelentésre, mivel az emberek nincsenek tisztában azzal, hogy ez mennyire jelentős. Védje meg számítógépét és mobil eszközeit, maximalizálja online biztonságát.

Biztosak vagyunk abban, hogy a világ vezető védelmi és hírszerző szervezetei megbirkóznak a kiberbiztonsági feladatokkal.

Ma már rendelkezünk megfelelő módszerekkel, amelyek segítségével megtudhatjuk a támadók IP-címét, tartózkodási helyét és egyéb részleteket.

Felhasznált irodalom:

[1] Milica D. Đekić, The Internet of Things Cybersecurity Standardization, Tehnika, Vol. 74, Issue 4, pp. 603-607, 2019.

[2] Milica D. Đekić, A Smart Configuration of Computer as a Prevention from Hacking and Cyber Espionage, Tehnika, Vol. 71, Issue 5, pp. 761-764, 2016.

[3] Milica D. Đekić, How to Maintain a Business Continuity Despite Cyber Incidents? Tehnika, Vol. 70, Issue 2, pp. 346-349, 2015.

[4] Milica D. Đekić, The Use of Video Detection as a Function of Traffic Safety, Tehnika, Vol. 66, Issue 3, pp. 471-475, 2011.

[5] Milica D. Đekić, The Internet of Things Security, Tehnika Vol. 72, Issue 2, pp. 309-312, 2017.

[6] Milica D. Đekić, Gyula Mester, Understanding Cyber Technologies in a Physical Way, Tehnika Vol. 76, Issue 5, pp. 690-693, 2021.

[7] Milica D. Đekić, Gyula Mester, COVID-19 as a Scam Challenge, Tehnika, Vol.76, Issue 1, pp. 115-120, 2021.

[8] Gyula Mester, Merenje rezultata naučnog rada. Tehnika-Mašinstvo, Vol. 64, Issue 3, pp. 445-453, 2015.

[9] Aleksandar Rodic, Gyula Mester, Ambientally Aware Bi-Functional Ground-Aerial Robot-Sensor Networked System for Remote Environmental Surveillance and Monitoring Tasks. Proceedings of the 55th ETRAN Conference, Section Robotics, RO2 5, 1-4, 2012.

[10] Aleksandar Rodic, Milos Jovanovic, Svemir Popic, Gyula Mester, Scalable Experimental Platform for Research, Development, and Testing of Networked Robotic Systems in Informationally Structured Environments. Proceedings of the IEEE SSCI 2011, Symposium Series on Computional Intelligence, Workshop on Robotic Intelligence in Informationally Structured Space, DOI:10.1109/RIISS.2011.594577 9, Paris, France, pp. 136-143, 2011.

[11] Gyula Mester, Szilveszter Pletl, Gizella Pajor, Djuro Basic, Adaptive Control of Rigid-Link Flexible-Joint Robots. Proceedings of 3rd International Workshop of Advanced Motion Control, Berkeley, USA, March 20-23, pp. 593-602, 1994.

[12] Attila Nemes, Gyula Mester, Unconstrained Evolutionary and Gradient Descent-Based Tuning of Fuzzy-partitions for UAV Dynamic Modeling. FME Transactions, ISSN:1451-2092, DOI:

10.5937/fmet1701001N, Vol. 45, No. 1, pp. 1-8, 2017.
[13] Attila Albini, Gyula Mester, László B. Iantovics, Unified Aspect Search Algorithm. Interdisciplinary Description of Complex Systems, INDECS, Vol. 17, Issue 1-A, pp. 20-25, 2019.
[14] Gyula Mester, Cloud Robotics Model. Interdisciplinary Description of Complex Systems, Vol. 13, Issue 1, ISSN 1334-4684, DOI: 10.7906/indecs.13.1.1, pp. 1-8, 2015.
[15] Gyula Mester, Distance Learning in Robotics. Proceedings of the Third International Conference on Informatics, Educational Technology and New Media in Education, ISBN 86-83097-51-X, Sombor, Serbia and Montenegro, pp. 239-245, 01-02.04.2006
[16] Josip Kasac, Vladimir Milic, Josip Stepanic, Gyula Mester, A Computational Approach to Parameter Identification of Spatially Distributed Nonlinear Systems with Unknown Initial Conditions. 2014 IEEE Symposium on Robotic Intelligence in Informationally Structured Space (RiiSS), Publisher IEEE, DOI:10.1109/RIISS. 2014.7009170, Orlando, USA, pp. 1-7, 09-12.12.2014.
[17] Gyula Mester, Univerziteti regiona na Šangajskoj rang listi univerziteta u svetu 2012, Zbornik radova XIX Skupa Trendovi razvoja, Kopaonik, Serbia, pp. 1-5, 2013.
[18] Gyula Mester, Metode Naučne Metrike i Rangiranja Naučnih rezultata, Proceedings of the 57th ETRAN Conference, pp. RO3.5.1-3, 2013.
[19] Gyula Mester, The Evaluation of the Impact Factor of the Journal Acta Polytechnica Hungarica, Proceedings of the TREND Conference, pp. 70-73, 2011,
[20] Gyula Mester, Felsőoktatási Világranglisták 2011, Proceedings of the Conference Informatika a felsőoktatásban, Debrecen, Hungary, pp. 269-277, 2011.
[21] Jelena Pisarov, Gyula Mester, Programming the mBot Robot in School, Proceedings of the MechEdu International Conference & Workshop 2019, pp. 45-48, ISBN 978-86-918815-5-9, Subotica Tech, Subotica, Serbia, 12.12.2019.
[22] Gyula Mester, Jelena Pisarov and Dalma Zilahy, Magyarországi robotikai kutatók ranglistája, XXXV. Jubileumi Kandó Konferencia 2019 (JKK2019), ISBN 978-963-449-163-7, Budapest, Hungary, pp. 224-233, 2019.11.14-15.
[23] Gyula Mester, Aleksandar Rodic, Modeling and Navigation of an Autonomous Quad-Rotor Helicopter, E-society Journal: Research and Applications, Vol. 3, No. 1, pp. 45-53, 2012.
[24] Jelena Pisarov, Gyula Mester, The Future of Autonomous Vehicles, FME Transactions, Vol. 49, No. 1, DOI: 10.5937/fme2101029P, pp. 29-35, December 2020.

[25] Janos Simon, Gyula Mester, Critical Overview of the Cloud-Based Internet of Things Pilot Platforms for Smart Cities, Interdisciplinary Description of Complex Systems: INDECS, Vol. 16, Issue 3-A, pp. 397-407, 2018.
[26] Jelena L. Pisarov, Gyula Mester, The Use of Autonomous Vehicles in Transportation, Tehnika, Vol. 76, No. 2, pp. 171-177, DOI:10.5937/tehnika2102171P, 2021.
[27] Gyula Mester, Jelena Pisarov and Endre Németh, Óbudai Egyetem rangsorolása a Webometrics 2019-es ranglistákon, XXXV. Jubileumi Kandó Konferencia 2019 (JKK2019), Budapest, Hungary, pp. 234-240,14-15.11.2019.
[28] Gyula Mester, Academic Ranking of World Universities 2009/2010, The Ipsi BgD, Transactions on Internet Research, Vol. 7, Issue 1, pp. 44-47, 2011.
[29] Mester, G.: New Trends in Scientometrics, Proceedings of the 33rd International Scientific Conference Science in Practice, pp. 22-27, 2015.