Kiss Tibor[1]

Az eBizalom szerepe az illegális szerek online kereskedelmében

Bevezetés

Az információs technológia fejlődésével egyre szélesebb teret nyer a normasértő emberi magatartások különböző mintázatainak megjelenése a kibertérben. E deviáns magatartások egyik markáns metszéspontját adja az illegális szerek online kereskedelme, amely nemcsak a tudományos vizsgálódás, de a szélesebb közvélemény figyelmét is kivívta az utóbbi években. A virtuális feketepiac működésének mozgatórugója egyrészről az óriási adózatlan jövedelem megszerzésének lehetősége és a tiltott vagy illegális forrásból származó árukra és szolgáltatásokra való fizetőképes kereslet, másrészről az illegális szerek (kábítószerek, gyógyszerek) által előidézett szükségletek kielégítésének kényszere (Castells 2005, 117–119.; Kiss–Parti–Prazsák 2019, 72–73.). A vevők és az eladók között az elmúlt egy évtizedben kiformálódott stabil kapcsolati egyensúly az interneten zajló illegális kereskedelmet annak a globális haszonszerzési láncolatnak a meghatározó részévé tette, amely a harmadik generációs informatikai bűnözés legalsó és legfelső szintjét köti össze (Wall 2008, 55–56.). Az így kialakuló illegális adásvételi folyamatokat az erre irányuló tudományos vizsgálatok többsége a társas bűnelkövetési alakzatok online cselekvései közé sorolja, és a szervezett bűnözői körök egyik legnagyobb jövedelemszerzési forrásának tekinti, amelyben a kábítószer és az illegális gyógyszerkereskedelem a levirágzóbb. Ezzel szemben számos olyan tanulmány is napvilágot látott, amelyben több kérdés merült fel a szervezett bűnözés online formációinak entitása körül. Létezhet-e olyan szerveződés, amely alkalmas az illegális kereskedelem működtetésére az internet nehezen elérhető hálózati pontjain, valamint az ilyen csoportoknak vagy hálózatoknak van-e új, eddig nem ismert struktúrája (Broadhurst et al. 2014, 2.)?

[1] Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Kriminológiai Tanszék, tanársegéd; r. őrnagy.

https://doi.org/10.36250/00869_24

A 2000-es évek első évtizedében indított kutatások eredményei szerint napjainkra már több olyan szerveződés is működik az interneten, amely a klasszikus szervezetek jelenlétén kívül elkülöníthető, „önálló" közösségként is értelmezhető. Leukfeldt a Hollandiában lefolytatott kutatások eredményeit szintetizáló tanulmányában például azt állította, hogy *összetételük* szerint alapvetően kétfajta formáció lokalizálható a kibertérben, mégpedig a társadalmakon belüli (helyi) közösségeké, illetve a nemzetközi kapcsolatokban gyökerező (nemzetközi) összetételű csoportoké. Okfejtésében kiemelte, hogy az efféle szerveződések homogén vagy heterogén jellegénél még fontosabb a szervezetek struktúrájának és kapcsolati elrendeződésének megismerése, ugyanis ebben rejlik a klasszikus szervezett bűnözői alakzatoktól való eltérés vagy hasonlóság körvonalazhatósága, a globális hálózat nyújtotta lehetőségek feltérképezhetősége és ezzel együtt a felszámolásukra hivatott szervezetek eredményes működése. Leukfeldt szerint a hálózatokon létrejövő szervezett közösségek működésében kulcsfontosságú szerepe van a találkozási pontoknak (konvergenciapontoknak), amelyek azon felül, hogy a bűnelkövetők kapcsolódási platformjait testesítik meg, központi szerepet töltenek be a közösségi koordinációban és a hálózatok felépítésében, és ezáltal az illegális kereskedelmi platformok működésében.

Ugyanerről szólt a szervezett bűnözés kibertérben működő csoportjainak tipológiáját felállító Kim-Kwang Raymond Choo vizsgálata, amelyben világszerte, de leginkább a kínai szervezett bűnözői csoportok interneten kialakított kapcsolatrendszerét térképezte fel. A szerzőpáros három szervezett bűnözői közösségi típust különített el egymástól annak figyelembevételével, hogy tevékenységükben milyen szerepet tölt be a kibertér és az IT-technológia, a csoportok tagjai a virtuális környezetben milyen technikai módszereket használnak, továbbá milyen célok elérésére törekednek. A kutatók szerint vannak *hagyományos szervezett bűnözői csoportok,* amelyek a technológiát és az internet hálózatát eszközként veszik igénybe olyan hagyományos bűncselekmények megvalósításában, mint a kábítószer-kereskedelem, a zsarolás, a csalás, az emberkereskedelem, a pénzmosás, illegális szerek és gyógyszerek terjesztése. Ebbe a kategóriába a hagyományos térben régóta működő, világszerte ismert, ugyanakkor kiterjedt kapcsolatrendszerrel rendelkező bűnszervezeteket sorolták, amelyek a globális hálózatot és annak kommunikációs csatornáit jövedelmező piactérként és információszerzési csatornaként használják, miközben hagyományos környezetben működnek. A másik csoportba a *szervezett számítógépes bűnelkövetőket* sorolták, akik – bár a virtuális piactereken vagy platformokon kapcsolatba kerülnek a hagyományos bűnszervezetekkel – azoktól mégis elkülönülnek, ugyanis a működésük és „szakértelmük" kizárólag a kibertérre korlátozódik (vagyis a kibertér inkább az elkövetésük tárgya). Jellemzően kisebb csoportokból állnak, és nem maradnak fenn olyan hosszú

ideig – eltérően a klasszikus bűnszervezetektől (például rosszindulatú támadásokat indító ötfős hackercsoportok). A szervezett számítógépes bűnelkövetők egymással is csak globális hálózatokon működő titkosított platformokon találkoznak, és tevékenységeik mentén tagozódnak (például vírusírók, megtévesztő tartalmakat közvetítő hamis weboldalak készítői, automatizált eszközöket értékesítők, online játékosok). A szerzőpáros végül a harmadik csoportba sorolta az *ideológiai, politikai irányultságú szélsőséges csoportokat támogató bűnszervezeteket.* A szervezett bűnözői körök ezen csoportja kapcsolatban áll a szélsőséges közösségekkel és terrorszervezetekkel, pontosabban szolgáltatásokat nyújt és támogatja azokat olyan tevékenységekkel, mint a pénzmosás, a fegyverek, robbanóanyagok beszerzése, a toborzás, a hacktivista cselekvések vagy épp a kiemelt infrastruktúrák megbénítására irányuló rendszerintegritás elleni bűncselekmények. Az efféle bűnszervezetek az előző két közösség közt állnak, és az internet hálózatát, illetve az IT-eszközöket eszközként használják, ugyanakkor jellemző rájuk a hálózatokon belüli kizárólagos működés is (Choo 2008).

Egy másik tipológia Michael McGuire kriminológus kutatási eredményeihez fűződik, aki az efféle közösségek három típusát vázolta fel. Az *első típus* kizárólag az internet globális hálózatán működik, és kétféle szerveződést foglal magában. Az egyik a rajszerű *(swarms group)* szerveződés, amely inkább a hacktivista és a gyűlöletcsoportokra jellemző, és azon felül, hogy rengeteg résztvevőt gyűjt össze, inkább az ideológiájuk közös, de ehhez képest nem túl strukturáltak. A csomópontszerű *(hubs group)* szerveződés sokkal szervezettebb, strukturáltabb, mint a rajszerű. Céltudatos, komoly számítástechnikai szakértelemmel rendelkező résztvevőkkel működik, és jellemzően illeszthető az adathalász támadásokra, a rendszerintegritás elleni támadásokra létrejött közösségekre (például DoS-, DDoS-támadások, malware-ek terjesztése). A *hubs* formáció tipikus alakzata az internetes kereskedelmi platformoknak is, ahol kisebb-nagyobb bazárokat működtetnek (például Silk Road). A *második típus* a hibridek típusa, ahol a szervezetek online és offline kombinációja működik. Ezen belül is kétféle szerveződés rajzolódik ki, amelyek közül az egyik a klaszterszerű hibrid szerveződés *(clustered hybrid group),* amelyekben egy kisebb közösség az offline és az online tér között mozog (például offline térben megszerzi a bankkártyaadatokat és online térben felhasználja) egy folyamatban azonos célért. Ugyanezen típus második szerveződése a kiterjesztett hibrid szerveződés *(extended hybrid group),* amely hasonló a klaszterszerűhöz, azonban jóval nagyobb létszámban, több csoporttal, sokféle hasonló bűncselekményre specializálódva, de kevésbé centralizáltan tevékenykedik. McGuire szerint a *harmadik típusba* azok a közösségek tartoznak, amelyek az online hálózatot és a technológiát használják offline szervezett tevékenységeik megkönnyítésére. A harmadik típus is két alszerveződésre osztható. Az egyik ezek

közül a hierarchikus *(hierarchies group)* szerveződés, amelyben hagyományos hierarchikus bűnszervezetek terjeszkednek az online térben, és a legsúlyosabb bűncselekményekhez használják az internetet (például zsarolás, csalás, tiltott online szerencsejátékok, rendszerfeltörések, gyermekkorúakról készült pornográf felvételek kereskedelme). A harmadik típus második szerveződése az aggregált szerveződés *(aggregate group),* amelyben a hagyományos bűnszervezetek kizárólag offline cselekményeikhez használják a hálózatot és a technológiát. Ez utóbbinak van a legkevesebb köze a kibertérhez, vagyis kizárólag eszközként használják azt (Broadhurst et al. 2014, 4–7.).

McGuire és Choo tipológiája számos további kutatásnak adott kiindulási pontot, főként azokban a csoportokban, amelyek a két tipológiában a kibertérre korlátozódtak. Az újabb tudományos munkákban már kizárólag a globális hálózatokon tevékenykedő közösségek szereplőinek viszonyrendszerét járták körül, és kapcsolati vektoraik vizsgálatai mentén kimondottan a felépítésük (decentralizáltság vagy hierarchizáltság) megismerésére törekedtek. A konvergenciapontokat ezekben a vizsgálatokban már nem a hagyományos bűnszervezetek csomópontjainak egy részeként értelmezték, hanem a kiberközösségek konkrét csomópontjaiként. A kutatók szerint mivel a szervezett bűnözés hálózati működését a kibertérben számos konvergenciapont működése tartja össze – amit McGuire és Choo eredményei is alátámasztottak –, így az ott látható közösségek tagjai *hálózatosan kapcsolódnak egymáshoz, és egyértelműen decentralizáltak.* Ezzel szemben Lu és munkatársai a konvergenciapontokban zajló közösségen belüli interakciók vizsgálatából arra következtettek, hogy ezekben a pontokban még mindig az alá-fölé rendeltségi viszony rajzolódik ki – ahol a bizalom és a hírnév a legfontosabb (Lu et al. 2010, 30–34.). Lu megállapításait később Yip munkatársaival végzett kutatása is megerősítette azzal a kitétellel, hogy a konvergenciapontokban fennálló hierarchia egyáltalán nem olyan tartós, mint a hagyományos szervezetek csomópontjain belül, ugyanis a belépő tagok hamar újabb kapcsolatokat és ezzel újabb fórumokat (konvergenciapontokat) építhetnek, gyengítve a hierarchia legfelső fokán állók központi szerepének állandóságát (Yip–Shadbolt–Webber 2012, 1–6.).

A tanulmányokban levezetett eredményekből következtetésként levonható, hogy a kibertérben tevékenykedő bűnszervezetek struktúrája *hálózatos, decentralizált* felépítésű és a decentralizált struktúrában megtalálható csomópontok szereplői közt működő alá-fölé rendeltségi viszony nagyon képlékeny. Így ez a konstrukció az illegális kereskedelmet működtető helyi és nemzetközi közösségek kialakítására már több mint alkalmas. A kutatási eredmények többségében az elkövetőkre koncentráltak, valamint a kereskedelmi tevékenységeknek színteret adó hálózati helyek létezését és strukturális felépítését határolták körül, de kevésbé fókuszáltak a szervezett közösségek tagjai – mint eladók és a vásárlók –

közötti kapcsolat kohéziójának és egyensúlyának fenntartására hivatott humán faktorokra. Olyan tényezőkre, amelyek függetlenek a szervezett csoportok felépítésétől, főként a vásárlói oldalon fogalmazódnak meg és a kereskedelmi tranzakciók sikerét eredményezik.

A vásárlói bizalom jelentősége

Az internetes hálózatokon zajló interakciókat tanulmányozó kriminológiai tudományterület képviselői az illegális kereskedelemnek teret adó internetes szürkefoltok (konvergenciapontok) működésének gyökerét elsősorban a John Thibaut és Harold Kelley (1959) amerikai pszichológusok által felállított *csereelméletből* eredeztetik. Az elmélet szerint a csoport tagjai folyamatosan javakat vagy szolgáltatásokat cserélnek egymással az optimális haszon elérésére. Viszont a javak áramlásának iránya által meghatározott kapcsolatok fennmaradásának fontos alapfeltétele, hogy a javak cseréjével megvalósuló haszonnak mindkét fél esetében magasabbnak kell lennie, mint a kapcsolat fenntartásának költsége (Csepeli 2014, 91.). Az elméletet felhasználó kiberkutatók meggyőződése szerint az internetes marketekben a csereelmélet tárgya lehet akár pénz, valamely szükséglet kielégítésére irányuló szolgáltatás vagy értékes információ, amely a közösségek fennmaradása mellett az internetes platformokat is folyamatosan revitalizálja (Leukfeldt 2015, 94–97.). Az illegális kereskedelemre irányuló kutatások eredményeinek mindegyikében jól körvonalazható az a következtetés, hogy a hálózati pontokban a kínálati oldalon az értékesítők (a haszonszerzési szükségletek érdekében), a keresleti oldalon a vásárlók (addiktív vagy más szükségleteik kielégítése érdekében) kerülnek egymással kapcsolatba, és a haszon érdekében kölcsönösen lemondanak a morális szabályok betartásáról − vállalva az ezzel járó kockázatokat (Kiss 2019, 106.). Az így kialakuló adásvételi folyamat egyfajta szerződésen alapul, amelyet a vevők és az eladók között megformálódó érzékeny *bizalom* garantál. A legális online webkereskedelemben (például az eBayen) működő bizalom (eTrust) már jól ismert fogalom, amelyet a legális online kereskedelem hátterében az elmúlt 15 évben sokan vizsgáltak. Yi, Ahmad és Dhanapal például hosszan vizsgálta az internetes vásárlók legfontosabb bizalmi tényezőit többféle legális online kereskedelmi folyamatban. Megállapításuk szerint az online kereskedelmi platformokat látogatókat elsősorban az információbiztonsággal és az adatvédelemmel kapcsolatos aggodalmaik befolyásolják a vásárlásról való döntéseikben. Másodsorban az internetszolgáltatók megbízhatósága, a fogyasztók kockázatérzékelése, az intézményi bizalom és a gazdasági ösztönzők határozzák meg a vásárlást elősegítő bizalom kialakulását (Yi–Ahmad–Dhanapal 2009, 154.). Lee és Turban szerint a leg-

fontosabb vásárlói bizalmi kategóriák körébe az internetes kereskedő és az internetes vásárlási közeg megbízhatósága, az internetes vásárlás kontextuális tényezői és egyéb tényezők tartoznak, beleértve az egyéni bizalomra való hajlamot (Lee–Turban 2001, 80.). Al-Dwairi kutatása a biztonsági és adatvédelmi funkciókra összpontosított. Véleménye szerint a weboldal olyan jellemzői, mint a dizájn, a tartalom, a biztonság és az adatvédelem nagymértékben befolyásolják a vásárlók döntését, ezért ezek az e-kereskedelem fontos bizalmi tényezői (Al-Dwairi 2013, 5.). Ilmudeen kereskedelmi bizalomról szóló tanulmányának eredményei szerint az ügyfél döntését egy észlelt kockázati dimenzió befolyásolja, amelyet számos kockázati tényező kombinációja határoz meg. Ilyen tényezők körébe tartozik a teljesítmény-, a fizikai, a pénzügyi, a pszichológiai, a társadalmi, valamint a szállítás- és időkockázat (Ilmudeen 2018, 3–4.).

Vásárlói bizalom az online feketekereskedelemben

A legális online kereskedelem folyamatainak bizalmi tényezőiről szóló fenti tanulmányokból nemcsak az univerzális bizalmi struktúra szintetizálható, hanem olyan egyéni és társadalmi motivációk összessége is, amely a vásárlás sikerének előfeltételei közé tartozik. Az egyéni motivációs tényezők tartalmazzák az egyén anyagi helyzetét, szükségleteit, a bizalom iránti hajlandóságot. A társadalmi motivációs tényezők viszont a vásárolt tárgy vagy szolgáltatás igénybevételének társadalmi elfogadottságát, a jogi szabályozókat és a vásárlók demográfiai diszpozícióit foglalják magukban. A bizalmi faktorok ennél szélesebb körben határozhatók meg, és legalább 6 kategóriába sorolhatók az alábbi struktúra szerint.

(1) Egyéni és közösségi kategória:
- internetes kereskedő vagy weboldal-/webtartalom-szolgáltató megbízhatósága;
- az eladó vagy a weboldal-/webtartalom-szolgáltató elérhetősége;
- az eladó vagy a weboldal-/webtartalom-szolgáltató támogatási szolgáltatása;
- a szükségletek kölcsönös kielégítése és az elégedettség.

(2) Technológia és hálózat kategóriája:
- az internetes hálózatok, az informatikai technológia (hardver és szoftver) és a számítógépes rendszerek megbízhatósága (például az árukhoz és szolgáltatásokhoz való biztonságos hozzáférés garanciája az informatikai technológiával és a hálózattal);
- a weboldal felépítése.

(3) Adatvédelem és magánélet kategóriája:
– a személyes adatok védelme;
– a fizetési adatok védelme.

(4) Fizetési tranzakció kategóriája:
– a fizetési műveletek hozzáférhetősége és egyszerűsége;
– pénznem vagy más fizetési eszköz versenyképes értéke.

(5) Termékek és szolgáltatások kategóriája:
– az áruk és szolgáltatások széles választéka;
– az áruk és szolgáltatások garanciája;
– az áruk és szolgáltatások minősége.

(6) Szállítási szolgáltatások:
– az áruk szállításának garanciája;
– a leszállított áruk integritása.

Abban az esetben, ha a legális online kereskedelemben a motivációk és a bizalom faktorai nem vagy csak elégtelenül funkcionálnak, az üzleti kapcsolat egyensúlytalanná válik, majd összeomlik. Kétségtelenül felmerül a kérdés, hogy milyen tényezők működnek az internetes illegális gyógyszer- és drogkereskedelemben. Néhány európai darkwebkutatásban már megjelent a bizalom hatásfokának vizsgálata, amely csupán a konvergenciapontokban működő bűnelkövetői közösségek tagjai közötti attitűdök explorációját jelentette (lásd: Leukfeldt 2015; Broadhurst et al. 2014), de az eladók és főként a vevők közötti online feketekereskedelmi folyamatokra nem tért ki. Mindezek alapján vajon feltételezhető-e az, hogy a legális és az illegális online kereskedelmet ugyanazok a motivációs és bizalmi tényezők tartják fenn, és teszik racionálissá a vásárló normasértésről hozott döntéseit (a racionális döntés elmélete: Becker 1976; Cornish–Clarke 1986)? A kiberteret kutató kriminológusok egyetlen faktor eltérését már biztosan prognosztizálták, mégpedig a névtelen részvétel és azonosíthatatlan műveletek iránti igényt. Az illegális üzletekben a vevők részéről (és az eladókéról is) az egyik legfontosabb a lebukás kockázatának csökkentése. Abban az esetben, ha a bizalmi faktorok az anonimitás igényén felül megegyeznek a kétféle kereskedelmi folyamatban, és azok száma magas, akkor ugyanaz történik az online feketepiacon, mint a legális internetes kereskedelemben, vagyis a vásárlók száma emelkedik. Ebben az esetben a tiltott szereket értékesítő platformokon a bizalmi tényezők azokat a vásárlókat is illegális és visszatérő vásárlásra ösztönözhetik, akik normál körülmények között ezt nem tennék meg. Továbbá az sem kizárható, hogy a bizalmi faktorok jelen-

léte közvetett módon támogatja azoknak a kábítószereknek és gyógyszereknek a feketepiaci kereskedelmét, amelyek a törvényes kereskedelemben nem elérhetők, vagyis nyilvánvalóvá teszi a tiltott anyagok online kereskedelmének kiegészítő funkcióját a globális szerkereskedelemben.

A bizalom szerepe láthatóan felértékelődött az online feketekereskedelemben, ezért egyre időszerűbb azoknak a kutatásoknak az elindítása, amelyek elsősorban a vásárlók bizalmának feltérképezésére összpontosulnak, valamint azokra a motivációkra, amelyek az egyént és a közösséget alapvetően a tiltott szerek vásárlására ösztönzik. Az efféle vizsgálat arra is rávilágítana, hogy az online feketepiac olyan szürkezónát foglal magában, amelynek szerepe a szükségletek kielégítésén felül hiánypótló, ami már önmagában magyarázó erejű az online illegális kábítószer- és gyógyszerkereskedelem dinamikus működése tekintetében.

Irodalomjegyzék

Al-Dwairi, Radwan M. (2013): E-Commerce Web Sites Trust Factors: An Empirical Approach. *Contemporary Engineering Sciences,* Vol. 6, No. 1. 1–7. DOI: https://doi.org/10.12988/ces.2013.13001

Becker, Gary S. (1976): *The Economic Approach Becker to Human Behavior.* Chicago (US-IL), University of Chicago Press. DOI: https://doi.org/10.7208/chicago/9780226217062.001.0001

Broadhurst, Roderic – Grabosky, Peter – Alazab, Mamoun – Chon, Steve (2014): Organizations and Cybercrime: An Analysis of the Nature of Groups engaged in Cyber Crime. *International Journal of Cyber Criminology,* Vol. 8, No. 1. 1–20.

Castells, Manuel (2005): *A hálózati társadalom kialakulása.* Budapest, Gondolat.

Choo, Kwang-Kim Raymond (2008): Organised Crime Groups in Cyberspace: A Typology. *Trends in Organized Crime,* Vol. 3, No. 11. 270–295. DOI: https://doi.org/10.1007/s12117-008-9038-9

Cornish, Derek B. – Clarke, Ronald V. (1986): *The Reasoning Criminal: Rational Choice Perspectives on Offending.* Berlin, Springer.

Csepeli György (2014): *Szociálpszichológia mindenkinek.* Budapest, Kossuth.

Ilmudeen, Aboobucker (2018): *Consumers' Perceived Security Risks in Online Shopping: A Survey Study in Sri Lanka.* DOI: https://doi.org/10.2139/ssrn.3344634

Kiss Tibor – Parti Katalin – Prazsák Gergő (2019): *Cyberdeviancia.* Budapest, Dialóg Campus.

Kiss Tibor (2018): Cyberbűnözés. In Frigyer László szerk.: *Nemzetközi jellegű szervezett bűnözés nyomozásának kutatása információáramlási szempontból. II.* Budapest, NKE.

Lee, Matthew K. O. – Turban, Efraim (2001): A Trust Model for Consumer Internet Shopping. *International Journal of Electronic Commerce,* Vol. 6, No. 1. 75–91. DOI: https://doi.org/10.1080/10864415.2001.11044227

Leukfeldt, Rutger Eric – Jansen, Jurjen (2015): Cyber Criminal Networks and Money Mules: An Analysis of Low-Tech and High-Tech Fraud Attacks in the Netherlands. *International Journal of Cyber Criminology,* Vol. 9, No. 2. 173–184.

Leukfeldt, Rutger Eric (2015): Organised Cybercrime and Social Opportunity Structures: A Proposal for Future Research Directions. *The European Review of Organised Crime,* Vol. 2, No. 2. 91–103.

Lu, Young – Luo, Robert – Polgar, Michael F. – Cao, Yuanyuan (2010): Social Network Analysis of a Criminal Hacker Community. *Journal of Computer Information Systems,* Vol. 51, No. 2. 31–41.

Wall, David S. (2008): Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime. *International Review of Law, Computers and Technology,* Vol. 22, Nos. 1–2. 45–63. DOI: https://doi.org/10.1080/13600860801924907

Yi, Thaw – Ahmad, Kamil Mahmood – Dhanapal, Durai Dominic (2009): A Study on the Factors That Influence the Consumers' Trust on E-commerce Adoption. *International Journal of Computer Science and Information Security,* Vol. 4, No. 1–2.

Yip, Michael – Shadbolt, Nigel – Webber, Craig (2012): Structural Analysis of Online Criminal Social Networks. *2012 International Conference on Intelligence and Security Informatics,* 60–65. DOI: https://doi.org/10.1109/isi.2012.6284092