# A DOLGOK INTERNETÉNEK (IoT) IRÁNYÍTÁSA

**Lawrence J. Trautman**[*]
**Mohammed T. Hussein**
**[†]Louis Ngamassi[‡]**
**Mason J. Molesky**[**]

**ABSZTRAKT: A** technológiai változások mai növekvő üteme a számítógépek feldolgozási sebességének gyors növekedéséből adódik, ha a feldolgozási kapacitás költségcsökkenésével párosul, és történelmi jelentőségű. Világszerte több milliárd ember mindennapi életét változtatta meg örökre a technológia csupán az elmúlt néhány évben. A költséges adatvédelmi incidensek továbbra is riasztó ütemben zajlanak. A mesterséges intelligencia, a gépi tanulás és az internetre csatlakoztatott több milliárd érzékszervi eszköz hatásának irányításával kapcsolatos emberi kihívás a jelen cikk témája.

Ez a cikk kilenc részből áll. Először is meghatározza a tárgyak internetének (IoT) fogalmát, megjegyzi az internethez csatlakoztatott érzékszervi eszközök robbanásszerű növekedését, példákat hoz a tárgyak internetéhez kapcsolódó eszközökre, és a tárgyak internetének ígéretéről beszél. Másodszor, a cikk tárgyalja a vállalatirányításra vonatkozó jogi követelményeket, amelyek a tárgyak internetének irányításával kapcsolatos kihívás mérlegelésének alapjául szolgálnak. Harmadszor, megvizsgálja a tárgyak internetének lehetséges veszélyeit. Negyedszer a cikk a Mirai botnetet tárgyalja. Ötödször, a cikk a tárgyak internetét fenyegető veszélyvektorok sebezhetőségét vizsgálja válság idején. Hatodszor, a cikk a MUD (Manufactured Usage Description) met- odológiát tárgyalja. Hetedszer a közelmúltbeli szabályozási fejleményekről szól. Végül a cikk megvizsgál néhány ajánlást, és következtetéseket fogalmaz meg. Úgy véljük, hogy ez a cikk hozzájárul a tárgyak internetéhez kapcsolódó rosszindulatú szoftvereknek való széles körű kitettség megértéséhez, és kiegészíti a vállalati kockázatok irányításával kapcsolatos, még kialakulóban lévő, de már kialakulóban lévő szakirodalmat, amely létfontosságú társadalmi jelentőségű téma.

**Hivatkozás**: Lawrence J. Trautman, Mohammed T. Hussein, Louis Ngamassi, & Mason J. Molesky, *A tárgyak internetének (IoT) kormányzása*, JURIMETRICS60 J. 315-51 (2020).

---

[*]Trautman úr a Prairie View A&M Uni- versity üzleti jog és etika docense. A Vállalati Igazgatók Országos Szövetsége (NACD) New York-i és washingtoni/baltimore-i tagozatának korábbi elnöke. A Lawrence.J.Trautman@ gmail.com címen érhető el.

[†]Dr. Hussein a Prairie View A&M University vezetői információs rendszerek (MIS) tanszékének adjunktusa. A mthussein@pvamu.edu címen érhető el.

[‡]Dr. Ngamassi a Prairie View A&M University vezetői információs rendszerek (MIS) docense és a Texas A&M University, College Station veszélycsökkentési és helyreállítási központjának munkatársa. A longamassi@pvamu.edu címen érhető el.

[**]Molesky úr a George Washington Egyetem adjunktusa. A masonmolesky@gmail.com címen érhető el.

A jelen megjegyzések alapját a Seventh Annual Conference on Gov- ernance of Emerging Technologies, Sandra Day O'Connor College of Law, Arizona State Univer- sity, May &22 A kézirat tudományos közleményként való 23,2019.megjelölése a Cornell University-nél arXiv:2004.03765 [cs.CY]. Minden hiba és mulasztás a sajátunk.



Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

> A felgyorsulás korába lépünk. A társadalom alapjául szolgáló modelleket, amelyek nagyrészt a változás lineáris modelljén alapulnak, minden szinten újra kell definiálni. Az exponenciális növekedés robbanásszerű ereje miatt a XXI. század a mai fejlődési ütem mellett 20 000 évnyi fejlődésnek fog megfelelni; a szervezeteknek képesnek kell lenniük arra, hogy egyre gyorsabb ütemben újradefiniálják magukat.
>
> -Ray Kurzweil, a Google műszaki igazgatója[1]

## I. ÁTTEKINTÉS

A technológiai változások mai növekvő üteme a számítógépek feldolgozási sebességének gyors növekedéséből adódik, és a feldolgozási kapacitás költségcsökkenésével együtt történelmi jelentőségű.[2] Giaretta, Dragoni és Massacci így számol be: "Az intelligens otthonok egyre több IoT-eszközzel vannak felszerelve, amelyek egyre több információt rögzítenek az emberek életéről. A gyártók azonban kevés vagy egyáltalán nem fordítottak figyelmet a biztonságra " [3]Ahogy az U.S. National
Institutes of Standards and Technology júliusi, *Core Cybersecurity feature Baseline for Securable IoT Devices* című 2019tervezetében: *A Start- ing Point for IoT Device Manufacturers*:

> A gyártók hihetetlenül sokféle és nagy mennyiségű tárgyak internetét (Internet of Things, IoT) használó eszközt hoznak létre, amelyek legalább egy, a fizikai világgal közvetlen interakcióra képes átalakítót (érzékelőt vagy ak- tuátort) tartalmaznak, legalább egy hálózati interfésszel rendelkeznek (pl. Ethernet, WiFi, Bluetooth, Long-Term Evolution [LTE], ZigBee), és nem hagyományos informatikai eszközök, amelyek esetében a kiberbiztonsági funkciók azonosítása és végrehajtása már jól ismert (pl. okostelefon, laptop). Számos IoT-eszköz olyan berendezések számára biztosít számítási funkciókat, adattárolást és hálózati csatlakoztathatóságot, amelyek korábban nem rendelkeztek ezekkel a funkciókkal. Ezek a funkciók viszont új hatékonyságot és technológiai képességeket tesznek lehetővé a berendezések számára, például távoli hozzáférést biztosítanak a felügyelethez, konfiguráláshoz és hibaelhárításhoz. A tárgyak internete a fizikai világra vonatkozó adatok elemzésére és az eredmények felhasználására is képes, hogy jobban tájékoztassa a döntéshozatalt, megváltoztassa a fizikai környezetet és előre jelezze a jövőbeli eseményeket.[4]

Világszerte több milliárd ember mindennapi életét változtatta meg örökre a technológia az elmúlt néhány évben.[5] A költséges adatvédelmi incidensek továbbra is

---

1. Lawrence J. Trautman, *Bitcoin, virtuális valuták és a törvény és a szabályozás küzdelme a lépéstartásért*, 102 MARQ. L. REV. 447, 470 (2018) (idézi THOMAS L. FRIEDMAN, THANK YOU FOR BEING LATE: AN OPTIMIST'S GUIDE TO THRIVING IN THE AGE OF ACCELERATIONS (1872016)).

2. *Id.*

3. Alberto Giaretta et al., *Protecting the Internet of Things with Security-by-Contract and Fog Computing*, *in* PROC2019. IEEE 5TH WORLD FORUM ON INTERNET OF THINGS 11, (2019).

4. MICHAEL FAGAN ET AL., DRAFT NISTIR 8259, CORE CYBERSECURITY FEATURE BASELINE FOR SECURABLE IOT DEVICES: A STARTING POINT FOR IOT DEVICE MANUFACTURERS, vii. pont (2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8259-draft.pdf [https://perma.cc/QEB7-2638].

5. Néhány példa a közelmúlt technológiai vívmányaira, amelyek mélyreható hatással vannak: Google (1998-ban alapították); Facebook (2004); bitcoin, blokklánc és virtuális valuták (2009); Uber (2009); WhatsApp (2009); Instagram (2010). A Google-ról lásd: Lawrence J. Trautman, *How Google Perceives Customer Privacy, Cyber, E-Commerce, Political and Regulatory*



Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

riasztó ütemben.[6] 2020-ra "az IoT-eszközök egyre gyakrabban lesznek érintettek kibertámadásokban, ami aggodalmat kelt a közösségben a kritikus infrastruktúrát, a vállalatokat és a polgárokat fenyegető kockázatok miatt. " [7]A nemzetközi szabványügyi testület, az Internet Engineering Task Force (IETF) a kockázatok mérséklésére törekedve "arra ösztönzi az IoT-gyártókat, hogy IoT-eszközeik rendeltetésére vonatkozóan hivatalos specifikációkat dolgozzanak ki a gyártó felhasználási leírása (MUD) formájában, hogy a hálózati viselkedésük bármilyen működési környezetben lezárható és szigorúan ellenőrizhető legyen".[8] A cikk témája az a kihívás, amellyel az embereknek szembe kell nézniük, amikor megpróbálják szabályozni a mesterséges intelligencia, a gépi tanulás és az internetre csatlakoztatott több milliárd érzékszervi eszköz hatását.

Ez a cikk kilenc részből áll. Először is meghatározza a tárgyak internetének (IoT) fogalmát, megjegyzi az internethez csatlakoztatott érzékszervi eszközök robbanásszerű növekedését, példákat hoz a tárgyak internetének eszközeire, és a tárgyak internetének ígéretéről beszél.

---

*Megfelelési kockázatok*, WM10. & MARY BUS. L. REV. 1,17 (2018) (idézi: Alphabet Inc. negyedéves jelentés (Form 10-Q), at (72017. október 27.)). A Facebookról, a bitcoinról, a blokkláncokról és a virtuális valutákról szóló vitákat lásd Lawrence J. Trautman, *Is Disruptive Blockchain Technology the Future of Financial Services?* , CONSUMER69 FIN. L.Q. REP. 232,234 (2016) [a továbbiakban: Trautman, *Disruptive Blockchain Technology*]; Lawrence J. Trautman & Alvin C. Harrell, *Bitcoin Versus Regulated Payment Systems: What Gives?* , CARDOZO38 L. REV. 1041 (2017); Lawrence J. Trautman, *Virtual Currencies; Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox?* , RICHMOND20 J. L. & TECH. 1,43 (2014) [a továbbiakban: Trautman, *Virtual Currencies*]. Az Uberről lásd: *Company Info*, UBER, https://www.uber.com/newsroom/company-info/ [https://perma.cc/UDE2-9L54]. A WhatsAppról szóló vitát lásd: Parmy Olson, *Exclusive: The Rags-to-Riches Tale of How Jan Koum Built WhatsApp Into Facebook's New $19 Billion Baby*, FORBES (Feb. 19, 72014,:58 PM), https://www.forbes.com/sites/parmyolson/2014/02/19/exclusive- inside-story-how-jan-koum-built-whatsapp-into-facebooks-new-19-billion-baby/ [https://perma.cc/Z RM5-22WM]. Az Instagramról lásd Amelia Tait, *How Instagram Changed the World*, GUARDIAN (2020. május 3.), https://www.theguardian.com/technology/2020/may/03/how-instagram- changed-our-world [https://perma.cc/KP2F-R5K9]; Gwyn Topham, *Look Ma, No Hands: Mit fog jelenteni, ha minden autó képes lesz magától vezetni?* , GUARDIAN (201725,. nov.), https://www.theguard ian.com/business/2017/nov/25/autonomous-vehicles-when-all-cars-drive-themselves-what-will-it-mean [https://perma.cc/8XRJ-3KNT].

6. *Lásd általában* BRUCE MIDDLETON, A CYBER SECURITY ATTACKS TÖRTÉNETE: TO1980 PRESENT (2017); *lásd a* IV. részt.

7. Ayyoob Hamza et al., *Clear as MUD:* IOT S&P'18: PROCEEDINGS OF THE 2018 WORKSHOP ON IOT SECURITY AND PRIVACY (82018); *lásd még* Sarah Coble, *Amazon Doorbell Camera Lets Hackers Access Household Network*, INFOSECURITY MAG. (Nov. 7, 2019), https://www.infosecurity-magazine.com/news/amazon-doorb ell-camera/ [https://perma.cc/UB8H-ZLBZ]; Angella Foster, *When Parents Spy on Nannies*, Op-Ed, N.Y. TIMES (201919,. aug.), https://www.nytimes.com/2019/08/19/opinion/nanny-cams-privacy.html [https://perma.cc/9H5V-2A8R]; Sandra E. Garcia, *Data Breach at Wyze Labs Exposes Information of Million2.4 Customers*, N.Y. TIMES (2019. dec.30,), https://www.nytimes.com/2019/ 12/30/business/wyze-security-camera-breach.html [https://perma.cc/VHY3-NBTW]; Kate Murphy, *A Paranoid Guide to Fighting the 'Bugging Epidemic'*, N.Y. TIMES (2019. nov. 15.), https://www.ny times.com/2019/11/15/technology/surveillance-bugging-bugging-protection.html [https://perma.cc/TDN6-QB SF]; Zack Whittaker, *Amazon Ring Doorbells Expose Home Wi-Fi Passwords to Hackers*, TECH CRUNCH (2019. nov. 7., 7:43 AM), https://techcrunch.com/2019/11/07/amazon-ring-doorbells-wifi- hackers/ [https://perma.cc/YXB5-TB7X].

8. Hamza et al., *Supra* note 7.



Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

IoT. Másodszor, a cikk a tárgyak internetének irányításával kapcsolatos kihívás mérlegelésének alapjául a vállalatirányításra vonatkozó jogi követelményeket tárgyalja. Harmadszor, megvizsgálja a tárgyak internetének potenciális veszélyeit. Negyedszer a cikk a Mirai botnetet tárgyalja. Ötödször a cikk a tárgyak internete fenyegetésvektorainak sebezhetőségét vizsgálja válság idején. Hatodszor a cikk a gyártott felhasználás leírásának módszertanát tárgyalja. A hetedik cikk a legújabb szabályozási fejleményeket tárgyalja. Végül a cikk néhány ajánlást fogalmaz meg, és következtetéseket von le. Úgy véljük, hogy ez a cikk hozzájárul a tárgyak internetéhez kapcsolódó rosszindulatú szoftvereknek való széles körű kitettség megértéséhez, és kiegészíti a vállalati kockázatok szabályozásával kapcsolatos, még kialakulóban lévő, de már kialakulóban lévő szakirodalmat, amely létfontosságú társadalmi jelentőségű téma.

## II. A DOLGOK INTERNETE (IoT)

> A folyamatos és gyors technológiai fejlődés továbbra is központi szerepet játszik a gazdasági jólét és a társadalmi jólét szempontjából, ugyanakkor potenciális új veszélyeket is hordoz magában. A tárgyak internete (IoT) új eszközök milliárdjait kapcsolja az internethez, de ezzel egyidejűleg a kiberszereplők támadási lehetőségei is bővülnek a hálózatok és információk ellen.
>
> -Daniel R. Coats, a Nemzeti Hírszerzés igazgatója, május 11,2017[9]

A tárgyak internetét úgy lehet meghatározni, mint "az internethez, és ennek következtében egyre inkább egymáshoz kapcsolódó eszközök hatalmas hálózatát".[10] A legegyszerűbben fogalmazva, minden olyan érzékszervi eszköz, amely kapcsolatot találhat az internethez, a tárgyak internetének része. Ez a meghatározás magában foglalja a viselhető eszközöket, például az órákat vagy bármilyen, a ruházaton viselt érzékelő eszközt, amely az egészségügyi életjeleket, például a szívritmust, a testhőmérsékletet vagy a vérnyomást érzékeli; az okos telefonokat; a háztartási eszközöket, például a bejárati ajtó videokameráit, a növények és a kertészet öntözési igényeit, a televíziók vezérlésére szolgáló hangkommunikációs eszközöket, a szobahőmérsékletet és így tovább. A katonai érzékelési alkalmazások is erőteljesek: az IoT távérzékelő eszközök figyelik a csapatok és járművek mozgását; szonár és űrérzékelő alkalmazások; valamint az egészséges és sebesült katonák életjeleit a hadszíntéren, hogy csak néhányat említsünk.

Bruce Sinclair azt írja, hogy "a tárgyak internete (IoT) nem más, mint az internet továbbfejlesztése. Nem több és nem kevesebb. Az IoT üzleti kihatásai azonban forradalmiak, és bevezetik az eredménygazdaságot. "[11] Sinclair úr továbbá megállapítja, hogy "A dolgok internetének gyilkos alkalmazása az eredmények. Az eredmények azok, amelyeket az ügyfelek végső soron akarnak. Nem is a termékek érdeklik őket, hanem a következők.

---

9. *Az Egyesült Államok hírszerző közösségének világméretű fenyegetettségi értékelése: Meghallgatás a hírszerzési bizottság előtt*, 115. kong. 3 (2017) (Daniel R. Coats, Office of the Director of Nat'l Intelligence) [a továbbiakban: Coats Statement], https://www.dni.gov/files/documents/ Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf [https://perma.cc/984S- AUL3].

10. Bill Newhouse, *IOT Considerations in the Hospitality Sector*, HOSPITALITY UPGRADE, nyár, 2019,44,44,http://mag.hospitalityupgrade.com/publication/frame.php?i=592422&p=46&pn=&ver=html5.

11. BRUCE SINCLAIR, IOT INC.: HOGYAN HASZNÁLHATJA AZ ÖN CÉGE A DOLGOK INTERNETÉT A KÖVETKEZŐKRE WIN IN THE OUTCOME ECONOMY xi (2017).



Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

mit tesznek értük a termékek [A] fogyasztók nem akarnak autót birtokolni; azt szeretnék, hogy
hogy gyorsan és biztonságosan eljusson egyik helyről a másikra."[12]

Lawrence J. Trautman és Peter C. Ormerod azt írják, hogy "az újszerű fogyasztói eszközök elterjedése és a megnövekedett internetfüggő üzleti és kormányzati adatrendszerek soha nem látott mértékű sebezhetőségeket hoznak létre. "[13] Megjegyzik, hogy ezek a "[d]igitális sebezhetőségek a jog számos különböző területét érintik: a magánélet védelmét, a [14]kockázatkezelést, a [15]vállalatirányítást[16] (beleértve a gondossági,[17] ellenőrzési [18]és közzétételi[19] kötelezettségeket), a jogsértések bejelentését,[20]

---

12. *Id.*, xxii.

13. Lawrence J. Trautman & Peter C. Ormerod, *Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things*, 72 U. MIAMI L. REV. 761, 764 (2018) (idézi Trey Herr & Allan A. Friedman, *Redefining Cybersecurity*, DEF. TECH. PROGRAM BRIEF (Am. Foreign Pol'y Council, Washington, D.C.), 2015. január 1., 1-2. o.; Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1250-511227, (2003)).

14. *Id.* (idézi Corey Ciocchetti, *The Privacy Matrix*, U12. FLA. J. TECH. L. & POL'245,Y 249(2008); Neil M. Richards & Jonathan H. King, *Big Data and the Future for Privacy*, *in* RESEARCH HANDBOOK ON DIGITAL TRANSFORMATIONS 272, 283 (F. Xavier Olleros & Majlinda Zhegu szerk., 2016); Sasha Romanosky & Alessandro Acquisti, *Privacy Costs and Personal Data Protection: Economic and Legal Perspectives,* BERKELEY24 TECH. L.J. 1064-651061, (2009); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, (5902014); Robert Kirk Walker, *The Right to be Forgotten,* HASTINGS64 L.J. 269-70257, (2012); Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection (Version 2.0) (*3George Washington Law Sch. Pub. Law Research Paper No. 132, 2005).

15. *Id.* at 764, (idézi Liam M.D. Bailey, *Mitigating Moral Hazard in Cyber-Risk Insurance*, 3 J.L. & CYBER WARFARE 1, 8-9 (2014); Shauhin A. Talesh, *Data Breach, Privacy, and Cyber Insurance* 6-7 (Legal Studies Research Paper Series No. 2017-23, 2017); Lawrence J. Trautman & Kara Altenbaumer-Price, *D&O Insurance: A Primer*, AM. U. BUS. L. REV. 337,340 (2012)).

16. *Id.* at (764,idézi773 Lucian A. Bebchuk et al., *What Matters in Corporate Governance?* , 22 REV. FIN. STUD. 783, 788 (2009); Lawrence J. Trautman & Kara Altenbaumer-Price, *The Board's Responsibility for Information Technology Governance*, 28 J. MARSHALL J. COMPUTER & INFO. L. 313, 315-17 (2011); John Armour et al., *Agency Problems, Legal Strategies, and Enforcement* 11-129,, John M. Olin Ctr. for Law, Econ., & Bus., Working Paper No. 2009644,)).

17. *Id.* 765. o. (idézi Stephen M. Bainbridge et al., *The Convergence of Good Faith and Oversight*, 55 UCLA L. REV. 559, 574-75; Melvin A. Eisenberg, *The Duty of Good Faith in Corporate Law*, 31 DEL. J. CORP. L. 111, (2005)).

18. *Id.* (idézi Robert T. Miller, *The Board's Duty to Monitor Risk after Citigroup*, 12 U. PA. J. BUS. L. 1154-551153, (2010)).

19. *Id.* (idézi Bernard S. Black, *The Core Fiduciary Duties of Outside Directors*, ASIA3 BUS. L. REV. 1, 18-19 (2001); Henry T.C. Hu, *Too Complex to Depict? Innovation, "Pure Information", and the SEC Disclosure Paradigm*, TEX90. L. REV. 1601, 1614-15 (2012); Peter A. Swire, *A biztonsági és versenyképességi okokból történő közzététel elmélete: Open Source, Proprietary Software, and Government Agencies*, 42 HOU. L. REV. 1333, 1344-45 (2006)).

20. *Id.* (idézi Dana Lesemann, *Once More Unto the Breach: An Analysis of Legal, Technological and Policy Issues Involving Data Breach Notification Statutes*, 4 AKRON INTELL. PROP. J. 203, 206-08 (2010); Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, MICH105. L. REV. 913,918, 923-25 (2007); Jane K. Winn, *Are "Better" Security Breach Notification Laws Possible?* , 24 BERK. TECH. L. J. 1, 1-2 (2009); Fabio Bisogni, Evaluating Data Breach Notification Laws, What Do the Numbers Tell Us?, (Aug. 201315,) (kiadatlan kézirat), https://ssm.com/abstract=2236144)).



Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

információ- és adatbiztonság, [21]értékpapír-szabályozás, háborús [22]jog, [23]alkotmányos rendelkezések [24]és még sok más."[25]

## A. Az érzékelő eszközök robbanásszerű növekedése

Az eszközöket összekötő IoT-termékek otthoni és munkahelyi használata 2020-ra várhatóan "eléri a milliárdot".20.4[26] A National Institutes of Standards and Tech- nology (NIST) megjegyzi:

> A tárgyak internete (IoT) a fizikai világgal kölcsönhatásban álló különböző technológiák gyorsan fejlődő és bővülő gyűjteménye. Az IoT-eszközök az információs technológia (IT) és az operatív technológia (OT) világának ötvözéséből származnak. Számos IoT-eszköz a felhőalapú számítástechnika, a mobil számítástechnika, a beágyazott rendszerek, a nagy adatmennyiség, az alacsony árú hardver és más technológiai fejlesztések konvergenciájának eredménye. Az IoT-eszközök számítási funkciókat, adattárolást és hálózati csatlakoztathatóságot biztosíthatnak olyan berendezések számára, melyek

---

21. *Id.* (idézi Ian Brown et al., *Information Security and Cybercrime*, *in* LAW AND THE INTERNET 671, 671 (Lilian Edwards & Charlotte Waelde eds., 3d ed. 2009); Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1708-11 (2010); Daniel J. Solove, *The New Vulnerability*: SECURING PRIVACY IN THE INTERNET AGE 111, 111 (Anupam Chander et al. szerk., 2008); Richard Warner & Robert H. Sloan, Defending Our Data: The Need for Information We Do Not Have 1-2 (201611,. aug.) (kiadatlan kézirat), https://ssrn.com/abstract=2816010; Josephine Wolff, Models for Cybersecurity Incident Information Sharing and Reporting Policies 3 (201413,. aug.) (kiadatlan kézirat), https://ssrn.com/abstract=2587398)).

22. *Id.* (idézi Zohar Goshen & Gideon Parchomovsky, *The Essential Role of Securities Regulation*, 55 DUKE L.J. 711, 732-37 (2006); Andrea M. Matwyshyn, *Material Vulnerabilities: Data Privacy, Corporate Information Security and Securities Regulation*, 3 BERKELEY BUS. L.J. 129, 136-37 (2005); Robert B. Thompson & Hillary A. Sale, *Securities Fraud as Corporate Governance: Reflections Upon Federalism*, 56 VAND. L. REV. 859, 869-70 (2003); Lawrence J. Trautman & George P. Michaely, *The SEC & The Internet: Regulating the Web of Deceit*, 68 CONSUMER FIN. L.Q. REP. 262, 262-63 (2014)).

23. *Id.* at (766idézi DANIEL SUI ET AL .,WOODROW WILSON INT'L CTR. FOR SCHOLARS, THE DEEP WEB AND THE DARKNET: A LOOK INSIDE THE INTERNETS' MASSIVE BLACK BOX (2015); Steven M. Bellovin et al., *Limiting the Undesired Impact of Cyber Weapons: Technical Requirements and Policy Implications*, 3 J. CYBERSECURITY 59, 60 (2017); Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right to Self-Defense*, 38 STAN. J. INT'L L. 207, 209-12 (2002); Michael N. Schmitt & Sean Watts, *The Decline of International Humanitarian Law* Opinio Juris *and the Law of Cyber Warfare*, TEX50. INT'L L. J. 224-25189, (2015); Scott Shackelford et al., *Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors*, CHI17. J. INT'L L. 25-271,3, (2016); Christopher S. Yoo, *Cyber Espionage or Cyberwar? International Law, Domestic Law, and Self-Protective Measures*, *in* CYBERWAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS (Jens David Ohlin et al. eds., 2015); Eric Talbot Jensen, *The Tallinn Manual 2.0*: *Highlights and Insights*, 48 GEO. J. INT'L L. 736-37735, (2017)).

24. *Id.* (idézi Peter C. Ormerod & Lawrence J. Trautman, *A Descriptive Analysis of the Fourth Amendment and the Third-Party Doctrine in the Digital Age*, ALB28. L.J. SCI. & TECH. 73, 88)).

25. *Id.* (idézi TREY HERR ET AL., BELFER CTR. FOR SCI. & INT'L AFFAIRS, THE CYBER SECURITY PROJECT, TAKING STOCK: ESTIMATING VULNERABILITY REDISCOVERY (2017)).

26. Press Release, Gartner, Inc., Gartner Says Billion8.4 Connected "Things" Will Be in Use in Up 2017,Percent31 From (2016Feb. 20177,), https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016 [https://perma.cc/6JE6-C5A8].



Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

> amelyek korábban nem rendelkeztek ilyenekkel, új hatékonyságot és technológiai képességeket biztosítva a berendezések számára, például távoli hozzáférést a felügyelethez, konfiguráláshoz és hibaelhárításhoz. A tárgyak internete a fizikai világra vonatkozó adatok elemzésére és az eredmények felhasználására is képes, hogy jobban tájékoztassa a döntéshozatalt, megváltoztassa a fizikai környezetet és előre jelezze a jövőbeli eseményeket. Bár az IoT teljes terjedelme nincs pontosan meghatározva, egyértelműen hatalmas. Minden ágazatnak megvannak a maga IoT-eszköztípusai, például az egészségügyi ágazatban a speciális kórházi berendezések, a közlekedési ágazatban az intelligens közúti technológiák, és nagyszámú olyan vállalati IoT-eszköz létezik, amelyet minden ágazat felhasználhat. Szinte minden fogyasztói elektronikai eszköznek, amelyek közül sokan a szervezetek létesítményeiben is jelen vannak, a változatai csatlakoztatott IoT-eszközökké váltak - konyhai készülékek, hőszabályozók, otthoni biztonsági kamerák, ajtózárak, villanykörték és televíziók.[27]

2019-ben Giaretta, Dragoni és Massacci a következő összegzést adják az IoT-környezetről:

> A Gartner Hype Cycle for Emerging Technologies szerint az Internet of Things (IoT) túllépett az úgynevezett kiábrándulás csúcsán, és a társadalomban betöltött szerepe felé tart. De még messze nem oldódott meg minden probléma, és minél inkább elterjedté válik az IoT, annál nehezebb lesz kezelni. Különösen az IoT biztonsága az egyik legnagyobb kiberbiztonsági kihívás, és az egyik legkínosabb kudarc. A hagyományos kiberbiztonsági megoldások számos technikai és üzemeltetési kihívás miatt hatástalannak bizonyultak az IoT esetében. Először is, az IoT-eszközök rendkívül heterogének, a szintek, nyelvek, operációs rendszerek és hálózatok között hatalmas különbségek vannak. Emellett az IoT-nek nincs egységes biztonsági kerete, és a szabványok még mindig nincsenek kidolgozva. Gyakran előfordul, hogy a biztonság nem tartozik a gyártók (sem az IT-adminisztrátorok) alapvető kompetenciái közé, és nem is feltétlenül képezi az IoT-termékfejlesztési folyamat részét.[28]

Egy nemrégiben végzett Google-keresés olyan fogyasztói termékeket azonosított, mint például egy bejárati ajtó IoT-kamerás monitor, amelynek értékesítési ára 34,95 USD; és egy bébi monitor, amely "Pet Camera Wireless IP Security WiFi Surveillance Camera with Cloud Storage Two Way Audio Pan/Tilt/Zoom Night Vision Motion Detect Re- mote Control for Home/Shop/ Office," 39,95 USD áron.[29] Az ábra csak egy példát mutat1 az internetre csatlakozó IoT-eszközök közül. IoT-érzékelők tucatjai találhatók egy tipikus okosotthonban, "míg az ipari alkalmazások akár több száz IoT-eszközre is kiterjedhetnek".[30] Az IoT-eszközök nagy száma "számos problémát vet fel, például az IoT-eszközök karbantartása és felügyelete, a kommunikációs protokollok engedélyezése és tiltása, valamint annak felügyelete, hogy milyen információk oszthatók meg meghatározott feltételek mellett".[31]

---

27. KATIE BOECKL ET AL., NISTR 8228, CONSIDERATIONS FOR MANAGING INTERNET OF THINGS (IOT) CYBERSECURITY AND PRIVACY RISKS, at iv (2019), https://nvlpubs.nist.gov/nistpubs/ ir/2019/NIST.IR.8228.pdf [https://perma.cc/ZYG4-8LDR].

28. Giaretta, et al., *Supra* note. 3.

29. Legutóbbi Google-keresés a "IoT kamera" kifejezésre.

30. Giaretta et al., *Supra* note. 3.

31. *Id.*



Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

**Ábra Példa1. az internetkapcsolatra szolgáló eszközre[32]**


## B. A dolgok internetének ígérete

Kris Alexander, az Akamai Technologies technológiai igazgatója megjegyzi, hogy a dolgok internete vagy a mindenek internete ígéretes:

> Az IoT/IoE ígérete az, hogy az eszközök mostantól összekapcsolódhatnak egymással (és az emberekkel), hogy új cselekvéseket tegyenek lehetővé - olyasmit, amit korábban nem tudtak; például figyelmeztessenek, ha a nyugalmi pulzusszámod túl magas, vagy megtanulják, hogy mennyire szereted hűvösnek találni a házadat, és mikor érsz haza, és beállítják a hőmérsékletet, mielőtt odaérsz.[33]

Bruce Sinclair szerint a rendszerintegrációs mérnökök "úgy tekintenek az IoT-technológiára, mint egy hálózati veremre, amely bizonyos értelemben egyszerűen egy protokolltérkép".[34] (Lásd a 2. ábrát). Sinclair úr aztán siet hozzátenni, hogy "[m]inden protokollt onnan, ahonnan az érzékelőadatok érkeznek, az alkalmazásig vizsgálni abszolút rossz módja a technológia szemléletének - legalábbis az üzleti életben. Ez vízvezeték-szerelés, és nem az, ahonnan az érték származik".[35]

---

32. Legutóbbi Google-keresés a "IoT kamera" kifejezésre.

33. Kris Alexander, *The Promise and Challenges of an Internet of Things (IoT)*, CIOREV, https://juniper-networks.cioreview.com/cxoinsight/the-promise-and-challenges-of-an-internet-of-things-iot-world-nid-4769-cid-73.html [https://perma.cc/5MJ5-R7V2].

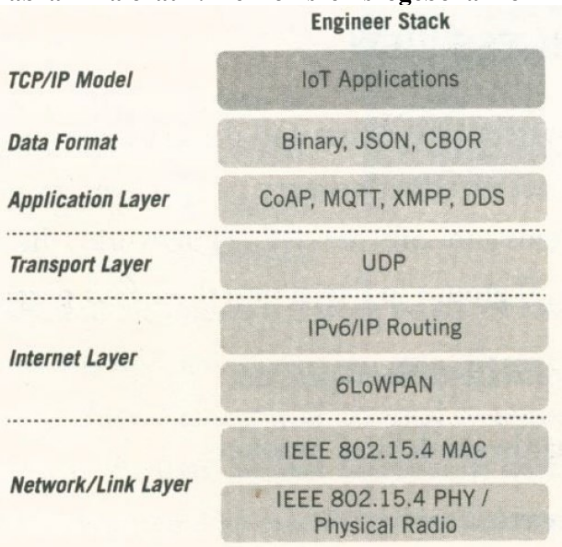
34. SINCLAIR, *Supra* note at11, 5.

35. *Id.*



Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

**ábra A hálózati2. mérnök szemszögéből az IoT[36]**




Bruce Sinclair az üzleti érték szempontjából írva megjegyzi, hogy "a vízvezetékrendszerek azonban csak eszköz a cél eléréséhez; ez a módja annak, hogy az adatok egyik helyről a másikra jussanak".[37] Bár Sinclair azt írja, hogy "nem tekintek az IoT-technológiára úgy, mint egy hálózati veremre, mert ez nem különíti el megfelelően és nem emeli ki, hogy hol keletkezik érték", a hálózati verem [38]men- tézése értéket kölcsönöz az itt folytatott vitánknak. Ezután annak bemutatása következik, hogy az IoT technológiai jelenségei hogyan kapcsolódnak a "gondossági kötelezettség" kihívást jelentő vállalatirányítási szempontjaihoz.

36. *Id.*; *lásd még* RACHELLE MILLER, SANS INST., THE OSI MODEL: AN OVERVIEW (2001), https://www.sans.org/reading-room/whitepapers/standards/osi-model-overview-543 [https://perma. cc/H3XU-9KUF] ; Peter Swire, *A Pedagogic Cybersecurity Framework: A Proposal for Teaching the Organizational, Legal, and International Aspects of Cybersecurity*, COMM. ACM, okt. 2018,23. o. (a nyílt rendszerek összekapcsolási modelljének "OSI Stack" hagyományos hét rétegén túl három réteg hozzáadását javasolja).

37. SINCLAIR, *Supra* note at11, 5.

38. *Id.*



Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

## III. A VÁLLALATIRÁNYÍTÁSI KIHÍVÁS

> [A nemzetünk magánszektorát és kormányzati hálózatait érő kibertámadások gyakorisága és hatása drámaian megnőtt az elmúlt évtizedben, és várhatóan tovább fog növekedni. Továbbra is azt látjuk, hogy a rosszindulatú kibertevékenységekről szóló jelentések mértéke és terjedelme növekszik, ami az ellopott vagy törölt vállalati adatok, a veszélyeztetett személyazonosításra alkalmas információk vagy az amerikai áldozatoknál felmerült helyreállítási költségek alapján mérhető. Az FBI-on belül a legveszélyesebb rosszindulatú kibertevékenységekre összpontosítunk: az állami támogatású hackerek és a globális szervezett bűnszövetkezetek által elkövetett magas szintű behatolásokra, valamint más, technikailag kifinomult támadásokra.
>
> -Christopher Wray, a Szövetségi Nyomozó Iroda igazgatója,
> Szeptember 27,2017[39]

A legrövidebben fogalmazva, a társaságok tisztségviselőinek és igazgatóinak két elsődleges kötelezettsége van a részvényesekkel szemben: *a lojalitás kötelezettsége* (nincs öntevékenység) és *a gondosság kötelezettsége* (az ésszerű viselkedés kötelezettsége). A gondossági kötelezettség az igazgatók és tisztségviselők számtalan felelősségi körére vonatkozik, beleértve a vállalat digitális adatainak kezelését is. A gondossági kötelezettség lényegében eljárási jellegű. Az elmúlt években egyre nagyobb hangsúlyt kapott az igazgatók azon felelőssége, hogy biztosítsák az ügyfelek és felhasználók adatainak védelmét.[40] A NIST megjegyzi:

> Sok szervezet nem feltétlenül van tudatában annak, hogy nagyszámú IoT-eszközt használ. Fontos, hogy a szervezetek megértsék az IoT használatát, mert sok IoT-eszköz másképp befolyásolja a kiberbiztonsági és adatvédelmi kockázatokat, mint a hagyományos IT-eszközök. Miután a szervezetek tisztában vannak a meglévő és a lehetséges jövőbeli IoT-használatukkal, meg kell érteniük, hogy az IoT jellemzői hogyan befolyásolják a kiberbiztonsági és adatvédelmi kockázatok kezelését, különösen a kockázatra való reagálás - a kockázat elfogadása, elkerülése, mérséklése, megosztása vagy átruházása - szempontjából.[41]

A következő szakaszok nagyon röviden tárgyalják a lojalitás és a gondoskodás vállalati kötelességeit.

### A. A hűség kötelessége

A delaware-i jog szerint a lojalitási kötelezettség megköveteli, hogy "a kötelesség és az önérdek között ne legyen konfliktus".[42] A bizalmi "lojalitási kötelezettség" alapkoncepcióját a következőképpen írták le

---

39. *Lásd* Lawrence J. Trautman & Peter C. Ormerod, *WannaCry, Ransomware, and the Emerging Threat to Corporations*, TENN86. L. REV. 503,507 (2019) (idézi *World-Wide Threats: Keeping America Secure in a New Age of Terror: Hearing Before the H. Comm. on Homeland Sec.* , 115th Cong. 29 (2017) (prepared statement of Christopher Wray, Director, Fed. Bureau of Investigation)).

40. *Lásd általában* Lawrence J. Trautman, *Governance of the Facebook Privacy Crisis*, PITT20. J. TECH. L. & POL'Y 43 (2020).

41. BOECKL ET AL., *fenti* 27,iv. megjegyzés.

42. *Lásd* Trautman & Altenbaumer-Price, *Supra* 16. lábjegyzet, 324. o. (idézi a Guth kontra Loft, A.2d 510503, (Del. 1939)).



Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

> [az a követelmény, hogy az igazgatónak a társaság érdekeit a saját érdekeivel szemben előnyben kell részesítenie, ha ezek az érdekek ütköznek. A gondossági kötelezettséghez hasonlóan a lojalitási kötelezettségnek is van egy őszinteségre vonatkozó aspektusa. Így amikor egy igazgató olyan helyzettel szembesül, amelyben személyes érdekei és a társaság érdekei ütköznek, a bíróságok nemcsak azt fogják gondosan megvizsgálni, hogy az ügyletben nem részesítette-e tisztességtelenül előnyben személyes érdekeit, hanem azt is, hogy teljesen őszinte volt-e a társasággal és annak részvényeseivel.[43]

Amint azt Trautman és Altenbaumer-Price megállapította, "az összeférhetetlenség "*önmagában* nem eredményezi a lojalitási kötelezettség megszegését". Inkább az a mód, ahogyan az érdekelt igazgató kezeli az összeférhetetlenséget, és a társaság és részvényesei iránti tisztességes eljárás, amely meghatározza az igazgató magatartásának helyességét." [44]Általában, kivéve azokat az eseteket, amikor az igazgató
nem titkolt pénzügyi érdekeltsége van egy jelentős vállalati beszerzés vagy szerződéses döntés kimenetelében, úgy tűnik, hogy a lojalitási kötelezettség nem igényel további figyelmet.

## B. Gondoskodási kötelezettség

Trautman és Altenbaumer-Price korábban azt írták, hogy "[a]z igazgatók gondossági kötelezettsége "mind a diszkrét döntéshozatali kontextusban, mind a felügyelet és ellenőrzés területén felmerül"."[45] Azt is megjegyezték, hogy "az 1985-ös *Smith v. Van Gorkom* land-mark ügy előtt,[46] kísérő hűtlen cselekmények hiányában, általánosan elfogadott volt, hogy 'a bíróságok ritkán találtak egyéni igazgatók felelősségét

---

43. *Id.* (idézi CHARLES R.T. O'KELLEY & ROBERT B. THOMPSON, CORPORATIONS AND MÁS ÜZLETI SZÖVETSÉGEK: (5. kiadás, 2006)).

44. *Id.* (idézi Byron Egan, *Igazgatói feladatok:* TEXASBARCLE WEBCAST: CORPORATE MINUTES/ DIRECTOR DUTIES (200823,. október)).

45. *Id.* 322. o. (idézi Lyman P.Q. Johnson & Mark A. Sides, *Corporate Governance and the Sarbanes-Oxley Act: The Sarbanes-Oxley Act and Fiduciary Duties*, 30 WM. MITCHELL L. REV. 1149, 1197 (2004) (idézi Citron v. Fairchild Camera & Instrument Corp., 569 A.2d 53, 66 (Del. 1989)); Brehm v. Eisner*, A*746.2d (244,Del264. 2000) ("Due care in the decision-making context is process due care only.").

46. *Lásd id.* (idézve a Smith kontra Van Gorkom, 488 A.2d 858 (Del.Supr. 1985) ügyet). Trautman és Altenbaumer-Price megjegyezte: "A Delaware-i Legfelsőbb Bíróság megállapította, hogy a Trans Union Corporation tapasztalt és szofisztikált igazgatói nem élvezték az üzleti ítélőképesség szabályának védelmét, és megszegték a részvényeseikkel szembeni bizalmi kötelességüket "(1) azzal, hogy nem tájékoztatták magukat minden olyan információról, amely ésszerűen rendelkezésükre állt és amely releváns volt a Pritzker fúzió jóváhagyásával kapcsolatos döntésük szempontjából; és (2) azzal, hogy nem hoztak nyilvánosságra minden olyan lényeges információt, amelyet egy ésszerű részvényes fontosnak tartana a Pritzker of- fer jóváhagyásának eldöntése során."". *Id.* 323. o. (idézi a *Van Gorkom*, 488 A.2d, 888. o.); *lásd még* PETER V. LETSOU, CASES AND MATERIALS ON CORPORATE MERGERS AND ACQUISITIONS 643 n.21 (2006) ("A Trans Union öt "belső" igazgatója jogi és számviteli háttérrel rendelkezett, 116 éve dolgozott együttesen a vállalatnál, és több éves68 együttes tapasztalattal rendelkezett az igazgatótanácsban. A Trans Union öt "külső" igazgatója között négy nagyvállalat vezérigazgatója és egy közgazdász volt, aki korábban egy jelentős üzleti iskola dékánja és egy egyetem kancellárja volt. A "külső" igazgatók együttesen több éves78 tapasztalattal rendelkeztek nagyvállalatok vezérigazgatójaként és 50 éves összesített tapasztalattal a Trans Union igazgatójaként. Így az alperesek azzal érvelnek, hogy az igazgatótanács kiválóan alkalmas volt arra, hogy megalapozott döntést hozzon a Trans Union javasolt "eladásáról", annak ellenére, hogy nem kaptak előzetes értesítést a javaslatról, a tanácskozás rövid volt, és úgy döntöttek, hogy nem konzultálnak befektetési bankárral, és nem kérnek fairness-véleményt.").



Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

a gondossági kötelezettségük megszegéséért.""[47] A tapasztalt és tapasztalt igazgatók ebben az esetben nem voltak jogosultak az üzleti ítélőképesség szabályának védelmére bizonyos esetekben, mert

> a gondossági kötelezettség meghatározza azt a módot, ahogyan az igazgatóknak eleget kell tenniük jogi kötelezettségeiknek . . . beleértve a vállalati tisztségviselők megválasztását, értékelését és díjazását; a vállalati stratégia, a költségvetések és a tőkekiadások felülvizsgálatát és jóváhagyását; a belső pénzügyi információs rendszerek és a pénzügyi beszámolási kötelezettségek felügyeletét, valamint a jogi követelményeknek való megfelelést; a részvényeseknek történő kifizetéseket; a nem a szokásos üzletmenethez tartozó ügyletek jóváhagyását; a bizottságok tagjainak kinevezését és a bizottsági hatáskörök ellátását, beleértve a fontos audit, kompenzációs és jelölő bizottságokat; valamint az alapító okirat és az alapszabály módosításának kezdeményezését.[48]

## C. Adatbiztonsági kötelezettség

Trautman és Ormerod professzorok azt állítják, hogy a széles körű gondossági kötelezettség magában foglalja az adatbiztonság biztosításának kötelezettségét. Ennek megfelelően megjegyzik, hogy

> [Ez a gondossági kötelezettség az igazgatók és tisztségviselők számtalan felelősségi körére vonatkozik, beleértve a vállalat digitális adatainak kezelését is. Az információs technológiával kapcsolatos gondossági kötelezettségnek tehát van egy kialakulóban lévő sajátos alkalmazási területe: az adatbiztonsági kötelezettség. Az alkalmazandó gondossági standard megköveteli az igazgatóktól, hogy "ésszerű" vagy "megfelelő" fizikai, technikai és adminisztratív biztonsági intézkedéseket hozzanak a vállalati adatok titkosságának, integritásának és rendelkezésre állásának biztosítása érdekében. "[49]

Nincs azonban egyetlen olyan forrás - például átfogó szövetségi törvény vagy rendelet -, amely az adatbiztonság biztosításának kötelezettségét írja elő. Ehelyett az adatbiztonsági rendszerek megvalósítására vonatkozó megfelelő jogi kötelezettségeket "az állami, szövetségi és nemzetközi törvények, szabályzatok, végrehajtási intézkedések és a szokásjog szerinti kötelezettségek, beleértve a "szerződéses" kötelezettségeket is, egyre bővülő szövevényében" határozzák meg.

---

47. *Lásd* Trautman & Altenbaumer-Price, *Supra* note. 16, (323idézi Jacqueline M. Veneziani, Note & Comment, *Causation and Injury in Corporate Control Transactions:* Cede & Co. v. Technicolor, Inc., 69 WASH. L. REV. 1167, 1194 n.3 (1994) ("Mielőtt a *Van Gorkom ügyet* eldöntötték, egy kommentátor azt mondta, hogy "[a]z olyan esetek keresése, amelyekben az igazgatókat ... önkereskedéssel nem bonyolított gondatlanság miatt felelősségre vonták származékos perekben, nagyon kevés tűt keres egy nagyon nagy szénakazalban."); Joseph W. Bishop, Jr., *Sitting Ducks and Decoy Ducks: New Trends in the Indemnification of Corporate Directors and Officers*, YALE77 L.J. (1078,19681099)). *De lásd id.* (idézve Norwood P. Beveridge, Jr., *The Corporate Director's Duty of Care: Riddles Wisely Expounded*, 24 SUFFOLK U. L. REV. 923, 945-46 (1990) (vitatva Bishop professzor állítását, és megjegyezve, hogy valójában számos olyan eset van, amely a gondossági kötelezettség megsértését tartja fenn)).

48. *Id.* (idézi Johnson & Sides, *Supra* note 45 (idézi *Citron*, 569 A.2d, 66. o.; *Eisner*, 746 A.2d, 264. o.).

49. Lawrence J. Trautman & Peter C. Ormerod, *Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach*, 66 AM. U. L. REV. 1231, 1235 (2017) [a továbbiakban Trautman & Ormerod, *Yahoo Data Breach*] (idézi THOMAS J. SMEDINGHOFF, INFORMATION SECURITY LAW: THE EMERGING STANDARD FOR CORPORATE COMPLIANCE (292008)).



Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

kötelezettségvállalások, valamint egyéb kifejezett és hallgatólagos kötelezettségek a vállalati adatok "ésszerű" vagy "megfelelő" biztonságának biztosítására"."[50]

## D. Vezetés a csúcson

A kibertámadások elleni hatékony vállalati programhoz a felső vezetés elkötelezettségére van szükség, hogy világosan kommunikálja, hogy a jó kiberhigiénia fontos és elsődleges fontosságú, nem csak üres szónoklat. Minden szervezetben megfelelő erőforrásokat kell biztosítani, ha reális előrelépést akarunk elérni a kiberfenyegetés ellen. A kibertámadások és az adatlopás valós fenyegetést jelentenek minden szervezet számára: vállalkozói induló vállalkozások, [51]nonprofit szervezetek, [52]önkormányzatok, [53]oktatási intézmények [54]és nagyvállalatok számára egyaránt.[55]

## E. Igazgatótanácsi tehetség és tapasztalat

A vállalati igazgatótanácsok jelölőbizottságai számára kihívást jelent az olyan igazgatók kiválasztása és toborzása, akik rendelkeznek az adat- és információs rendszerek kockázatainak irányításához szükséges készségekkel és tapasztalattal.[56] Nagyon kevés igazgató rendelkezik informatikai vagy villamosmérnöki háttérrel. Ennek eredményeképpen sok igazgatótanácsot frusztrál az a feladat, hogy olyasmit irányítson, amiről nagyon keveset tud.[57]

## F. Audit- vagy kockázatkezelési bizottság

A vállalati igazgatóságok bizottságokon keresztül működnek. Sok szervezetnél az igazgatótanács auditbizottsága gondoskodik arról, hogy a vállalkozásnak szilárd védelme legyen a kibertámadásokkal szemben.[58] Más igazgatóságok kockázati bizottságot hoztak létre, mivel az adatbiztonság egyre nagyobb hangsúlyt kap számos szervezetnél.

# IV. Potenciális IoT-fenyegetések

Trautman professzor már számos alkalommal beszélt a tárgyak internetének sebezhetőségéről, és hallgatósága különösen fogékonynak találta a következőket.

---

50. *Lásd id.* (idézi SMEDINGHOFF, 49. lábjegyzet). *Lásd általában* Lawrence J. Trautman, *Cybersecurity: What About U.S. Policy?* , U2015. ILL. J.L. TECH. & POL'Y (3412015); Lawrence J. Trautman, *Congressional Cybersecurity Oversight: Who's Who & How It Works*, 5 J.L. & CYBER WARFARE (1472016).

51. *Lásd általában* Lawrence J. Trautman et al., *Some Key Things U.S. Entrepreneurs Need to Know About the Law and Lawyers*, 46 TEX. J. BUS. L. 155 (2016).

52. *Lásd általában* Lawrence J. Trautman & Janet Ford, *Nonprofit kormányzás:* AKRON52 L. REV. 971 (2018).

53. *Lásd általában* Lawrence J. Trautman, *Cybersecurity: Mi a helyzet az amerikai politikával?* , 2015 U. ILL. J.L. TECH. & POL'Y 341 (2015).

54. *Lásd általában* David D. Schein & Lawrence J. Trautman, *The Dark Web and Employer Liability*, 18 COLO. TECH. L.J. 49 (2020).

55. *Lásd általában* Lawrence J. Trautman, *The Board's Responsibility for Crisis Governance*, HASTINGS13 BUS. L.J. 275 (2017) [a továbbiakban: Trautman, *Crisis Governance*].

56. *Lásd általában* Lawrence J. Trautman, *The Matrix: Az igazgatótanács felelőssége az igazgatóságért Kiválasztás és toborzás*, FLA11. ST. U. BUS. REV. 75 (2012).

57. *Lásd általában* Lawrence J. Trautman, *Who Qualifies as an Audit Committee Financial Expert Under SEC Regulations and NYSE Rules?* , DEPAUL11 BUS. & COMM. L. J. 205 (2013).

58. *Lásd id.*



Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

annak leírása, hogy az IoT-használat hogyan fékezi meg az adatbiztonsági veszélyeket. Arra kéri hallgatóságát, hogy "kérem, csukják be a szemüket, és képzeljék el, hogy éjszaka egy sötét tengerparton sétálnak. Séta közben apró szúrásokat észlel a lábán (úgy érzi, mintha talán szúnyogcsípés lenne, de nem az). Egy idő után észreveszik, hogy a lábuk elzsibbadt".[59] Nem tudod, hogy "a strandot hipo- dermikus tűk milliárdjai borítják, amelyek mindegyike olyan helyi érzéstelenítő zsibbasztó anyagot tartalmaz, mint a Novo- cain (némelyik vírussal szennyezett, gondolj az Ebolára vagy a HIV-re). Ez megközelíti azt a kockázatot, amit mindannyian a tárgyak internete kapcsán tapasztalunk. Most már kinyithatja a szemét."[60] Daniel R. Coats, a Nemzeti Hírszerzés igazgatója a Szenátus Különleges Hírszerzési Bizottsága előtt az amerikai hírszerző közösség világméretű fenyegetettségi értékeléséről szóló meghallgatásokra2017 készített előkészített megjegyzéseiben szintén megjegyzi, hogy

> [Az "intelligens" eszközök széles körű beépítése a mindennapi tárgyakba megváltoztatja az emberek és a gépek egymás közötti és a körülöttük lévő világgal való interakcióját, gyakran javítva a hatékonyságot, a kényelmet és az életminőséget. Az eszközök alkalmazása ugyanakkor sebezhetőséget is eredményezett mind az általuk támogatott és az általuk vezérelt infrastruktúrában, mind az általuk irányított folyamatokban. A kiberszereplők már eddig is használták a tárgyak interneteinek eszközeit elosztott szolgáltatásmegtagadási (DDoS) támadásokhoz, és becsléseink szerint ez folytatódni fog. A jövőben az állami és nem állami szereplők valószínűleg IoT-eszközöket fognak használni hírszerzési műveletek vagy belbiztonsági műveletek támogatására, illetve célzott számítógépes hálózatokhoz való hozzáférésre vagy azok megtámadására.[61]

A tárgyak internetének biztonsági sebezhetőségeiről másképpen is gondolkodhatunk, ha figyelembe vesszük az értékes tárgyakat tartalmazó otthonok vagy lakások biztonságos lezárása érdekében tett lépéseket, ha azokat felügyelet nélkül hagyják. Itt, csakúgy, mint az értékes személyes adatvagyonok esetében, a rosszul védett IoT-eszközök használata nagyjából azzal egyenértékű, mintha a ház bejárati ajtaját bezárnánk, a hátsó ajtót pedig nyitva hagynánk. Gondoljunk csak bele, milyen mértékben veszélyeztetik az otthonokat és a családokat a nem biztonságos IoT-eszközök. Streiff, Das és Cannon professzorok a következőket írják: "Az IoT-játékok érzékelői képességei más kritikus adatokkal együtt, beleértve a helymeghatározási információkat is, jelentős kockázatot hordoznak a rosszindulatú tevékenységek szempontjából. Még a helymeghatározás kiszivárgásához vezető, nem túl kifinomult támadások is problémásak lehetnek a veszélyeztetett népességcsoportok, például a gyermekek számára. A szülők számára ezek olyan kockázatok, amelyekre általában nincsenek felkészülve".[62] Bruce Sinclair jóvoltából az IoT fenyegetésvektorok grafikus illusztrációja az ábra. 3.

---

59. Lawrence J. Trautman, Remarks Presented at the Seventh Annual Conference on Governance of Emerging Technologies, Sandra Day O'Connor College of Law, Arizona State University, May 22 & (23,a2019 szerzőknél).

60. *Id.*

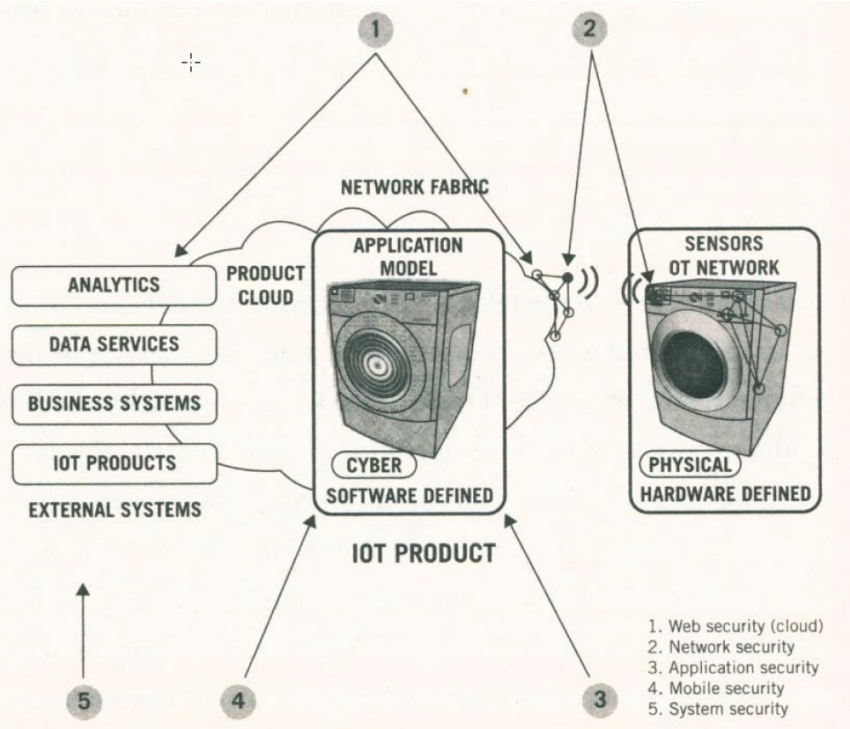
61. Coats-nyilatkozat, *Supra* note at9, 4.

62. Joshua Streiff et al., Overpowered and Underprotected Toys Empowering Parents with Tools to Protect Their Children, IEEE Humans and Cybersecurity Workshop (HACS 2019) (2019. december 12-14.).

Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

**Ábra Támadási3. vektorok az IoT-ben[63]**




## A. Adatszegések folytatódnak

Mostanra minden olvasónak tisztában kell lennie azzal, hogy a nem megfelelő adatbiztonság folyamatos veszélyt jelent.[64] Az adatbiztonság megsértésének előzményeiről, természetéről és jelenlegi fenyegetettségi profiljáról szóló átfogó vita meghaladja e cikk kereteit. Ez a cikk azonban a következő adatvédelmi incidensekre összpontosít: Target (2013. december); Yahoo (2013, de csak évekkel később jelentették); Equifax (2017); Office of Personnel Management (2015. június); Marriott Hotels (2019. január); és Capital One Financial Corp. (2019. július). Ezeket a nagy és széles körben elterjedt jogsértéseket részben azért választottuk, mert e cikk egyik szerzője úgy véli, hogy mindegyiknek áldozata volt. Ezen túlmenően a IV.G. szakasz röviden tárgyalja a Capital One Financial Corp. legalább 106 millió kártyaigénylőjét érintő, először júliusban bejelentett jogsértéssel kapcsolatos jelenlegi ismereteinket A 2019.történeti hivatkozás érdekében az ábra bemutatja a 4"bejelentett incidensek" című ábrát.

63. SINCLAIR, *Supra* note at11, (244mindezek a veszélyforrások komolyak).

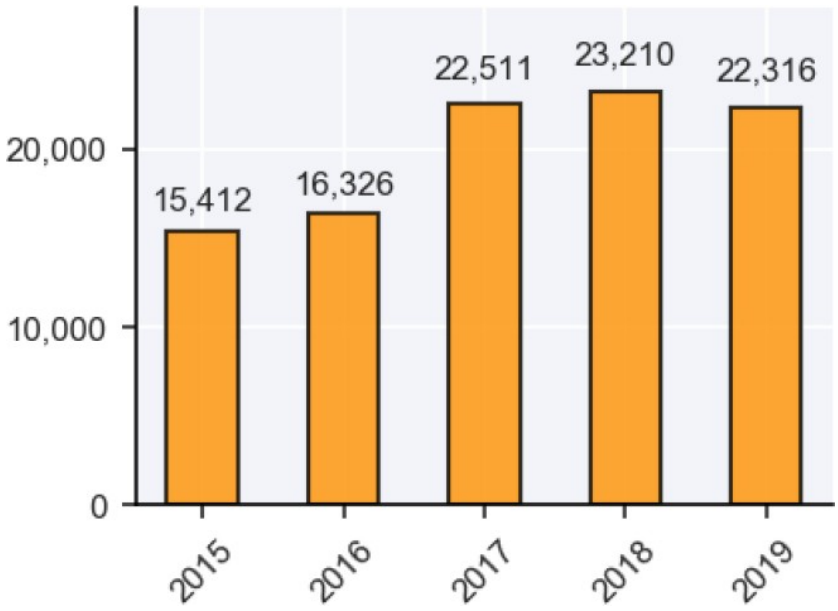
64. *Lásd* Julia Carpenter & Bouree Lam, *The Capital One Hack:* WALL ST. J., https://www.wsj.com/articles/the-capital-one-hack-life-in-the-time-of-brea ch-fatigue-11564824600 [https://perma.cc/6T9C-EN8E].



Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

a személyazonosításra alkalmas információk elvesztése, ellopása vagy kiszolgáltatottsága" a a 2014-től az év végéig tartó időszak 2019.

**Ábra A személyazonosításra alkalmas információk (PII) elvesztésével, ellopásával vagy kiszolgáltatásával kapcsolatos bejelentett4. incidensek száma[65]**




Az ábra az eddigi10 legjelentősebb jogsértések listáját mutatja5 be július óta. 2019.

**Ábra Top 5.All-Time10 Breaches júliustól kezdve 2019[66]**

1. **YAHOO (Egyesült Államok).** 2016. december 14-én jelentették, hogy egymilliárd3 rekordot sértettek meg.
2. **DU CALLER GROUP (Kína).** 2 milliárd rekord: ügyfélnevek, címek helytelenül hozzáférhetővé tétele a nyilvános telefonkönyvben, május 13-án, 2017.

65. KOCKÁZATON ALAPÚ SEC., ÉVVégi2019 jelentés: VULNERABILITÁS QUICKVIEW 1. ábra13 (2020), https://pages.riskbasedsecurity.com/hubfs/Reports/2019/2019%20Year%20End%20Vulnerability%20QuickView%20Report.pdf [https://perma.cc/XG2Y-X87D].

66. CYBER RISK ANALYTICS, 2019 MIDYEAR QUICKVIEW DATA BREACH REPORT 12 (2019), https://pages.riskbasedsecurity.com/hubfs/Reports/2019/2019%20MidYear%20Data%20Breach%20QuickView%20Report.pdf [https://perma.cc/42FK-QH2Q].



Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

3. **RIVER CITY MEDIA (Egyesült Államok).** 1,3 milliárd rekord: nevek; címek; IP-címek; e-mail hirdetési ruhák; meg nem nevezett számú pénzügyi dokumentum; chatnaplók és biztonsági mentés; hibás rsync biztonsági mentés által kitéve, 2017. március 3.
4. **NETEASE, INC, dba 163.com (Kína).** Jelentések szerint 1,2 milliárd rekordot loptak el hackerek (e-maileket, címeket és jelszavakat), és eladásra kínálták a sötét weben, 2017. január 25. .
5. **ISMERETLEN (India).** Falusi szintű vállalkozói operátorok árulnak hozzáférést az Aadhaar-adatbázishoz, 2018. január 3. 1 190 millió indiai állampolgár neve, címe, e-mail címe, születési dátuma, telefonszáma, faxszáma, neme, IP-adata és fényképe . . . Január 3,2018.
6. **VERIFICATIONS.IO (Észtország).** 982 millió név, cím, e-mail cím, születési dátum, telefonszám, faxszám, nem, IP-cím, személyes jelzáloghitel összege és FTP-szerver hitelesítő adatai, amelyek egy rosszul konfigurált adatbázis miatt kerültek az internetre. 2019. március 7.
7. **FIRST AMERICAN FINANCIAL CORPORATION (Egyesült Államok)** Körülbelül egymillió885, neveket, társadalombiztosítási számokat, telefonszámokat, e-mail és fizikai címeket, vezetői engedélyek képeit, banki adatokat, valamint jelzáloghitelezők nevét és hitelszámát tartalmazó ingatlan-zárási tranzakciós nyilvántartás került nyilvánosságra az interneten a nem biztonságos közvetlen tárgyi hivatkozások (IDOR) áramlása miatt.
8. **ISMERETLEN (Hollandia).** 711 millió rekord megsértése: e-mail címek; jelszavak; hitelesítő adatok ex- posed az interneten egy rosszul konfigurált adatbázis miatt, 2017. január 3.
9. **CULTURA COLECTIVA (Mexikó).** 540 Millió Facebook felhasználói azonosító, fióknevek, kommentek és like-ok kerültek ki az internetre egy rosszul konfigurált adatbázis miatt.
10. **YAHOO (Egyesült Államok).** 500 millió rekordot érintő betörés: felhasználónevek; e-mail címek; telefonszámok; születési dátumok; zanzásított jelszavak és biztonsági kérdések és a hozzájuk tartozó válaszok, szeptember. 22,2016.[67]

Trautman professzor valószínűnek tartja, hogy háztartását az alábbi adatvédelmi incidensek mindegyike negatívan érintette: Target (2013); Yahoo (2013); Equifax (2017); Office of Personnel Management (2015. június); Marriott (2019. január); és Capital One Financial Corp. (2019. július).

67. *Id.*



Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

## B. Cél (2013)

Az amerikai Target kiskereskedelmi vállalat arról számolt be, hogy "a 2013. november 27. és december 15. között ellopott adatok között akár 70 millió ember személyes adatai is szerepelhetnek - több mint a vállalat által eredetileg becsült 40 millió".[68] Néhány évvel később a Target beleegyezett, hogy "18,5 millió dollárt fizet 47 államnak és a Columbia körzetnek az állami főügyészekkel kötött egyezség keretében".[69] A Target összesen 300 millió dollárra becsülte a jogsértés költségeit.[70]

## C. Yahoo (2013)

Amint az 5. ábra mutatja, a Yahoo-t az a megkülönböztetés jellemzi, hogy (1) a legnagyobb amerikai adatvédelmi incidensek közül többért is felelős; és (2) a leglassabban tájékoztatja a fogyasztókat ezekről az incidensekről.[71] Amint arról Trautman és Ormerod professzorok beszámoltak, szeptemberben a Yahoo22,2016 bejelentette, hogy az adatbetörés és az információk ellopása több mint egymillió500 felhasználói fiókból történt a 2014.Úgy tűnik, hogy ez a lopás neveket, születésnapokat, telefonszámokat, e-mail címeket, "hashed jelszavakat (a túlnyomó többség bcrypt segítségével) és néhány esetben titkosított vagy titkosítatlan biztonsági kérdéseket és válaszokat tartalmazott".[72] Ez a 2014-es lopás a bejelentés idején az eddigi legnagyobb adatlopás volt.[73] A Ya- hoo továbbá közzétette, hogy meggyőződésük szerint az ellopott adatok "nem tartalmaztak védtelen jelszavakat, fizetési kártyaadatokat vagy bankszámlaadatokat".[74] Alig két hónappal azelőtt, hogy a Yahoo nyilvánosságra hozta a 2014-es adatvédelmi incidensét, bejelentették a vállalat alaptevékenységének tervezett eladását a Verizon Communicationsnek.[75] A Yahoo ezután 2016 decemberének közepén bejelentette, hogy "újabb 1 milliárd ügyfélszámla került veszélybe az eddigi legnagyobb adatbetörés rekordjának felállítása2013, során".[76]

---

68. Maggie McGrath, *Target Data Breach Spilled Info on as Many as 70 Million Customers*, FORBES (Jan. 201410,), https://www.forbes.com/sites/maggiemcgrath/2014/01/10/target-data-breach. -spilled-info-on-as-many-as-70-million-customers/#6343ee5ae795 [https://perma.cc/57H5-CWD9].

69. Rachel Abrams, *Target to Pay $18.5 Million to States 47in Security Breach Settlement*, N.Y. TIMES (2017. május 23.), https://www.nytimes.com/2017/05/23/business/target-security-breach- settlement.html [perma.cc/44GB-JVH4].

70. Vincent Lynch, *Cost of Target2013 Data Breach Nears $300 Million*, HASHEDOUT (2017. május 26.), https://www.thesslstore. com/blog/2013-target-data-breach-settled/ [https://perma.cc/L9 SD-Z6F5].

71. *Lásd* Trautman & Ormerod, *Yahoo Data Breach*, *fenti* jegyzet, 49,1233-34. o.

72. *Id.* at 1233 (idézve: Press Release, Yahoo! Inc., An Important Message to Yahoo Users on Security (Sept. 201622,), https://investor.yahoo.net/releasedetail.cfm?releaseid=990570)).

73. *Lásd* Nicole Perlroth, *Yahoo Says Hackers Stole Data on Million500 Users in2014* , N.Y. TIMES (Sept. 201622,), https://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html?_r. =0 [https://perma.cc/92KH-R7J8].

74. Suzanne Philion, *An Important Message to Yahoo Users in Security*, BUSINESSWIRE (2016. szeptember 22., 14:28), https://www.businesswire.com/news/home/20160922006198/en/Import ant-Message-Yahoo-Users-Security [https://perma.cc/SK76-E5Z7].

75. Trautman & Ormerod, *Yahoo Data Breach*, *supra* note at49, 1233.

76. *Id.* at 1233-34 (idézi Robert McMillan et al., *Yahoo Discloses New Breach of 1 Billion User Accounts*, WALL ST. J., (Dec 15, 2016, 5:19 PM), https://www.wsj.com/articles/yahoo-disclos es-new-breach-of-1-billion-user-accounts-1481753131)).



Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

## D. Equifax (2017)

Szeptemberben a globális7,2017, hitelinformációs ügynökség, az Equifax "bejelentette, hogy fogyasztói adatai egy "kibernetikai incidens" következtében veszélybe kerültek. " [77]McKay Smith és Garrett Mulrain jelentése szerint "ez az incidens egymillió 143amerikai fogyasztó, vagyis az amerikai lakosság közel százalékának45 személyazonosításra alkalmas adatainak (PII) elvesztését eredményezte".[78] Hogyan történhet ilyesmi? Úgy tűnik, hogy "[a] Belbiztonsági Minisztérium 2017. március 8-án figyelmeztette az Equifax tisztviselőit, hogy ki kell javítaniuk egy kritikus biztonsági rést a szoftverükben. A vállalat tisztviselői a riasztást belsőleg terjesztették, de nem foltozták be manuálisan az alkalmazást. Ez az egyetlen hibapont katasztrofálisnak bizonyult volna".[79]

## E. Office of Personnel Management (2015. június)

A 2015. júniusi, az Egyesült Államok Személyzeti Menedzsment Hivatalánál történt, Amerika legérzékenyebb információit tartalmazó betörés különösen nagy veszélyt jelent az amerikai nemzetbiztonságra, mivel az ellopott adatok "jelentősek voltak, mivel kifejezetten a szövetségi munkaerő biztonsági ellenőrzésére vonatkozó információkat célozták meg.... A katasztrofális kár . . . bekövetkezhet a jövőben, beleértve "a közhivatalnokok zsarolására, megszégyenítésére vagy más módon történő kényszerítésére való képességet".".[80]

## F. Marriott (2019. január)

Amint azt novemberben nyilvánosságra hozták, hackereknek30,2018, sikerült feltörniük a szállodalánc hűségprogramjának adatbázisát, és 383 millió rekordot tettek közzé: neveket, címeket, foglalási adatokat és útlevélszámokat.[81] *A The Wash- ington Post* szerint "a hackerek az elmúlt négy évben hozzáférhettek számos szállodalánc foglalási rendszeréhez, a betörés akár több millió500 ügyfél személyes adatait is felfedte, miközben aláhúzta a nyilvántartások magánjellegét, amelyek megmutatják, hogy az emberek hová és mikor utaznak - és kivel".[82]

---

77. McKay Smith & Garrett Mulrain, *Equi-Failure: The National Security Implications of the Equifax Hack and a Critical Proposal for Reform*, J9. NAT'L SEC. L. & POL'Y (5492018); *lásd még* Scott J. Shackelford & Austin E. Brady, *Is It Time for A National Cybersecurity Safety Board? Examining the Policy Implications and Political Pushback*, ALB28. L.J. SCI. & TECH. 56 (2018).

78. Smith & Mulrain, *supra* note at77, (554idézi Spencer Kimball & Liz Moyer, *Equifax Data Breach May Affect Million 2.5More Consumers Than Original Stated*, CNBC (Oct. 20172,), https://www.cnbc. com/2017/10/02/equifax-2-point-5-point-5-million-more-consumers-may-be-affected- by-data-breach-than-originally-stated.html [https://perma.cc/C5MK-2ES6]).

79. *Id*. 555.

80. *Id*. 563.

81. Taylor Telford & Craig Timberg, *Marriott Discloses Massive Data Breach Affecting Up to 500 Million Guests*, WASH. POST (2018. november 30.), https://www.washingtonpost.com/business/20 18/11/30/marriott-discloses-massive-data-breach-impacting-million-guests/?noredirect=on [https://pe rma.cc/N2VF-9DJ3].

82. *Id.*



Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

## G. Capital One Financial Corp. (2019. július)

Az Egyesült Államok ötödik legnagyobb hitelkártya-kibocsátója, a Capital One Financial Corp. 2019. július végén jelentette, hogy legalább 106 millió kártyabirtokos és igénylő adatait sértették meg.[83] Az ilyen adatszivárgások vállalatokat érintő költségeit jelzi, hogy a Capital One Financial Corp. törzsrészvényeinek értéke a bejelentés napján, 2019. július 30-án 5,9 százalékos csökkenéssel zárt.[84] *A Wall Street Journal* beszámolója szerint "Paige A. Thompson, az Amazon.com Inc. felhőalapú számítástechnikai egységének volt alkalmazottja letartóztatása. " [85]*A Wall Street Journal* története azzal folytatódik, hogy "úgy tűnik, hogy az eddigi legnagyobb banki adatrablások során egy olyan felhőben lévő sebezhetőséget használtak ki, amelyre biztonsági szakértők évek óta figyelmeztetnek".[86]

## H. Ransomware

A több milliárd IoT-érzékelő a zsarolóvírus-támadások átjárója? Trautman és Ormerod professzorok2018, a zsarolóvírusok történetéről és fejlődéséről részletes beszámolót adtak, [87]és ezt itt nem ismételjük meg. A Szövetségi Nyomozó Iroda (FBI) meghatározása szerint a zsarolóvírus a következő

> egy olyan típusú rosszindulatú szoftver, amely egy számítógépre vagy szerverre telepítve titkosítja a fájlokat, így azok hozzáférhetetlenné válnak, amíg a megadott váltságdíjat ki nem fizetik. A zsarolóprogramokat általában akkor telepítik, amikor a felhasználó rákattint egy rosszindulatú linkre, megnyit egy fájlt egy e-mailben, amely telepíti a rosszindulatú programot, vagy egy veszélyeztetett webhelyről történő drive-by letöltés (amely nem igényel felhasználói telepítést) révén.[88]

Az FBI azt állítja továbbá, hogy "[h]ospitáliák, iskolai körzetek, állami és helyi kormányzatok, bűnüldöző szervek, kisvállalkozások, nagyvállalatok - ezek csak néhány a zsarolóprogramok által érintett szervezetek közül.

---

83. Stacy Cowley & Nicole Perlroth, *Capital One Breach Shows a Bank Hacker Needs Just One Gap to Wreak Havoc*, N.Y. TIMES (2019. július 31.), https://www.nytimes.com/2019/07/30/busi ness/bank-hacks-capital-one.html [perma.cc/L79T-D858]; Nicole Hong et al., *Capital One Reports Data Breach Affecting Million10 Customers, Applicants*, WALL ST. J., https://www.wsj.com/article s/capital-one-reports-data-breach-11564443355 [perma.cc/V8T4-82HX].

84. Gunjan Banerji, *Capital One Shares Fall Nearly 6% After Breach*, WALL ST. J., https:// www.wsj.com/articles/capital-one-shares-plummet-after-breach-11564500956 [perma.cc/6V5D-UH YU].

85. Robert McMillan, *How the Accused Capital One Hacker Stole Reams of Data from the Cloud*, WALL ST. J., https://www.wsj.com/articles/how-the-accused-capital-one-hacker-stole-reams-of-data-from-the-cloud-11564911001 [perma.cc/6B25-JV5S]; *lásd még* Dana Mattioli et al., *Hacking Suspect Left Trail of Clues Online*, WALL ST. J. (2019. július 31., 20:31), https://www. wsj.com/ articles/capital-one-hacking-suspect-showed-strange-online-behavior-11564533092 [perma.cc/5FCD- XJEC].

86. McMillan, *Supra* note 85.

87. *Lásd* Trautman & Ormerod, *Supra* note. 13.

88. *A zsarolóvírus áldozatait felszólították, hogy jelentse a fertőzést a szövetségi bűnüldöző szerveknek, I. számú riasztás -091516-PSA*, SZÖVETSÉGI. BUREAU INVESTIGATION https://www.ic3.gov/media/2016/160915.aspx [https: //perma.cc/XK29-Z5SU].



Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

olyan szoftver, amely titkosítja vagy zárolja az értékes digitális fájlokat, és váltságdíjat követel azok visszabérléséért. "[89] Az Egyesült Államok Belbiztonsági Minisztériumának Kiberbiztonsági és Infrastruktúra Biztonsági Ügynöksége figyelmeztet: "A zsarolóvírusok nem csak otthoni felhasználókat céloznak; a vállalkozások is megfertőződhetnek zsarolóvírusokkal, ami negatív következményekkel járhat, beleértve az érzékeny vagy védett információk ideiglenes vagy végleges elvesztését, a rendszeres működés megzavarását, a rendszerek és fájlok helyreállítása miatt felmerülő pénzügyi veszteségeket, valamint a szervezet hírnevének esetleges károsodását." A zsarolóvírusok nem csak az otthoni felhasználókat támadják meg.[90] Vegyük figyelembe, hogy "[az] [ilyen típusú szervezetek által tárolt] fontos adatokhoz való hozzáférés ellehetetlenülése katasztrofális következményekkel járhat az érzékeny vagy védett információk elvesztése, a rendszeres működés megszakítása, a rendszerek és fájlok helyreállítása során felmerülő pénzügyi veszteségek, valamint a szervezet hírnevének esetleges károsodása szempontjából.".[91] Az FBI arra figyelmeztet, hogy "[a] zsarolóvírus-támadás során az áldozatok - miután meglátnak egy nekik címzett e-mailt - megnyitják azt, és rákattinthatnak egy olyan mellékletre, amely legitimnek tűnik, például egy számla vagy egy elektronikus fax, de amely valójában a rosszindulatú zsarolóvírus kódját tartalmazza".[92] Az FBI megjegyzi, hogy "az e-mail tartalmazhat egy legitimnek tűnő weboldal címet is, de amikor az áldozat rákattint, egy olyan weboldalra jut, amely rosszindulatú szoftverrel fertőzi meg a számítógépét".[93] Az FBI továbbá megállapítja:

> Amint a fertőzés jelen van, a kártevő elkezdi titkosítani a helyi meghajtókon, a csatlakoztatott meghajtókon, a mentési meghajtókon és potenciálisan az ugyanazon a hálózaton lévő más számítógépeken lévő fájlokat és mappákat [amelyekhez az áldozat számítógépe csatlakozik]. A felhasználók és a szervezetek általában nem tudnak a fertőzésről, amíg nem tudnak többé hozzáférni az adataikhoz, vagy amíg számítógépes üzeneteket nem látnak, amelyek a támadásról tájékoztatják őket, és váltságdíjat követelnek a visszafejtő kulcsért cserébe. Ezek az üzenetek tartalmazzák a váltságdíj kifizetésének módjára vonatkozó utasításokat, általában bitcoinokkal, mivel ez a virtuális valuta anonimitást biztosít.[94]

A rosszindulatú és költséges zsarolóvírus-támadások naponta folytatódnak, többek között Atlanta, [95]Baltimore [96]és sok más város polgárai számára is jelentős fennakadásokat okozva.[97] Folyamatosan új zsarolóvírus-támadásokat találnak. Januárban például Ravi Gidwani biztonsági22,2020, szakértő arról számolt be, hogy "egy csúnya és egyszeri

---

89. *Mit vizsgálunk:* FBI. GOV, https://www.fbi.gov/investigate/cyber [https: //perma.cc/TB33-R2KY].

90.*Lásd a WannaCry Ransomware-rel kapcsolatos jelek (TA17-132A)*, DEP'T HOMELAND SEC. (2017. május 12.), https://www.us-cert.gov/ncas/alerts/TA17-132A [https://perma. cc/V8P4-9KUW] (a felsorolásban szereplő pontok kihagyva).

91. *Mit vizsgálunk:* Megjegyzések: *Kiberbűnözés*, *supra* note 89.

92. *Id.*

93. *Id.*

94. *Id.*

95. *Lásd pl.* , Press Release, The U.S. Attorney's Office N. Dist. of Ga., Atlanta U.S. Attorney Charges Iranian Nationals for City of Atlanta Ransomware Attack (2018. december 5.), https://www. justice.gov/usao-ndga/pr/atlanta-us-attorney-charges-iranian-nationals-city-atlanta-ransomware-att ack [https://perma.cc/BET3-QBTE].

96.*Lásd pl.* , Niraj Chokshi, *Hackers Are Holding Baltimore Hostage: How They Struck and What's Next*, N.Y. TIMES (May 22, 2019), https://www. nytimes.com/2019/05/22/us/baltimore-ran somware.html [https://perma.cc/S8PC-NE4P].

97. *Lásd* Trautman & Ormerod, *supra* note at39, 507.



Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

típusú zsarolóprogram, amely a Node.js keretrendszert használja, amely lehetővé teszi, hogy megfertőzze a
Windows alapú operációs rendszer."[98] Ez azért jelentős, mert

> A Node.js egy nyílt forráskódú, platformokon átívelő JavaScript futtatási környezet, amely a JavaScript kódot a böngészőn kívül hajtja végre. A V8-as JavaScript motorra épül. A Google nyílt forráskódú, nagy teljesítményű, C++ nyelven írt JavaScript és WebAssembly motorjára. Ezt használja többek között a Chrome és a Node.js is. ECMAScriptet és WebAssemblyt valósít meg, és Windows 7 vagy újabb Windows 7, macOS 10.12+ és Linux rendszereken fut, amelyek x64, IA-32, ARM vagy MIPS processzorokat használnak. A V8 önállóan is futtatható, vagy bármely C++ alkalmazásba beágyazható. Érdekes módon a felhasználók könnyen megfertőződhetnek ezzel a Nodera zsarolóprogrammal online böngészés közben, akár egy rosszindulatú HTA fájlra kattintva, akár malvertisementként kiszolgáltatva.[99]

Tim Trautman szoftvermérnök szerint ez azért lehet jelentős, mert mint JavaScript keretrendszer. Elmagyarázza: "A Node-ot nagyon nagy közösség veszi körül. A Node-on futó Ransomware növelheti a Ran- somware-támadások elterjedtségét azáltal, hogy csökkenti a technikai belépési korlátot a szoftvermérnökök sokkal nagyobb / technikailag kevésbé jártas csoportja számára".[100] Az V. rész a Mirai néven ismert, különösen bomlasztó malware fenyegetés vizsgálatát tartalmazza.

## V. MIRAI BOTNET

Az Akamai arról számolt be, hogy 2016 júniusában elkezdett nyomon követni egy olyan kártevő törzset, amely IoT-eszközöket és otthoni internetes routereket céloz meg.[101] Nem sokkal később ez a Mirai néven futó kártevő világszerte elterjedt.[102] Elie Bursztein újságíró a Mirai-támadást azért tartja különösen figyelemre méltónak, mert "kis, ártalmatlan Internet-of-Things (IoT) eszközökön, például otthoni routereken, levegőminőség-mérőkön és személyes megfigyelő kamerákon keresztül hajtották végre. A Mirai a csúcspontján több mint sebezhető600,000 IoT-eszközt fertőzött meg".[103] Ahogy Bursztein kifejti,

> A Mirai alapvetően egy önterjesztő féreg... egy rosszindulatú program, amely úgy szaporodik, hogy sebezhető IoT-eszközöket talál, támad meg és fertőz meg. . . .
>
> A replikációs modul felelős a botnet méretének növeléséért azáltal, hogy minél több sebezhető IoT-eszközt rabszolgává tesz. Ezt úgy éri el, hogy (véletlenszerűen)

98. Ravi Gidwani, Az *első Note.js alapú Ransomware: Nodera*, QUICKHEAL. COM (Jan. 22, 2020), https://blogs.quickheal.com/first-node-js-based-ransomware-nodera/ [https://perma.cc/2TDE-ATCW].

99. *Id.*

100. Tim Trautman e-mailje Lawrence J. Trautmannek (Jan. 1522,2020,:03 CST) (a szerzőknél).

101. *Lásd* AKAMI TECHNOLOGIES, INC., AKAMAI'S [STATE OF THE INTERNET] / SECURITY: Q3 2016 REPORT 6 (Martin McKeay szerk., 2016), https://www.akamai.com/us/en/multimedia/documents/ state-of-the-internet/q3-2016-state-of-the-internet-security-report.pdf [https://perma.cc/5NTL-397S].

102. *Id.*

103. Elie Bursztein, *A hírhedt Mirai IoT botnet belsejében: A Retrospective Analysis*, CLOUDFLARE BLOG (Dec. 1214,2017,:41 PM), https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/ [https://perma.cc/CSQ9-F4SR].



Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

> az egész internetet átvizsgálják a lehetséges célpontok után kutatva és támadva. Amint egy sebezhető eszközt talál, a modul jelenti azt a C&C szervereknek, hogy megfertőzze a legújabb Mirai hasznos terheléssel. . . .
>
> A Mirai kezdeti verziója az eszközök megtámadásához kizárólag az IoT-eszközök által gyakran használt 64 jól ismert alapértelmezett bejelentkezési/jelszó-kombinációból álló rögzített készletre támaszkodott. Bár ez a támadás nagyon alacsony technológiai színvonalú volt, rendkívül hatékonynak bizonyult. [104]

Az Akamai megjegyzi, hogy az IoT-eszközök és egyéb képességek használata általában nem
a botnetekben találhatóak teszik a Mirai-t "igazán kivételessé, különösen a Generic Routing Encapsulation (GRE) alapú támadások, a támadási forgalom különböző szintű testreszabása és a telnet szkennelés. Ezen túlmenően, a támadásokat közvetlenül a Mirai által generált
a forráskód nyilvános kiadásáig valószínűleg új, jobb képességű, jobb minőségű Mirai változatai a közeljövőben."[105] Továbbá, Akami jelenti:

> A Mirai egy olyan botnet, amely nem létezne, ha több hálózat gyakorolná az alapvető higiéniát, például a nem biztonságos protokollok alapértelmezett blokkolását. Ez nem újdonság - a 2011-es és 2012-es Brobot-támadásokban is hasonló hálózati higiéniai problémákat láttunk a fertőzés forrásaként. A botnet féregként terjed, a telnet és több mint 60 alapértelmezett felhasználónév- és jelszó-kombináció segítségével szkenneli az internetet további megfertőzendő rendszerek után kutatva. Úgy tűnik, hogy e rendszerek többsége digitális videófelvevő (DVR), ip-kompatibilis megfigyelő kamerák és fogyasztói routerek. Miután egy rendszer megfertőződött, csatlakozik a botnet parancsnoki és vezérlési (C2) struktúrájához, majd folytatja a többi sebezhető rendszer keresését, miközben támadási parancsokra vár.[106]

2018 májusában az Egyesült Államok kereskedelmi és belbiztonsági minisztériuma közösen közzétette *a Jelentés az elnöknek az internet és a kommunikációs ökoszisztéma ellenálló képességének fokozásáról a botnetek és más elosztott fenyegetések ellen című dokumentumot (A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Au- tomated, Distributed Threats).*[107] Ez a kiadvány az érdekelt ügynökségekkel folytatott konzultációk eredménye volt, többek között: "a védelmi, az igazságügyi és a külügyminisztériummal, a Szövetségi Nyomozó Irodával, az ágazati ügynökségekkel, a Szövetségi Hírközlési Bizottsággal és a Szövetségi Kereskedelmi Bizottsággal".[108] Az IoT-eszközök gyors növekedésének eredményeként a jelentés megjegyzi, hogy "a DDoS [distributed denial of service] támadások mérete több mint egy terabit/másodpercre nőtt, ami messze meghaladja a várt méretet és a többletkapacitást. Ennek eredményeként az ilyen típusú támadásokból való helyreállítási idő túl lassú lehet, különösen, ha misszió-kritikus szolgáltatásokról van szó".[109] Ezeket az automatizált és elosztott támadásokat (pl. botnetek) "különféle rosszindulatú tevékenységekre használják, amelyek túlterhelik a

---

104. *Id.*

105. AKAMI TECHNOLOGIES, INC.,, *fenti* megjegyzés
.101,15 106. *Id.* at 15-16.

107. U.S. DEP'T OF COMMERCE & U.S. DEP'T OF HOMELAND SEC., A REPORT TO THE PRESIDENT ON ENHANCING THE RESILIENCE OF THE INTERNET AND COMMUNICATIONS ECOSYSTEM INHILIENCE OF BOTNET AND OTHER AUTOMATED, DISTRIBUTED THREATS (2018), https://csrc.nist.gov/ CSRC/media/Publications/white-paper/2018/05/30/enhancing-resilience-against-botnets--report-to.
-the-president/final/documents/eo_13800_botnet_report_-_finalv2.pdf [https://perma.cc/549A-S4G3].

108. *Id*. 3.

109. *Id*. 5.

Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

hálózati erőforrások, tömeges mennyiségű spam küldése, keylogger és egyéb rosszindulatú programok terjesztése; botnetek által terjesztett zsarolóprogram-támadások, amelyek túszul ejtik a rendszereket és az adatokat."[110] A jelentés továbbá megállapítja, hogy "[a] hagyományos DDoS-csökkentési technikák, például a hálózati szolgáltatók többletkapacitást építenek ki a botnetek hatásainak elnyelésére, a várható méretű botnetek elleni védelemre szolgálnak ... . [de] nem a botnetek által elősegített egyéb rosszindulatú tevékenységek, például a zsarolóprogramok vagy a számítógépes propaganda orvoslására tervezték".[111] Megjegyzi továbbá, hogy

> [A Mirai botnetből 2016 őszén indított DDoS-támadások például olyan szintű tartós forgalmat értek el, amely számos elterjedt DDoS-csökkentő eszközt és szolgáltatást túlterhelt, sőt, még egy olyan DNS-szolgáltatást is megzavart, amely számos DDoS-csökkentő stratégia általánosan használt eleme volt. Ez a támadás rávilágított a fogyasztói IoT-eszközökben rejlő növekvő bizonytalanságokra és fenyegetésekre is. Mivel új technológiáról van szó, az IoT-eszközöket gyakran fontos biztonsági funkciók és gyakorlatok nélkül építik és telepítik. Míg az eredeti Mirai-változat viszonylag egyszerű volt, és az eszközök gyenge jelszavait használta ki, a későbbiekben egyre kifinomultabb botnetek alakultak ki; a Reaper botnet például ismert kódsebezhetőségeket használ fel az eszközök hosszú listájának kihasználására, az egyik legnagyobb DDoS-támadás pedig a közelmúltban a viszonylag ismeretlen MemCacheD szoftverben újonnan felfedezett sebezhetőséget használta ki. Ezek a példák világosan mutatják az ilyen méretű és kiterjedésű botnetek által jelentett kockázatokat, valamint a jövőbeni támadások várható innovációját és növekvő méretét és összetettségét.[112]

2016 decemberében az oknyomozó kiberriporter, Brian Krebs kiadott egy történetet, amelyben megjegyezte,

> A héten közzétett új kutatások rengeteg új takarmányt adhatnak a Mi- rai számára, egy olyan rosszindulatú programtörzs számára, amely a rosszul védett tárgyak internetének (IoT) de- vices-ét rabszolgává teszi, hogy erőteljes online támadásokban használja fel. Ausztriai kutatók több mint 80 különböző IP-kameramodellben fedeztek fel egy pár hátsó ajtót a Sony Corp. Külön izraeli biztonsági szakértők triviálisan kihasználható gyengeségeket fedeztek fel közel félmillió fehér címkével ellátott IP-kameramodellben, amelyeket a Mirai jelenleg nem keres.[113]

## VI. IoT-fenyegetettségi vektorok válság idején

A válság idején jelentkező kormányzási kihívások az elmúlt években számos tudományos kutatás középpontjában álltak.[114] Mielőtt a tárgyak internetének válsághelyzetben való sebezhetőségével foglalkoznánk, fontos a tárgyak internetének rendszere sebezhetőségének munkadefiníciója, valamint a válsághelyzet kontextusának rövid tárgyalása.

---

110. *Id.*
111. *Id.*
112. *Id.* 6-7.
113. Brian Krebs, *Researchers Find Fresh Fodder for IoT Attack Cannons*, KREBS ON SECURITY (2016. december 6., 10:22), https://krebsonsecurity.com/2016/12/researchers-find-fresh-fodder-for-iot-attack-cannons/ [https://perma.cc/G326-PPMA].
114. *Lásd általában* Trautman, *Crisis Governance*, 55. lábjegyzet; JOHN ARMOUR ET AL ,„PRINCIPLES OF FINANCIAL REGULATION 370-90 (2016) (banki kormányzás); Kenneth A. Bamberger,



Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

## A. IoT rendszer sebezhetőség

Amint azt a II. részben tárgyaltuk, a tárgyak internettel összekapcsolt eszközök hatalmas hálózata. Ezek az eszközök vezeték nélküli kapcsolatokon keresztül lépnek kapcsolatba egymással, hogy emberi beavatkozás nélkül hozzanak létre, cseréljenek ki és továbbítsanak adatokat. Mohamed Abomhara és Geir M. Køien a tárgyak internetének sebezhetőségét úgy definiálja, mint a tárgyak internetének rendszerében vagy annak kialakításában található gyengeségeket, amelyek lehetővé teszik a behatolók számára, hogy parancsokat hajtsanak végre, jogosulatlan adatokhoz férjenek hozzá, és szolgáltatásmegtagadási támadásokat hajtsanak végre.[115] A sebezhetőségek lehetnek az IoT-hardver vagy -szoftver hibái, az IoT-rendszerekben alkalmazott irányelvek és eljárások gyengeségei, vagy az IoT-rendszerekkel való visszaélés a felhasználók részéről.[116]

## B. Válságkörnyezet

Az Egészségügyi Világszervezet (WHO) meghatározása szerint a katasztrófa minden olyan előre nem látható esemény, amely olyan mértékű kárt, pusztítást, ökológiai zavart, emberi életek elvesztését, emberi szenvedést, valamint az egészség és az egészségügyi szolgáltatások romlását okozza, amely az érintett közösségen túlmutató reagálási erőfeszítéseket igényel.[117] A természeti katasztrófák minden évben jelentős gazdasági veszteségeket és társadalmi hatásokat okoznak. Az egyre növekvő népességgel és infrastruktúrával a világ katasztrófákkal kapcsolatos veszélyeknek való kitettsége egyre nő. A katasztrófahelyzetek változékonyak és

---

*Megfelelési technológiák:* TEX. L. REV. 669 (2010); ASWATH DAMODARAN, RISK MANAGEMENT: A CORPORATE GOVERNANCE MANUAL (Sept. 23,
2010); Andrew Ellul, *The Role of Risk Management in Corporate Governance*, 7 ANN. REV. FIN. ECON. 279 (2015); Lawrence O. Gostin & Eric Friedman, *Ebola: A Crisis in Global Health Leadership*, 384 LANCET 1323 (2014) (számos azonos irányítási kérdés vonatkozik a COVID-19 világjárványra és a széles körű kiberkockázatra); Michelle M. Harner, *Ignoring the Writing on the Wall: The Role of Enterprise Risk Management in the Economic Crisis*, J5. BUS. & TECH. L. (452010); Louis- Marie Ngamassi Tchouakeu et al., *Exploring Barriers to Coordination Between Humanitarian NGOs: A Comparative Case Study of Two NGO's Information Technology Coordination Bodies*, *in:* INFORMATION SYSTEMS AND MODERN SOCIETY: SOCIAL CHANGE AND GLOBAL DEVELOPMENT.
87-112 (John Wang szerk., 2013) (vizsgálja és tárgyalja a humanitárius nem kormányzati szervezetek (NGO-k) információs és kommunikációs technológiai (ICT) koordinációs szervein belüli koordinációs kihívásokat); Michael Pirson & Shann Turnbull, *Corporate Governance, Risk Management, and the Financial Crisis-An Information Processing View* (Fordham U. Sch. Bus., Working Paper No. 2011-003, 2010); Usha Rodrigues, *Corporate Governance in an Age of Separation of Ownership from Ownership*, 95 MINN. L. REV. 1822 (2011); Paul Rose, *Regulating Risk by 'Strengthening Corporate Governance'*, CONN17. INS. L.J. (2010); Andrea H. Tapia és mások, *Coordinating Humanitarian Information: The Problem of Organizational and Technical Trajectories*, 25 J. INFO. TECH. & PEOPLE 240 (2012) (két humanitárius információs koordinációs szervet vizsgál, amelyek mindketten azzal foglalkoznak, hogy a humanitárius segítségnyújtásban részt vevő több szervezet számára mechanizmusokat találjanak az információs technológia és az irányítás körüli erőfeszítések összehangolására).

115. *Lásd* Mohamed Abomhara & Geir M. Køien, *Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks*, 4(1) J. CYBER SEC. & MOBILITY 65 (2015).

116. *Id.*

117. *Lásd:* WORLD HEALTH ORG., COMMUNITY EMERGENCY PREPAREDNESS: A MANUAL FOR MANAGERS AND POLICY-MAKERS (1999), http://whqlibdoc.who.int/publications/9241545194.pdf [https://perma.cc/UNG4-6K9Y].



Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

gyakran nem rutinszerű cselekvéseket eredményeznek.[118] Katasztrófák idején a tudás deficitje a normális helyzetekhez képest rendkívül eltérő, és az embereknek néha improvizálniuk kell, hogy megfeleljenek a válsághelyzetre való reagálás szempontjából kritikus feltételeknek. A katasztrófavédelemnek időnként kevés vagy semmilyen információ alapján kell döntéseket hoznia. A katasztrófák fő jellemzői a kiszámíthatatlanság, a korlátozott erőforrások elérhetősége az érintett területeken és a környezet dinamikus változásai.[119] A katasztrófák során az emberekre és az infrastruktúrára gyakorolt hatásokat nem lehet pontosan megjósolni.

A katasztrófavédelem olyan tervek kidolgozását foglalja magában, amelyek segítségével az emberek csökkenthetik a veszélyekkel szembeni sebezhetőségüket és megbirkózhatnak a katasztrófákkal. A katasztrófák kezelése során az egymás mellett vagy földrajzilag szétszórtan elhelyezkedő érdekelt feleknek együtt kell működniük a hatékony és eredményes katasztrófaelhárítás érdekében. Az információs és kommunikációs technológiák döntő szerepet játszanak a katasztrófakezelési életciklus minden egyes szakaszában (felkészültség, reagálás, helyreállítás, enyhítés).[120] A közelmúlt technológiai fejlődésével a tárgyak internetének megvan a lehetősége arra, hogy a katasztrófavédelem és -elhárítás egyik legfontosabb alaptechnológiájává váljon.[121] Akash Sinha és munkatársai a következő három fő alkalmazási területet határozzák meg a tárgyak internetének a katasztrófavédelemben: (1) a katasztrófakockázat minimalizálása és megelőzése - a katasztrófaesemények műholdas kommunikációval történő nyomon követése, korai figyelmeztető rendszerek kialakítása, a közösségi média használata a helyzetfelismerés érdekében; (2) katasztrófaelhárítás - valós idejű kommunikáció a hatékony és időben történő segélyezési műveletek érdekében; és (3) katasztrófaelhárítás - eltűnt személyek online keresése és pénzkezelési rendszerek. A tárgyak internete felhasználható a megelőző karbantartás és javítás megtervezésére is; annak értékelésére, hogy a szerkezetek képesek-e ellenállni egy közelgő időjárási eseménynek, miközben a normál működést folytatják, és lezárják a nem biztonságos eszközöket.[122] A katasztrófahelyzet dinamikus jellege megköveteli, hogy minimális idő alatt tudatos és pontos döntéseket lehessen hozni. Az IoT-technológia, amely képes azonnali információfrissítésre, kulcsszerepet játszhat a dinamikus munkafolyamatok adaptációjának megvalósításában.[123]

---

118. *Lásd* Jeannette Sutton et al., *Backchannels on the Front Lines: Emergent Uses of Social Media in the 2007 Southern California Wildfires*, *in* PROCEEDINGS OF THE 5TH INTERNATIONAL ISCRAM CONFERENCE-WASHINGTON, DC (2008).

119. *Lásd* ManzhuYu et al., *Big Data in Natural Disaster Management: A Review*, GEOSCIENCES, May 2018, art. no. 165.

120. *Lásd általában* Louis Ngamassi et al., *Use of Social Media for Disaster Management: A Prescriptive Framework*, J. ORGANIZATIONAL & END USER COMPUTING, July-Sept. 2016, 122. o.; Louis Ngamassi et al., *Examining the Role of Social Media in Disaster Management from an Attribution Theory Perspective*, *in* PROCEEDINGS OF THE 13TH INT'L CONFERENCE ON INFO. SYS. FOR CRISIS RESPONSE & MGMT. (ISCRAM)-RIO DE JANEIRO, BRAZIL (2016. május 22-25.); Louis Ngamassi et al., *Social Media Visual Analytic Toolkits for Disaster Management: A Review of the Literature*, *in* PROCEEDINGS OF THE 14TH INT'L CONFERENCE ON INFO. SYS. FOR CRISIS RESPONSE & MGMT. (ISCRAM)-ALBI, FRANCIAORSZÁG 785-97 (2017. május 21-24.).

121. *Lásd általában* Akash Sinha et al., *Impact of Internet of Things (IoT) in Disaster Management: A Task-Technology Fit Perspective*, ANNALS283 OPERATIONS RES. 759 (2019).

122. *Id*. 763.

123. *Id.*



Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

## C. IoT sebezhetőség válság idején

Bár a tárgyak internete óriási lehetőségeket rejt magában a katasztrófavédelem számára, válság idején számos kihívással is jár. Az olyan nagyszabású természeti katasztrófák, mint a 2004-es dél-ázsiai cunami, a 2005-ös Katrina hurrikán, a 2010-es haiti földrengés és a 2017-es Harvey hurrikán az információs és kommunikációs technológiai infrastruktúrák tömeges pusztulásához vezettek, és rávilágítottak a tárgyak internetének sebezhetőségére.[124] Válság idején az IoT-rendszerek néhány fő sebezhetősége a rendszerek interoperabilitásához és a rendszerek összekapcsolhatóságához kapcsolódik - két fontos fogalom az IoT-paradigmában.

Az IoT-rendszerek a különböző összekapcsolt objektumok interoperabilitására épülnek. Az IoT-objektumok az interneten keresztül intelligens módon lépnek kapcsolatba más eszközökkel. Válsághelyzetben ezen eszközök egy része valószínűleg tönkremehet, ami jelentősen akadályozhatja az IoT-rendszer hatékony működését. Ezért minél több tárgy van összekapcsolva egy IoT-rendszeren keresztül, annál nagyobb a lehetősége annak, hogy válsághelyzetben zűrzavar alakuljon ki. Ráadásul az IoT-szolgáltatások, mint például a folyamatautomatizálás, az eszközkezelés és a döntéshozatal, általában a felhőben vannak elhelyezve, hogy a felhasználók bármikor és bárhol hozzáférhessenek az IoT-eszközökhöz. Ha az internetes infrastruktúra katasztrófa esetén megsemmisül, az IoT-szolgáltatások nem lesznek elérhetőek a felhasználók számára. Az olyan technológiai fejlesztések, mint a "tartalomközpontú hálózat (Content-Centric Networking, CCN) ígéretes hálózati paradigmává vált, amely kielégíti a gyors csomagszállítás követelményeit az IoT vészhelyzeti alkalmazásai számára".[125]

# VII. GYÁRTOTT FELHASZNÁLÁSI LEÍRÁS (SÁR) MÓDSZERTANA

A NIST megjegyzi: "Sajnos az IoT-eszközökből gyakran hiányoznak a hatékony és eredményes funkciók, amelyeket az ügyfelek a kiberbiztonsági kockázatok mérséklésére használhatnak".[126] A NIST belső jelentése figyelmeztet8259:

> Következésképpen egyes IoT-eszközök kevésbé könnyen biztosíthatók az ügyfelek korábbi módszereivel, mivel az általuk elvárt kiberbiztonsági funkciók nem feltétlenül állnak rendelkezésre az IoT-eszközökön, vagy másképp működnek, mint ahogy az a hagyományos IT-eszközök alapján elvárható. Ez azt jelenti, hogy az IoT-eszközök ügyfeleinek további vagy új kiberbiztonsági ellenőrzéseket kell kiválasztaniuk, bevezetniük és kezelniük, vagy módosítaniuk kell a már meglévő ellenőrzéseket. Előfordulhat azonban, hogy a kockázatoknak a korábbiakkal azonos szintű csökkentését szolgáló új vagy testre szabott ellenőrzések nem minden ügyfél számára állnak rendelkezésre, illetve nem minden IoT-eszközzel valósíthatók meg. Ezt a problémát súlyosbítja, hogy az ügyfelek nem feltétlenül tudják, hogy a tárgyak internetéhez igazodva módosítaniuk kell meglévő informatikai folyamataikat. Az eredmény az, hogy sok IoT-eszköz nincs megfelelően biztosítva, így a támadók könnyebben kompromittálhatják azokat, és felhasználhatják arra, hogy kárt okozzanak az eszköz ügyfeleinek és

124. *Lásd* Trautman, *Crisis Governance*, *Supra* note at55, 338.

125. Fawaz Alassery, *Fast Packet Delivery Techniques for Urgent Packets in Emergency Applications of Internet of Things*, INT'L J. COMP. NETWORKS & COMM .,May at 2019,33.

126. *Lásd* FAGAN ET AL., *fenti* megjegyzés 4,vii. pontjában.

Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

> további aljas cselekedeteket (pl. elosztott szolgáltatásmegtagadási [DDoS] támadásokat) hajtanak végre más szervezetek ellen.[127]

Mivel az IoT-piacon a szabványosítás hiánya számos kibertámadáshoz és interoperabilitási problémához vezetett, az iparág kezdeti megoldásaként kifejlesztették a gyártott használati leírást (Manufactured Usage Description, MUD).[128] A nemzetközi szabványügyi testület, az Internet Engineering Task Force (IETF) márciusban2019 a MUD-szabványtervezetet egy kvázi elfogadott RFC 8520-as javasolt szabványba helyezte át.[129] Az RFC 8520 kiadására válaszul a Nemzeti Szabványügyi és Technológiai Intézet (NIST) kiadta a NIST Special Publication (NIST SP) 1800-15: Securing Small-Business and Home Internet of Things (IoT) De- vices-Mitigating Network-Based Attacks Using Manufacturer Usage Descrip- tion (MUD) tervezetét.[130] A NIST az Egyesült Államok kormányának a kiberbiztonsági szabványokkal foglalkozó szabványügyi testülete.[131] A dokumentum a következőképpen írja le a MUD-ot és annak célját:

> Az Internet Engineering Task Force MUD-architektúra (MUD - manufacturer usage descrip- tion) célja, hogy a tárgyak internete (IoT) eszközei úgy viselkedjenek, ahogyan azt az eszközök gyártói tervezték. Ez úgy érhető el, hogy a gyártók számára szabványos módot biztosítanak az egyes eszközök típusának azonosítására, valamint a tervezett funkciójuk ellátásához szükséges hálózati kommunikáció megjelölésére. A MUD használata esetén a hálózat automatikusan engedélyezi, hogy az IoT-eszköz a tervezett módon működjön, és a hálózat megtiltja az eszköz minden más viselkedését.[132]

Az otthonokban és kisvállalkozásokban használható, MUD-képes IoT-eszközök megnehezítik a rosszindulatú szereplők számára, hogy ezeket az IoT-eszközöket DDoS-támadások indítására használják az interneten keresztül.[133] A NIST kifejti, hogy "a MUD szabványos módszert biztosít arra, hogy a hozzáférés-szabályozási információk a hálózatvezérlő de- víziók számára elérhetővé váljanak".[134] A DDoS-támadások meghiúsulnak "az IoT-eszközökre és az IoT-eszközökről érkező illetéktelen forgalom megtiltásával. Még ha egy IoT-eszköz veszélybe is kerül, a MUD megakadályozza, hogy olyan támadásban használják fel, amely az eszköznek forgalmat kellene küldenie a következő helyekre

---

127. *Id.*

128. *Lásd* Ryan McCauley, *The Internet of Things Needs Standardization-Here's Why*, GOVTECH. COM (20171,. március), https://www.govtech.com/fs/The-Internet-of-Things-Needs-Standardization-Heres-Why.html [https://perma.cc/FTJ2-74SN].

129. INTERNET ENG'G TASK FORCE, RFC 8520, MANUFACTURER USAGE DESCRIPTION SPECIFICATION (2019. március), https://tools.ietf.org/html/rfc8520 [https://perma.cc/MR9K-YUN6].

130. *Lásd* DONNA DODSON ET AL., NIST SPECIAL PUBL'N 1800-15A, SECURING SMALL-BUSINESS AND HOME INTERNET OF THINGS (IOT) DEVICES: MITIGATING NETWORK-BASED ATTACKS USING MANUFACTURER USAGE DESCRIPTION (MUD) (Nov. 2019), https://csrc.nist.gov/publications/detail/sp/1800-15/draft [https://perma.cc/Z36R-YVT9].

131. *Lásd a* 113-283. sz. közjogi törvényt, a szövetségi információbiztonsági korszerűsítésről szóló törvényt (Federal Information Security Modernization Act of 2014.

132. DONNA DODSON ET AL., NIST SPECIAL PUBL'N 1800-15, SECURING SMALL-BUSINESS AND HOME INTERNET OF THINGS (IOT) DEVICES: MITIGATING MITIGATING NETWORK-BASED ATTACKS USING MANUFACTURER USAGE DESCRIPTION (MUD) 1 (Apr. 2019), https://www.nccoe.nist.gov/sites/de fault/files/library/sp1800/iot-ddos-nist-sp1800-15-preliminary-draft.pdf.

133. *Lásd általában* INTERNET ENG'G TASK FORCE, *fenti* megjegyzés. 129.

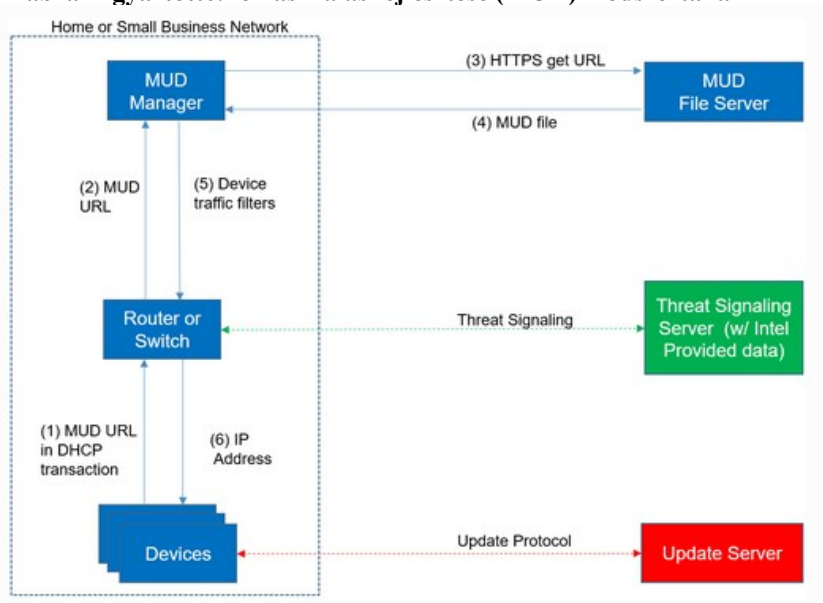
134. DODSON ET AL., *fenti* lábjegyzet 132.



Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

egy nem engedélyezett célállomás."[135] Az ábra vázlatosan mutatja6 be ezt a biztonsági módszertant.

**ábra A gyártott6. felhasználás fejlesztése (MUD) módszertana[136]**




## A. Leírás

A MUD részletesebb ábrázolása az IETF Manufacturer Usage Description Specification című dokumentumában található. Ez leírja, hogy alapvetően "a MUD három építészeti építőelemből áll", a következők szerint: (1) "Egy URL, amely a leírás megtalálására használható"; (2) "Maga a leírás, beleértve az inter- pretálás módját"; és (3) "Egy eszköz a helyi hálózatirányítási rendszerek számára a leírás lekérdezésére".[137]

## B. Tervezés

A MUD több célt is el kíván érni az alábbiak szerint:

- Az eszköz fenyegetési felületének jelentős csökkentése a gyártó által tervezett kommunikációra;
- A hálózati házirendek skálázásának lehetővé tétele a hálózatban lévő egyre növekvő számú eszköztípushoz;
- Legalább néhány sebezhetőség olyan módon történő kezelésének lehetővé tétele, amely gyorsabb, mint a rendszerek frissítésének időigénye. Ez különösen igaz a már nem támogatott rendszerekre;

135. *Id.*
136. *Id.* a 4-1. ábrán13.
137. *Lásd:* INTERNET ENG'G TASK FORCE, *fenti* megjegyzés.129, 11.



Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

- egy ilyen rendszer megvalósításának költségeit a lehető legalacsonyabb szinten kell tartani; és
- A gyártók számára bővíthetőségi lehetőséget biztosítanak az eszköz egyéb képességeinek vagy követelményeinek kifejezésére.[138]

Ezek a célok praktikussá teszik a keretrendszer használatát, miközben egységes biztonsági és használati szintet érnek el. A célok azonban megjegyzik, hogy

> A MUD nem foglalkozik az általános célú számítógépek hálózati engedélyezésével, mivel ezek gyártói nem tudnak elképzelni egy konkrét kommunikációs mintát, amelyet leírhatnának. Ezenkívül még az egyetlen vagy kis számú felhasználási céllal rendelkező eszközök is rendelkezhetnek nagyon széles körű kommunikációs mintákkal. A MUD önmagában ezekre sem alkalmas.
>
> Bár a MUD a hálózati rendszergazdáknak további védelmet nyújthat az eszközök sebezhetőségei esetén, soha nem fogja helyettesíteni a gyártóknak a sebezhetőségek javításának szükségességét.
>
> Végül, függetlenül attól, hogy a gyártó mit ír elő egy MUD fájlban, ezek nem irányelvek, hanem javaslatok. Az, hogy helyben hogyan kell ezeket alkalmazni, sok tényezőtől függ, és végső soron a helyi hálózati rendszergazdától függ, akinek el kell döntenie, hogy az adott körülmények között mi a megfelelő[].[139]

## C. A blokklánc ígérete

A blokklánc-technológia egy évtized alatt jelentős ígéretekkel tekintettek rá, mivel potenciálisan képes fokozott szoftverbiztonságot nyújtani.[140] Csak néhány további ígéretes alkalmazás a következő: intelligens szerződések; [141]virtuális valuták; [142]és számos pénzügyi szolgáltatási funkció, beleértve a végrehajtást és az elszámolást.[143] Jianli Pan és társszerzői 2018-ban írtak, és megfigyelték:

> A kialakulóban lévő tárgyak internete (IoT) jelentős skálázhatósági és titkossági kihívásokkal néz szembe. Egyrészt az IoT-eszközök "gyengék", és külső segítségre van szükségük. Az Edge computing ígéretes irányt kínál a központosított felhőalapú számítástechnika hiányosságainak kezelésére a nagyszámú eszköz skálázásában. Másrészt az IoT-eszközök az erőforrás-korlátok miatt viszonylag "sebezhetőek" a rosszindulatú hackerekkel szemben. A kialakulóban lévő blokklánc- és okosszerződés-technológiák számos új biztonsági funkciót kínálnak a tárgyak internete és az edge computing számára.[144]

Annak érdekében, hogy megoldást kínáljon ezekre a kérdésekre, egy "EdgeChain" nevű edge-IoT keretrendszert terveztek és prototípust készítettek "a blockchain és az intelligens

---

138. *Id.* 3-4.
139. *Id*. 4.
140. *Lásd* Lawrence J. Trautman & Mason J. Molesky, *A Primer for Blockchain*, UMKC88 L. REV. 239, 239-40 (2019).
141. *Id*. 241.
142. *Lásd* Trautman & Harrell, 5. lábjegyzet; Trautman, *Virtual Currencies*, 5. lábjegyzet. 5.
143. *Lásd* Trautman, *Disruptive Blockchain Technology*, *supra* note at5, 239.
144.Jianli Pan et al., *EdgeChain:* IEEE INTERNET THINGS J. (2018): *An Edge-IoT Framework and Prototype Based on Blockchain and Smart Contracts*, 6 IEEE INTERNET THINGS J. (4719,20184719).



Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

szerződések. Az alapötlet az engedélyekkel rendelkező blokklánc és a belső valuta vagy "érme" rendszer integrálása, hogy összekapcsoljuk a felhő-felhő erőforrás-állományát az egyes IoT-eszközök számlájával és erőforrás-használatával, és ezáltal az IoT-eszközök viselkedésével.".[145] Tekintsük át a Pan et al. tanulmányban bemutatott alábbi pontokat:

> Az EdgeChain egy kreditalapú erőforrás-kezelési rendszert használ annak szabályozására, hogy az IoT-eszközök mennyi erőforrást kaphatnak az edge-kiszolgálóktól, a prioritásra, az alkalmazástípusokra és a korábbi viselkedésre vonatkozó, előre meghatározott szabályok alapján. A szabályok és irányelvek érvényesítésére intelligens szerződéseket használnak az IoT-eszközök viselkedésének nem tagadható és automatizált módon történő szabályozására. A biztonságos adatnaplózás és ellenőrzés érdekében az összes IoT-tevékenység és tranzakció a blokkláncba kerül rögzítésre. Egy EdgeChain prototípust valósítunk meg, és kiterjedt kísérleteket végzünk az ötletek értékelésére. Az eredmények azt mutatják, hogy a blokklánc és az intelligens szerződések biztonsági előnyeinek elnyerése mellett az EdgeChainbe való integrálásuk költségei rea- sonálható és elfogadható tartományban vannak.[146]

Az így kapott tervezési sémát "[s]pecifikusan ... . [hogy] részlegesen hivatkozzon a Gyártói használati leírás (MUD) fájlokra, amelyek felsorolják az IoT-eszközök számára engedélyezett tevékenységeket és kommunikációt. Ezek a specifikációk tartalmazzák a bemeneti/kimeneti adattípust, a peremforrások igénylését, a MAC-címet, az IP-adresszt, a hálózati portot, a kommunikációs protokollt és a jelzési zászlókat. . minden eszköz egyedi fiókcímet regisztrál "[147] Így működik: "Amikor
regisztráció, a kiszolgáló ellenőrzi a [megadott] információkat, és korlátozza a regisztrációs adatok módosítási jogait. További paraméterek, például prioritás, érmeegyenleg, kredit és kérések időbélyegzője kerül fel- függesztésre az eszközkezelés érdekében."[148] A Pan et al. tanulmány számos más attribútumot is megemlít, amelyeket a szerzők a regisztrációs adatbázisukban definiáltak, "az összes eszköz kulcsinformációját, értékegységeit és példáit".[149] Ezek az attribútumok a következők: (1) "ac- count address", (2) "network port", (3) "input/output data". (4) "bandwidth re- quest", (5) "CPU request", (6) "memory request", (7) "storage request", (8) "MAC address", (9) "priority*," coin balance*," "credit*," "isBlocked*," "is- Registered*," és "last request id*".[150] Magyarázatként Pan és szerzőtársai megjegyezték: "Az Edge-kiszolgálók és az IoT-eszközök különböző jogosultságokkal rendelkeznek a nyilvántartás módosítására. A '*'-gal jelölt attribútumokat csak az edge szerver frissítheti. A többi alapvető attribútumot az IoT-eszközök által inicializált első regisztrációs folyamat során töltik fel".[151]

## D. A fogyasztói oktatás fontossága

Bármely mérnökprofesszor elmondja, hogy az emberi viselkedés és hozzáállás meghatározó szerepet játszik bármely terméktervezés sikerében. A NIST ad- vises:

---

145. *Id.*
146. *Id.*
147. *Id*. 4724.
148. *Id*. 4725.
149. *Id.*
150. *Id.* a tbl4725.1.
151. *Id*. 4725.



Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

> A tárgyak internetének kiberbiztonságával kapcsolatos kihívások kezelése szükségessé teszi a tárgyak internetének de- vice ügyfeleinek oktatását a tárgyak internetének kiberbiztonsági kockázatai és kockázatcsökkentése közötti különbségekről a hagyományos informatikához képest, amint azt a NIST a Belső jelentésben (IR) dokumentálta a tárgyak internetének (IoT) kiberbiztonsági és adatvédelmi kockázatainak kezelésére vonatkozó megfontolásokról8228,. A kihívások miatt az IoT-eszközök gyártóinak oktatása is szükséges, hogy miként határozzák meg azokat a kiberbiztonsági jellemzőket, amelyekkel az ügyfelek számára az IoT-eszközöknek rendelkezniük kell. Ez magában foglalja a gyártók és a vásárlók közötti kommunikáció javítását az eszközök kiberbiztonsági jellemzőiről és a kapcsolódó elvárásokról.[152]

## VIII. LEGÚJABB FEJLEMÉNYEK

### A. NIST

A NIST továbbra is értékes kutatási erőfeszítéseket, kiadványokat, valamint a kormányzati források és az ipar közötti kapcsolódási pontot biztosít. Václav Janecek professzor az IoT-eszközökből gyűjtött és létrehozott személyes adatok kincsestáráról ír, "amelyek kezelése komoly etikai és jogi kérdéseket vet fel. A személyes adatok tulajdonjoga alátámasztja az adatkezelés és -ellenőrzés körül forgó kérdéseket, például a magánélet védelmét, a bizalmat és a biztonságot, és fontos következményekkel jár a "digitális" gazdaság és az adatkereskedelem jövőjére nézve is".[153]

2020 januárjában a NIST kiadta az adatvédelmi keretrendszer 1.0-s verzióját.[154] Az adatvédelmi kockázatok kezelésére szolgáló új eszköz "a széles körben használt NIST Cybersecurity Framework (NIST kiberbiztonsági keretrendszer) mintájára kialakított átfogó struktúrát tartalmaz, és a két keretrendszert úgy tervezték, hogy kiegészítsék egymást, és idővel aktualizálják is".[155] A NIST megjegyzi, hogy az adatvédelmi érdekek "magukban foglalják az egyes egyénekre vonatkozó információkat, például a címüket vagy a társadalombiztosítási számukat, amelyeket egy vállalat a szokásos üzleti tevékenysége során gyűjthet és használhat fel . . . [megköveteli], hogy a szervezet ... intézkedéseket tegyen annak biztosítására, hogy [ezekkel az adatokkal] ne éljenek vissza olyan módon, amely zavarba hozhatja, veszélyeztetheti vagy veszélyeztetheti az ügyfeleket".[156] Bár az adatvédelmi keretrendszer nem rendelet vagy törvény, mégis "egy olyan önkéntes eszköz, amely segíthet a szervezeteknek a termékeikből és szolgáltatásaikból eredő adatvédelmi kockázatok kezelésében, valamint az őket érintő törvényeknek való megfelelés bizonyításában".[157] A NIST más, a tárgyak internetével kapcsolatos kérdésekkel foglalkozó, nemrégiben megjelent kiadványai is elérhetők.[158]

---

152. *Lásd* FAGAN ET AL., *fenti* megjegyzés 4,vii. pontjában.

153. Václav Janeček, *A személyes adatok tulajdonjoga a tárgyak internetén*, COMP34. L. & SEC. REV. 1039, 1039-40 (2018).

154. *Lásd* NAT'L INST. OF STANDARDS & TECH., VERSION 1.0, NIST PRIVACY FRAMEWORK: A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT (2020. január 16.), https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf [https://perma.cc/5QCL-LGPH].

155. Press Release, Nat'l Inst. of Standards & Tech., NIST Releases Version 1.0 of Privacy Framework (Jan. 202016,), https://www.nist.gov/news-events/news/2020/01/nist-releases-version-10-privacy-framework [https://perma.cc/8EZF-HAKH].

156. *Id.*

157. *Id.*

158. *Lásd* FAGAN ET AL., *fenti* megjegyzés 4,3-4. pontja.

Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

A kiberbiztonsági és adatvédelmi kockázatokról szóló vitánk végéhez közeledve fontos figyelembe venni, hogy "egy IoT-eszköz adatbiztonságát nem lehet[ene] mind az eszközön belül megoldani". Minden IoT-eszköz egy tágabb IoT-környezetben működik, ahol kölcsönhatásba lép más IoT- és nem IoT-eszközökkel, felhőalapú szolgáltatásokkal, emberekkel és más összetevőkkel".[159]

### B. Kaliforniai törvény SB 327

Egy új kaliforniai törvény 2020-tól kezdődően megköveteli a gyártóktól, hogy "ésszerű biztonsági funkciókat" építsenek be a csatlakoztatott eszközökbe vagy a tárgyak internetére.[160] Ez az egyik első olyan szabályozás az Egyesült Államokban, amely minden fogyasztói termékre/eszközre információbiztonsági követelményeket ír elő, és ezt a terhet a gyártókra hárítja.

## IX. AJÁNLÁSOK

A lehetséges lépések sokaságának mérlegelése után jó kiindulópontnak [161]bizonyulnak a 2018 közepén megjelent, *A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats című jelentésben* megfogalmazott célok és intézkedések. A jelentés vonatkozó része kimondja:

> E célok és intézkedések célja, hogy olyan, egymást kölcsönösen támogató intézkedések portfólióját mutassák be, amelyek végrehajtása drámai mértékben javítaná az ökoszisztéma ellenálló képességét. Az ajánlott intézkedések között vannak olyan folyamatban lévő tevékenységek, amelyeket folytatni vagy bővíteni kell, valamint új kezdeményezések is. Egyetlen beruházás vagy tevékenység sem képes minden veszélyt enyhíteni, de a szervezett megbeszélések és az érdekelt felek visszajelzései lehetővé teszik, hogy tovább értékeljük és rangsoroljuk ezeket a tevékenységeket a befektetések várható megtérülése és az ökoszisztéma ellenálló képességére gyakorolt mérhető hatásuk alapján. Arra számítunk, hogy az ökoszisztéma érdekelt felei együttműködnek a kormánnyal a javasolt tevékenységek végrehajtása, a támogatás és a vezető szerep lehetőségeinek megvalósítása, valamint a végrehajtás akadályainak elhárítása érdekében.[162]

Ennek megfelelően a jelentésben szereplő célok és intézkedések listája az alábbiakban kerül felsorolásra:

> **1. cél: Az alkalmazkodóképes, fenntartható és biztonságos technológiai piac felé vezető egyértelmű út meghatározása.**
>
> 1.1. intézkedés Az iparág által vezetett, inkluzív folyamatok alkalmazásával, önkéntes, iparági irányítású nemzetközi szabványokon alapuló, az otthoni és ipari alkalmazások életciklus-biztonságát támogató, nemzetközileg alkalmazható IoT-képességi alapvonalak létrehozása.

159. BOECKL ET AL .,*supra* note at27, 1.

160. S.B. Leg327,2018., Reg. Sess. (Cal. 2017), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327 [https://perma.cc/RTR9-JCHA].

161. *Lásd* U.S. DEP'T OF COMMERCE & U.S. DEP'T OF HOMELAND SEC.,, lásd a107, *fenti* megjegyzést. 25.

162. *Id.*



Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

Intézkedés A 1.2szövetségi kormányzatnak adott esetben ki kell használnia az iparág által kidolgozott képességi alapvonalakat az amerikai kormányzati környezetben lévő IoT-eszközök képességi alapvonalainak létrehozásakor, hogy megfeleljen a szövetségi biztonsági követelményeknek, elősegítse az iparági alapvonalak elfogadását és felgyorsítsa a nemzetközi szabványosítást.

intézkedés 1.3. Az iparnak szélesebb körben el kell fogadnia azokat a szoftverfejlesztési eszközöket és eljárásokat, amelyek jelentősen csökkentik a kereskedelmi forgalomban kapható szoftverek biztonsági réseinek előfordulását. A szövetségi kormánynak együtt kell működnie az iparral, hogy ösztönözze e gyakorlatok további elterjedését és alkalmazását, valamint a piaci elfogadás és az elszámoltathatóság javítását.

Intézkedés Az iparnak1.4 fel kell gyorsítania az innovatív technológiák fejlesztését és bevezetését az elosztott fenyegetések megelőzésére és mérséklésére. Ennek megfelelően a kormányzatnak adott esetben prioritásként kell kezelnie a kutatási és fejlesztési alapok és a technológiai áttörési erőfeszítések alkalmazását a DDoS megelőzés és enyhítés, valamint a botnetek létrehozásának megakadályozását célzó alapvető technológiák fejlesztésének támogatására. Adott esetben a civil társadalomnak fel kell erősítenie ezeket az erőfeszítéseket.

intézkedés 1.5. A kormánynak, az iparnak és a civil társadalomnak együtt kell működnie annak biztosítása érdekében, hogy a tárgyak internetére vonatkozó meglévő legjobb gyakorlatokat, kereteket és iránymutatásokat, valamint az átláthatóságot biztosító eljárásokat szélesebb körben elfogadják a digitális ökoszisztémában. A tárgyak internetének újonnan felmerülő kockázatait nyílt és inkluzív módon kell kezelni.

**2. cél: Az innováció előmozdítása az infrastruktúrában a változó fenyegetésekre való dinamikus reagálás érdekében.**

Intézkedés Az internetszolgáltatóknak2.1 és peering partnereiknek ki kell terjeszteniük a jelenlegi információmegosztást, hogy időben és hatékonyabban megoszthassák egymással a veszélyekkel kapcsolatos, akcióképes információkat mind belföldön, mind világszerte.

Intézkedés 2.2. Az érdekelt feleknek és a szakterület szakértőinek a NIST-tel konzultálva vezetniük kell a DDoS megelőzés és elhárítás CSF-profiljának kidolgozását.

Intézkedés A 2.3szövetségi kormánynak példát kell mutatnia, és demonstrálnia kell a technológiák gyakorlati alkalmazhatóságát, piaci ösztönzőket teremtve a korai alkalmazók számára.

2.4. intézkedés Az iparnak, a kormánynak és a civil társadalomnak együtt kell működnie az érdekeltek teljes körével az információmegosztási protokollok további fejlesztése és állandósítása érdekében.

intézkedés 2.5. A szövetségi kormánynak együtt kell működnie az amerikai és a globális infrastruktúra-szolgáltatókkal annak érdekében, hogy a hálózati forgalomirányítás legjobb gyakorlatát kiterjesszék az egész ökoszisztémára.



Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

**3. cél: Az innováció előmozdítása a hálózat peremén az automatizált, elosztott támadások megelőzése, észlelése és enyhítése érdekében.**

Intézkedés A 3.1hálózati iparágnak ki kell terjesztenie a jelenlegi termékfejlesztési és szabványosítási erőfeszítéseket a hatékony és biztonságos forgalomirányítás érdekében otthoni és vállalati környezetben.

3.2. intézkedés Az otthoni IT- és IoT-termékeknek könnyen érthetőnek és egyszerűen és biztonságosan használhatónak kell lenniük.

Intézkedés A vállalkozásoknak3.3 olyan hálózati architektúrákra kell áttérniük, amelyek megkönnyítik az automatizált, elosztott fenyegetések észlelését, megszakítását és mérséklését. Azt is figyelembe kell venniük, hogy saját hálózataik hogyan veszélyeztetnek másokat.

Intézkedés A 3.4szövetségi kormánynak meg kell vizsgálnia, hogy az IPv6 szélesebb körű bevezetése hogyan változtathatja meg a támadás és a védekezés gazdaságosságát.

**4. cél: A biztonsági, infrastrukturális és operatív technológiai közösségek közötti koalíciók előmozdítása és támogatása helyben és világszerte.**

Intézkedés Az internetszolgáltatóknak4.1 és a nagyvállalatoknak fokozniuk kell az információmegosztást a kormányzati szervekkel és egymással annak érdekében, hogy az automatizált, elosztott fenyegetésekkel kapcsolatban időben és megfelelőbben tudjanak információt szolgáltatni.

Intézkedés A 4.2szövetségi kormánynak két- és többoldalú nemzetközi kötelezettségvállalások révén elő kell mozdítania a legjobb gyakorlatok és a vonatkozó eszközök nemzetközi átvételét.

Intézkedés Az ágazatspecifikus4.3 szabályozó ügynökségeknek adott esetben együtt kell működniük az iparral a megtévesztő marketing biztosítása és a megfelelő ágazatspecifikus biztonsági megfontolások előmozdítása érdekében.

4.4. intézkedés A közösségnek meg kell határoznia a támadó eszközök és ösztönzők megzavarására irányuló befolyásolási pontokat és konkrét lépéseket kell tennie, beleértve a hírnévre vonatkozó adatok aktív megosztását és felhasználását.

intézkedés 4.5. A kiberbiztonsági közösségnek továbbra is együtt kell működnie az operatív technológiai közösséggel a tudatosság előmozdítása és a kiberbiztonsági technológiák beépítésének felgyorsítása érdekében.

**5. cél: A tudatosság és az oktatás növelése az egész ökoszisztémában.**

Intézkedés A 5.1magánszektornak önkéntes információs eszközöket kell létrehoznia és kezelnie az otthoni IoT-eszközökre vonatkozóan, amelyeket egy skálázható és költséghatékony értékelési folyamat támogat, és amelyekben a fogyasztók megbízhatnak és intuitív módon megérthetik.

Intézkedés A 5.2magánszektornak önkéntes címkézési rendszereket kell létrehoznia az ipari IoT-alkalmazások számára, amelyeket egy skálázható és

Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

költséghatékony értékelési folyamatot, hogy elegendő biztosítékot nyújtson a tárgyak internetének kritikus infrastrukturális alkalmazásaihoz.

5.3. intézkedés A kormánynak ösztönöznie kell az egyetemi és képzési ágazatokat, hogy a biztonságos kódolási gyakorlatokat teljes mértékben integrálják az informatikai és kapcsolódó programokba.

Intézkedés Az 5.4akadémiai szektornak a kiberbiztonság oktatására irányuló nemzeti kezdeményezéssel együttműködve a kiberbiztonságot alapvető követelményként kell bevezetnie valamennyi mérnöki tudományágban.

Intézkedés A 5.5szövetségi kormánynak figyelemfelkeltő kampányt kell indítania az otthoni IoT-eszközök biztonsági alapvonalának és márkajelzésének elismerése és elfogadása érdekében.[163]

Bár a fenti ajánlások mindegyike segít a botnetekkel és más automatizált, elosztott fenyegetésekkel szembeni ellenálló képesség előmozdításában, a szerzők tapasztalatai és az alábbiakban kifejtett támogató nyilatkozatok alapján ezeket az intézkedéseket a legnagyobb hatás elérése érdekében fontossági sorrendbe kell állítani:

**Intézkedés1.2** : A kormánynak lehetősége van arra, hogy amíg a tárgyak internete a születési fázisában van, segítsen kialakítani és ösztönözze a szabványok elfogadását, hogy az iparág jövője megfelelő biztonsági és irányítási képességekkel rendelkezzen. Az olyan funkciók, mint a biztonság és az interoperabilitás, költségmegtakarítási céllal elhagyhatók a kormányzat befolyása nélkül (amelynek feladata a közjó biztosítása, nem pedig a bot- tom vonal). A kormányzatnak a szabályozás, a beruházások és a szabványok önelfogadása révén kellene hatalmi eszközeit felhasználnia, hogy a funkciókat és a legjobb gyakorlatokra vonatkozó szabványokat a tárgyak internetének iparágába terelje.

**Intézkedés1.4** : Ez az intézkedés hangsúlyozza, hogy mind az ipar, mind a kormányzat fontos szerepet játszik a biztonságos és ellenálló tárgyak internetének megteremtésében. Fel kell ismernünk annak jelentőségét, hogy a kialakulóban lévő, életünk oly sok aspektusát közvetlenül befolyásoló technológiába megfelelő befektetéseket eszközöljünk, amíg még változtatni lehet rajta. A kormánynak azonosítania kell a tárgyak internete által okozott problémákat, például a DDoS-támadásokat, és elő kell mozdítania a megelőzésre/elhárításokra irányuló kutatást, miközben mindenki biztonságát és jólétét szolgáló megoldásokba kell befektetnie.

**3.2. intézkedés: A** kockázat gyakran abból adódik, hogy a végfelhasználó összezavarodik egy rendszer vagy eszköz használatával, ami káros reakciókat okoz, vagy véletlenül sebezhetőségeket hoz létre. Bryan D. Payne és W. Keith Edwards a *Brief Introduction into Usable Security* című tanulmányában megállapította, hogy "a rendszertervezés nagymértékben befolyásolhatja a felhasználó képességét arra, hogy megfelelő biztonsági döntéseket hozzon".[164] Ezért feltétlenül elő kell mozdítani az egyszerűségét a

163. *Id.* 25-47.

164. Bryan D. Payne & W. Keith Edwards, *A Brief Introduction to Usable Security*, IEEE INTERNET COMPUTING, May-June 2008, 13., 19. o. https://www.cc.gatech.edu/~keith/pubs/ieee-intro-usable-security.pdf.

Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

a termék és a "tervezés általi biztonság" koncepciója - ahol a biztonság a termék része - a kockázatok minimalizálása érdekében.

**3.3. intézkedés: A** fenti ajánlások általános célja a tárgyak internetének rugalmasságának növelése. Ez az intézkedés ezt a célt hangsúlyozza, a 2018. évi köz- és magánszféra közötti elemzési csereprogram *kiberkitartóképességről és reagálásról szóló* dokumentumában felvázolt elv alapján, miszerint az embereknek "[a]zzal kell számolniuk, hogy az ellenfél veszélyezteti vagy betör a rendszerbe vagy szervezetbe".[165] Továbbá a dokumentum megállapítja: "A kibertűrő képesség egy rendszer azon tulajdonsága, amely biztosítja, hogy a rendszer továbbra is ellátja a küldetés szempontjából alapvető funkcióit, még akkor is, ha kibertámadás éri".[166] Az összekapcsolhatóság korában nem elég egy biztonsági falat építeni, hanem proaktívan kell keresnünk, megszakítanunk és enyhítenünk a kockázatokat, miközben meg kell értenünk, hogy a kockázataink hogyan hatnak másokra.

A költséges adatvédelmi incidensek továbbra is riasztó ütemben folytatódnak. A mesterséges intelligencia, a gépi tanulás és az internetre csatlakoztatott több milliárd érzékszervi eszköz hatásának irányítására tett kísérletek nem szándékolt következményei minden érintett számára kihívást jelentenek. Ez a cikk hozzájárul a tárgyak internetével (IoT) kapcsolatos rosszindulatú szoftvereknek való széles körű kitettség megértéséhez, és kiegészíti a vállalati kockázatok kormányzásával kapcsolatos, születőben lévő, de kialakulóban lévő szakirodalmat, amely létfontosságú társadalmi jelentőségű téma.



Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973

165. CYBER RESILIENCE AND RESPONSE: PUBLIC-PRIVATE2018 ANALYTIC EXCHANGE PROGRAM 10 (2018), https://www.dhs.gov/sites/default/files/publications/2018_AEP_Cyber_Resilience_and_Response.pdf [https://perma.cc/3LV8-FP77].

166. *Id*. 6.



Elektronikusan elérhető a következő címen:
https://ssrn.com/abstract=3443973