NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA

Okosváros

Kihívások és biztonság

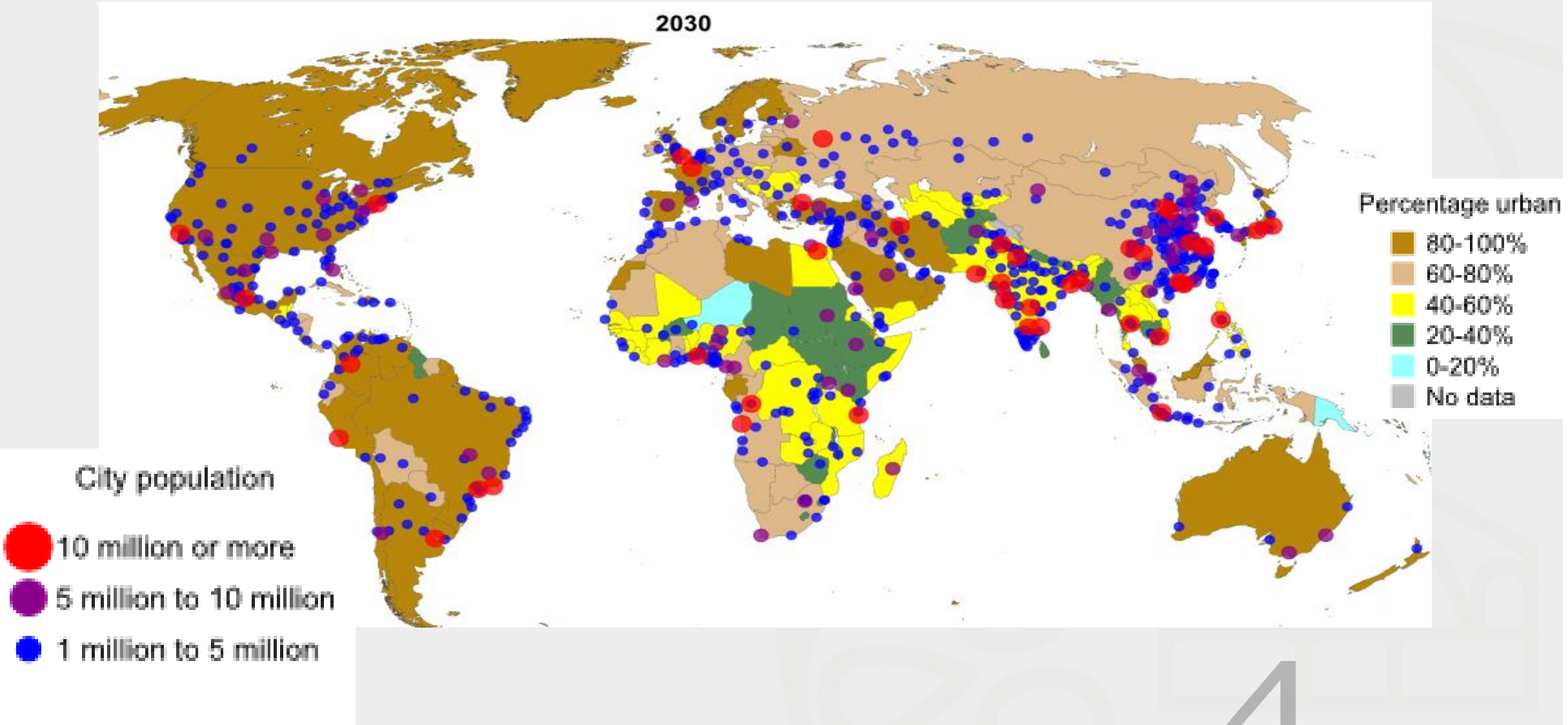
Orbók Ákos
NKE Kiberbiztonsági Tanszék

NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA

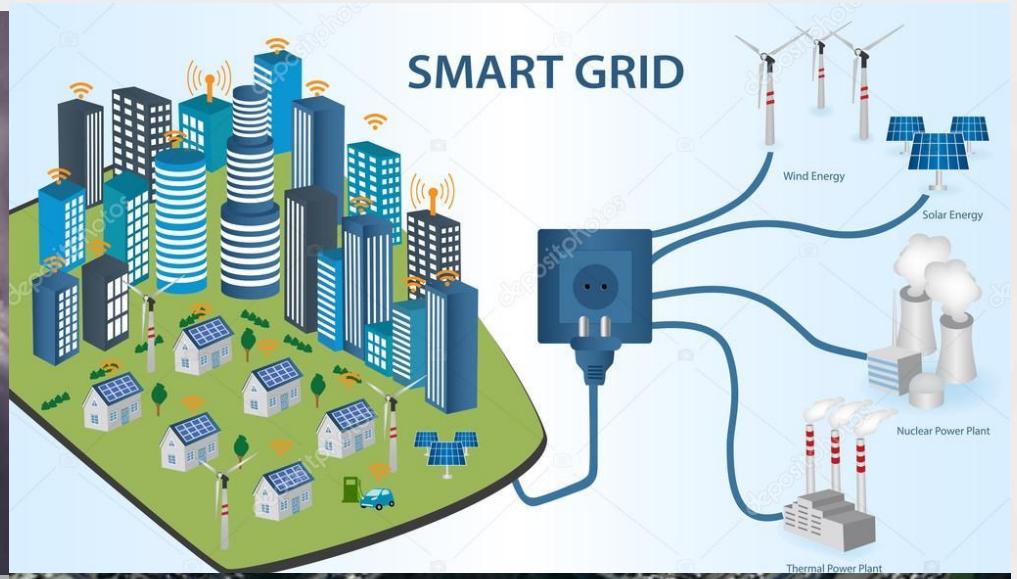
A városok globális kihívásai

Urbanizáció

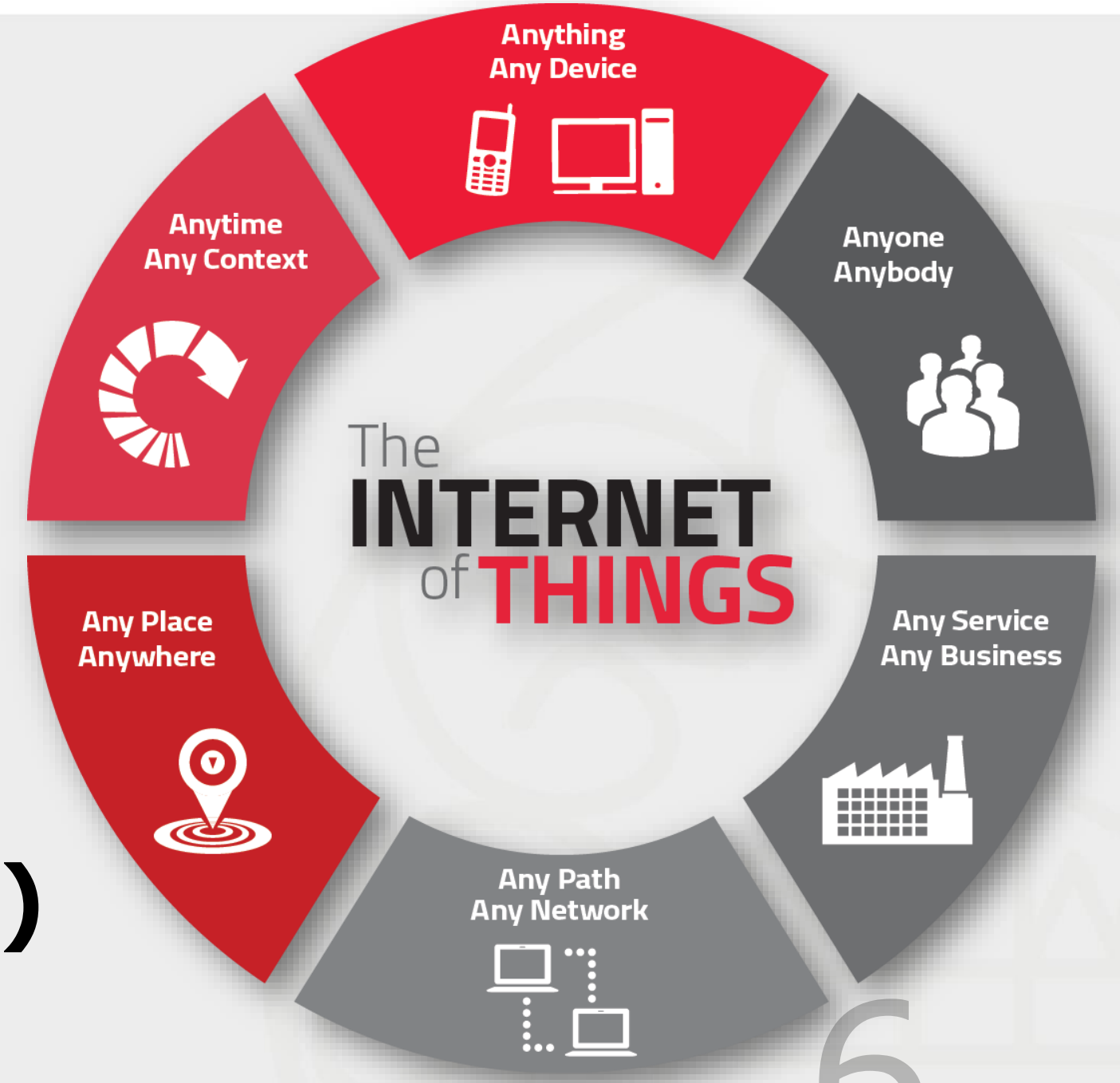
Urbanizáció



Infrastruktúra és fenntarthatóság



Technológia (IKT és IoT)



OKOSTELEFON FÜGGŐSÉG

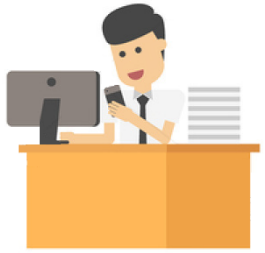
INFOGRAFIKA - 2017

2017-ben az okostelefon használat, a rendkívül többszínűsége miatt elterjedtebb, mint eddig bármikor. Nem csak telefonálásra, hanem tájékozódásra, szórakozásra és időtöltésre is egyre nagyobb arányban használjuk. A növekvő tendencia egyik legfontosabb eleme az egyre olcsóbb internet hozzáférés.

90%

Szabadidőben

Zenehallgatásra, játékokra, hírek olvasására és közösségi oldalak követésére.

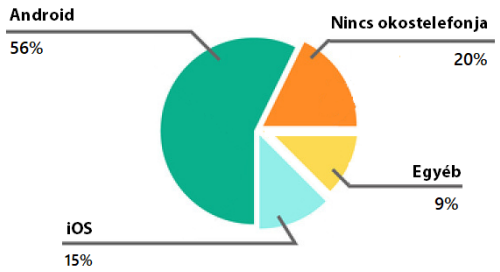


65%

Munka közben

A munkától függetlenül, okostelefont magán célra használók aránya

A megkérdezettek megoszlása operációs rendszer szerint



75%

Étkezéskor

Megdöbbentően nagy arányban olvasunk híreket, vagy böngésszük a közösségi portálokat ebéd, vagy akár vacsora közben.

80%

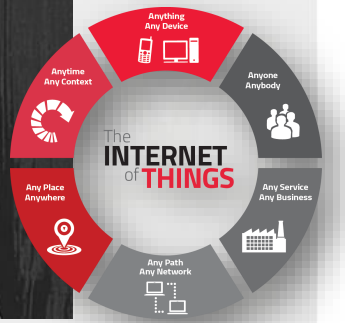
Lefekvés előtt

Gyakori probléma az álmatlanság és a reggeli kialvatlanság.

30%

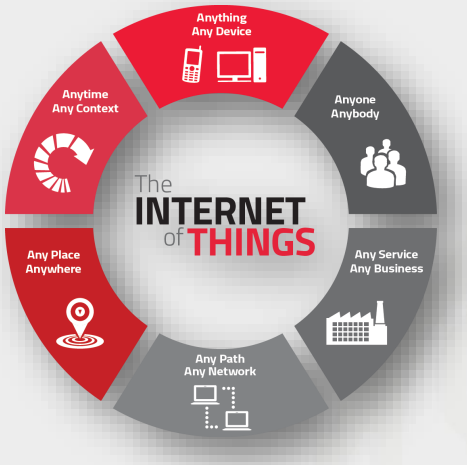
Vezetés közben

A megkérezettek jelentős százaléka nem "csak" telefonálni szokott, hanem rendszeresen használja üzenetküldésre és böngészésre is vezetés közben a telefoniát.



Biztonság vagy szabadság?

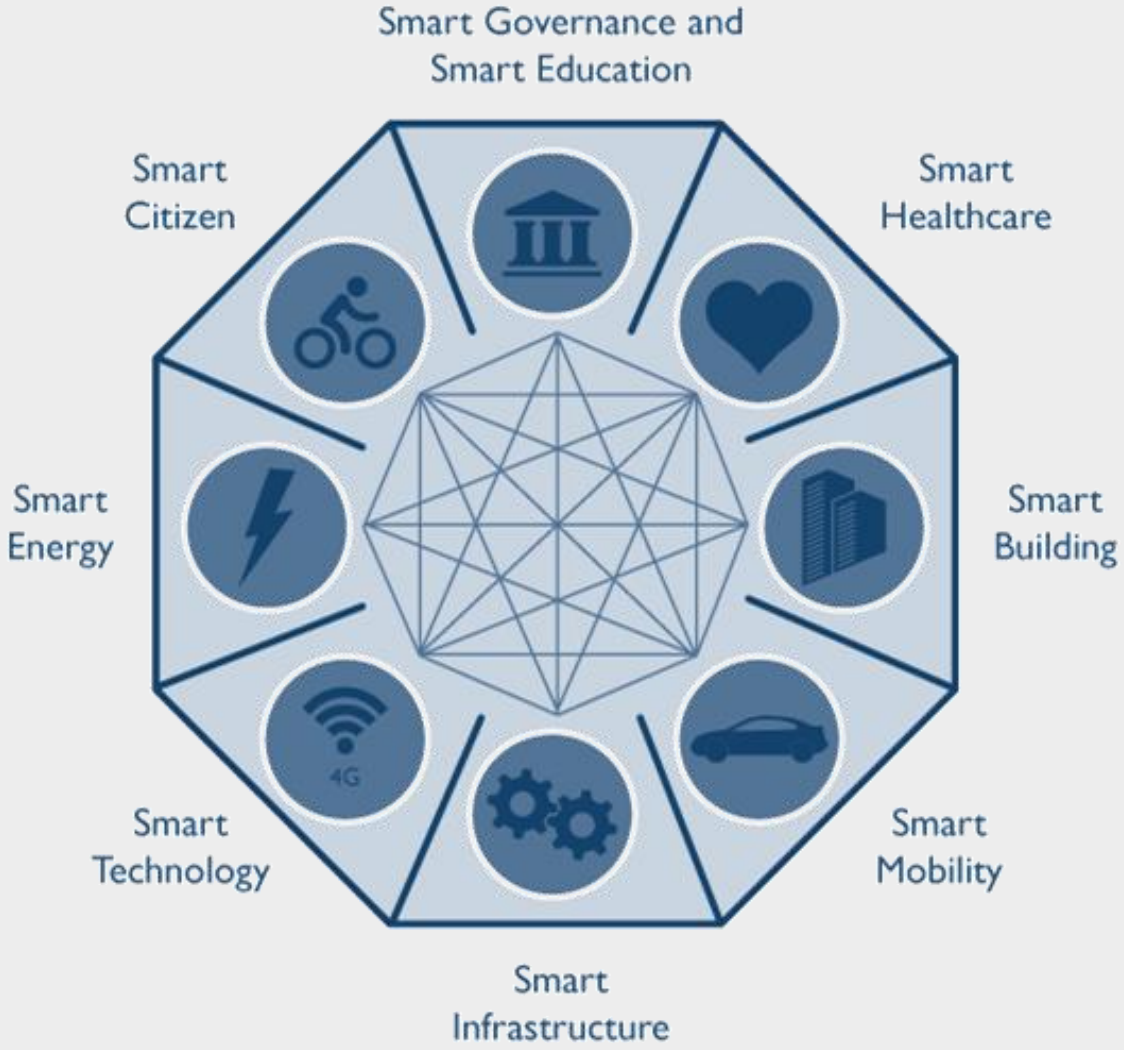
Biztonság

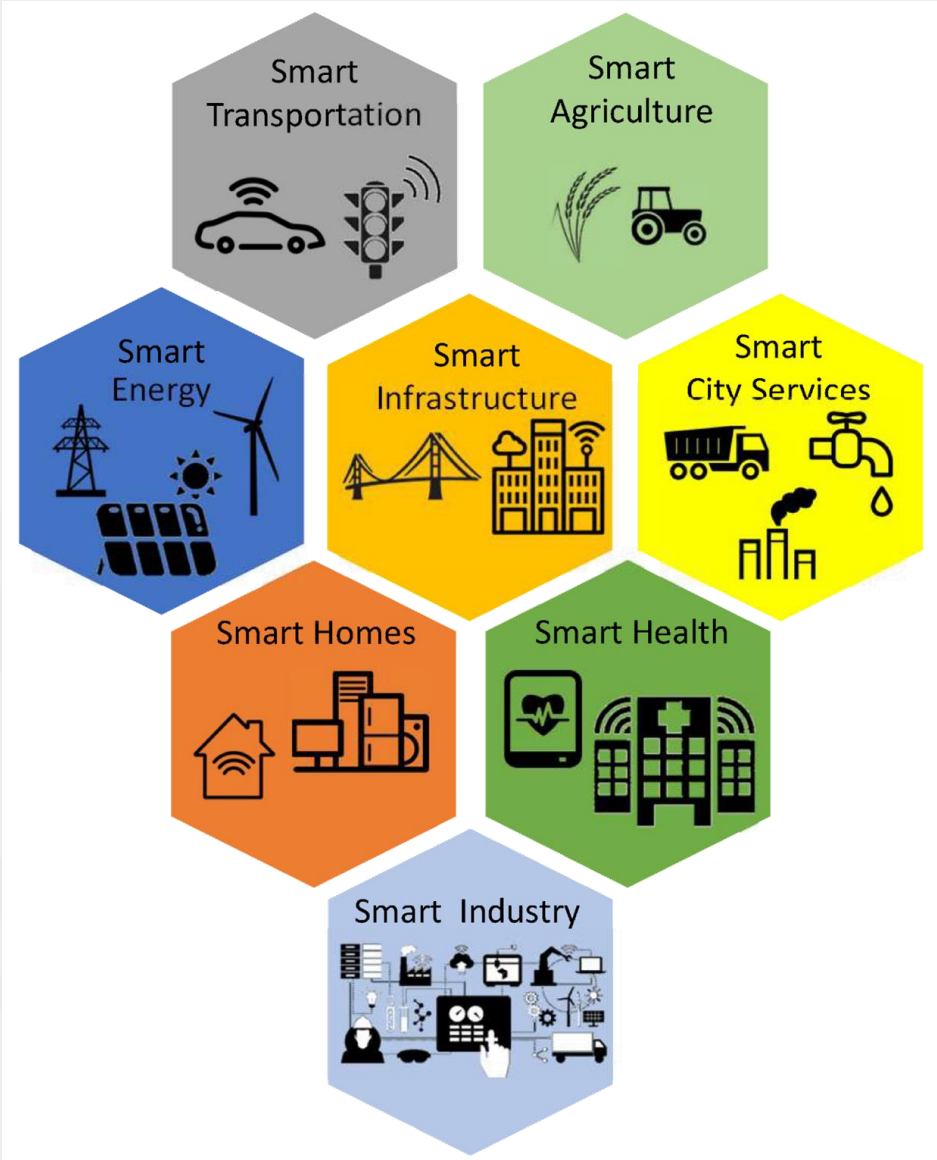


Szabadság

- Megfigyelés
- Intézményi korlátok
- Technológiai rendszer
- Hatalom megerősítés

- Adatvédelem
- Emergens viselkedés
- Humán „rendszer”
- Hatalom kibillentés



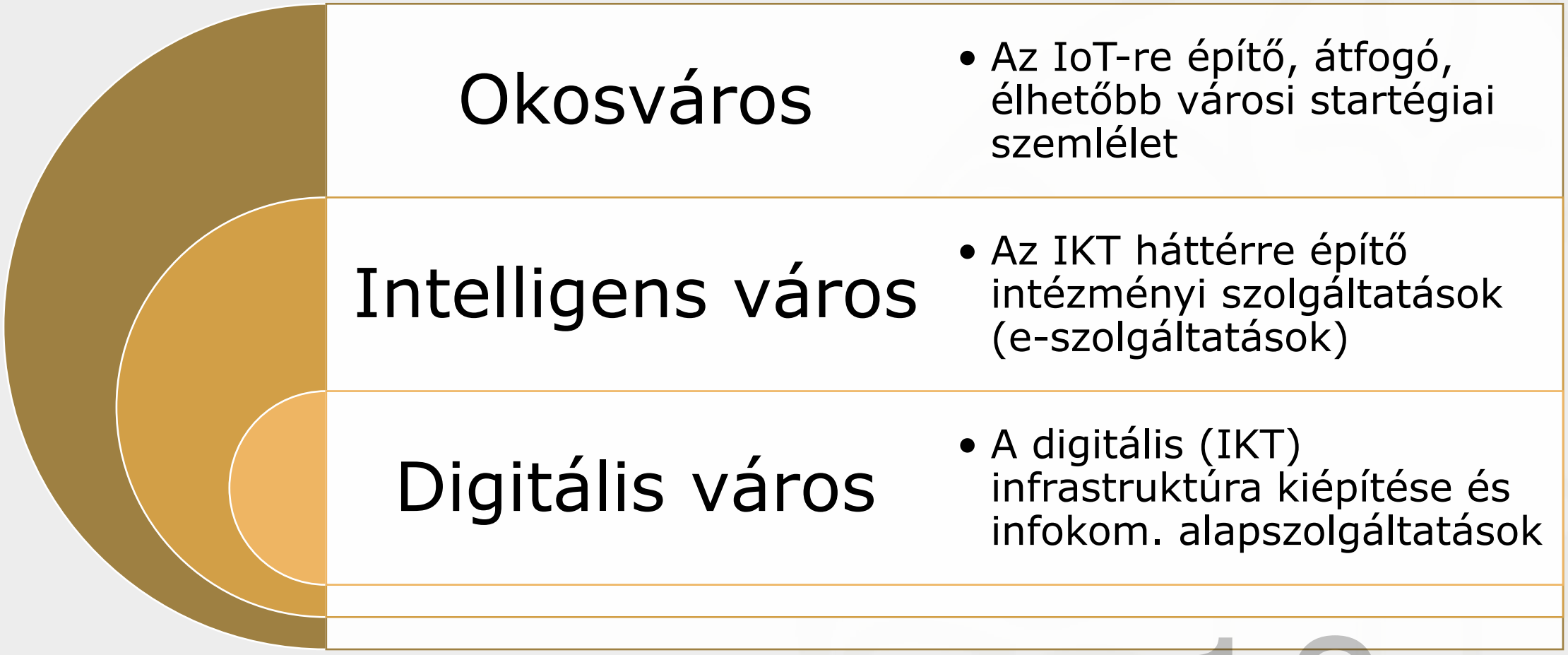


Syed, Abbas S., Daniel Sierra-Sosa, Anup Kumar, and Adel Elmaghraby. 2021. "IoT in Smart Cities: A Survey of Technologies, Practices and Challenges" *Smart Cities* 4, no. 2: 429-475. https://doi.org/10.3390/smartcities4020024

Forrás: https://www.mdpi.com/2624-6511/4/2/24#cite

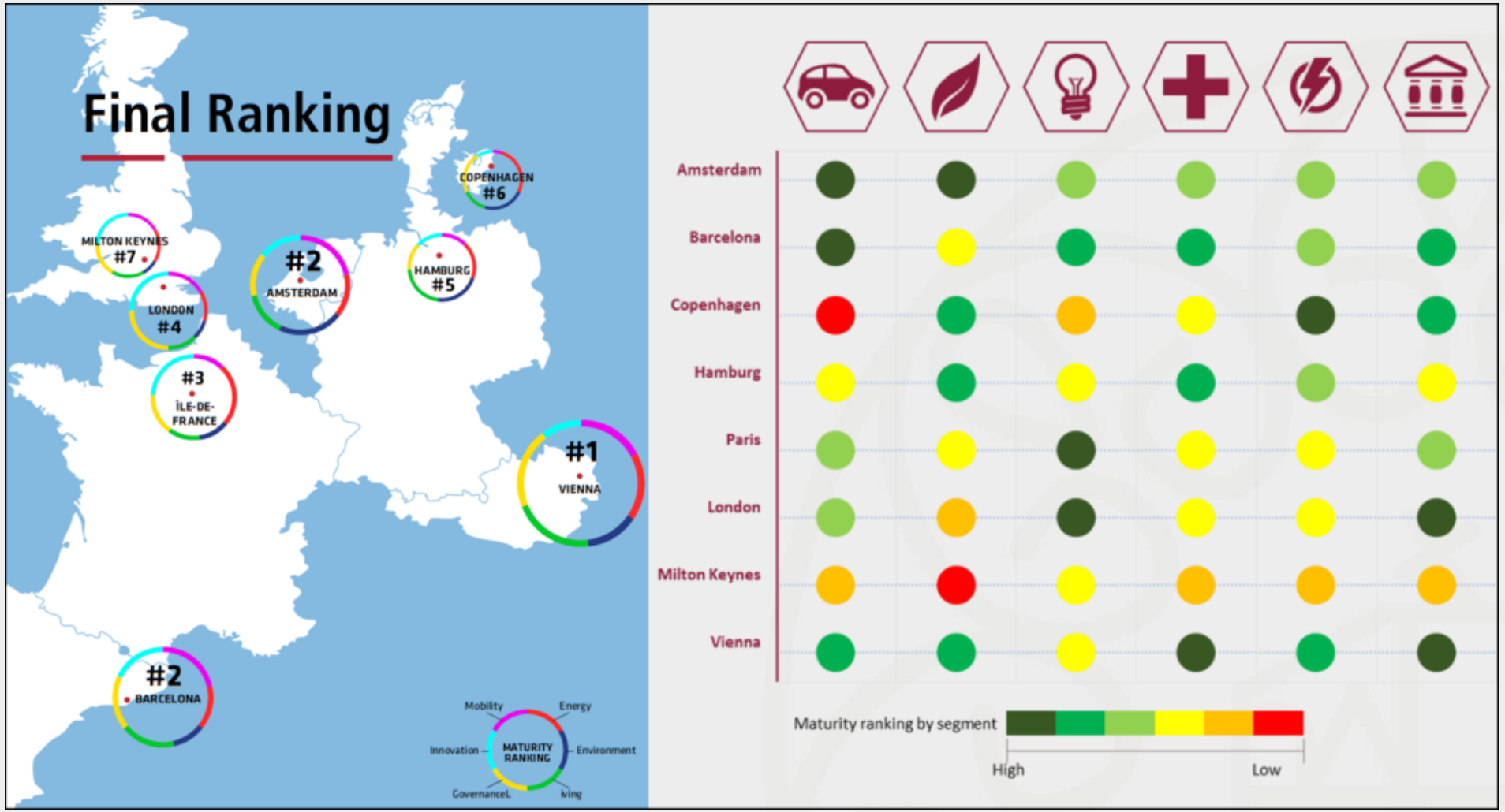
http://blogs-images.forbes.com/sarwantsingh/files/2014/07/fs_gfx_smart-cities-concepts-v1.png

Evolúciós szintek

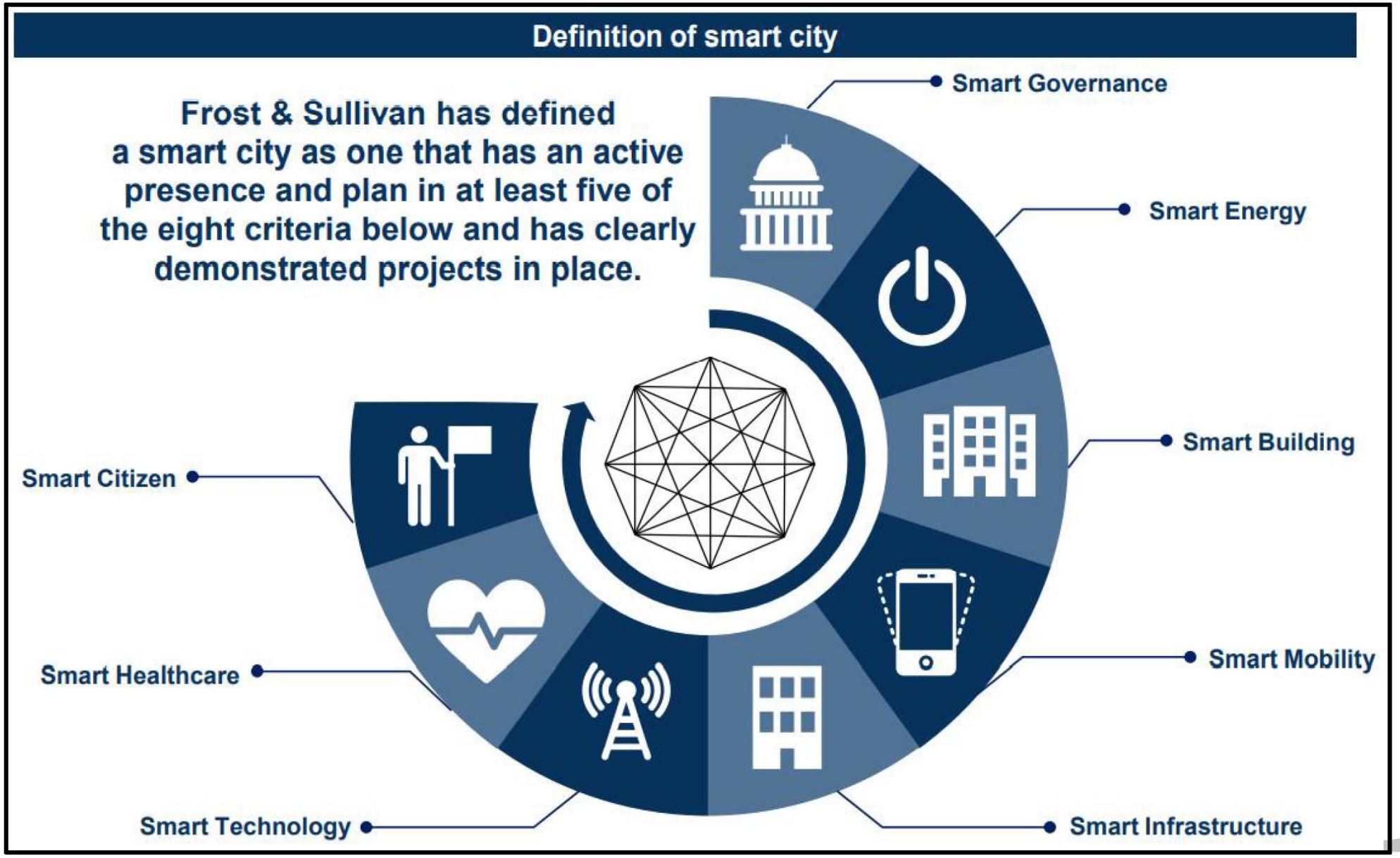


Sallai Gyula: Az okos város koncepció és az internet ökoszisztéma, Az okos város (Smart City) 2018

Európai okosváros rangsor



Bearing point: The unique aspects of European smart cities: strengths and challenges to face worldwide competition? https://www.bearingpoint.com/files/Article2net.png?w=1060



Lim, Seng B., etal. 2021. "Understanding and Acceptance of Smart City Policies: Practitioners' Perspectives on the Malaysian Smart City Framework" *Sustainability* 13, no. 17: 9559. https://doi.org/10.3390/su13179559 *https://www.mdpi.com/2071-1050/13/17/9559#cite*>

NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA

Kiberbiztonság

Kiberbiztonsági kihívások napjainkban

Kiberbiztonság az okos városokban

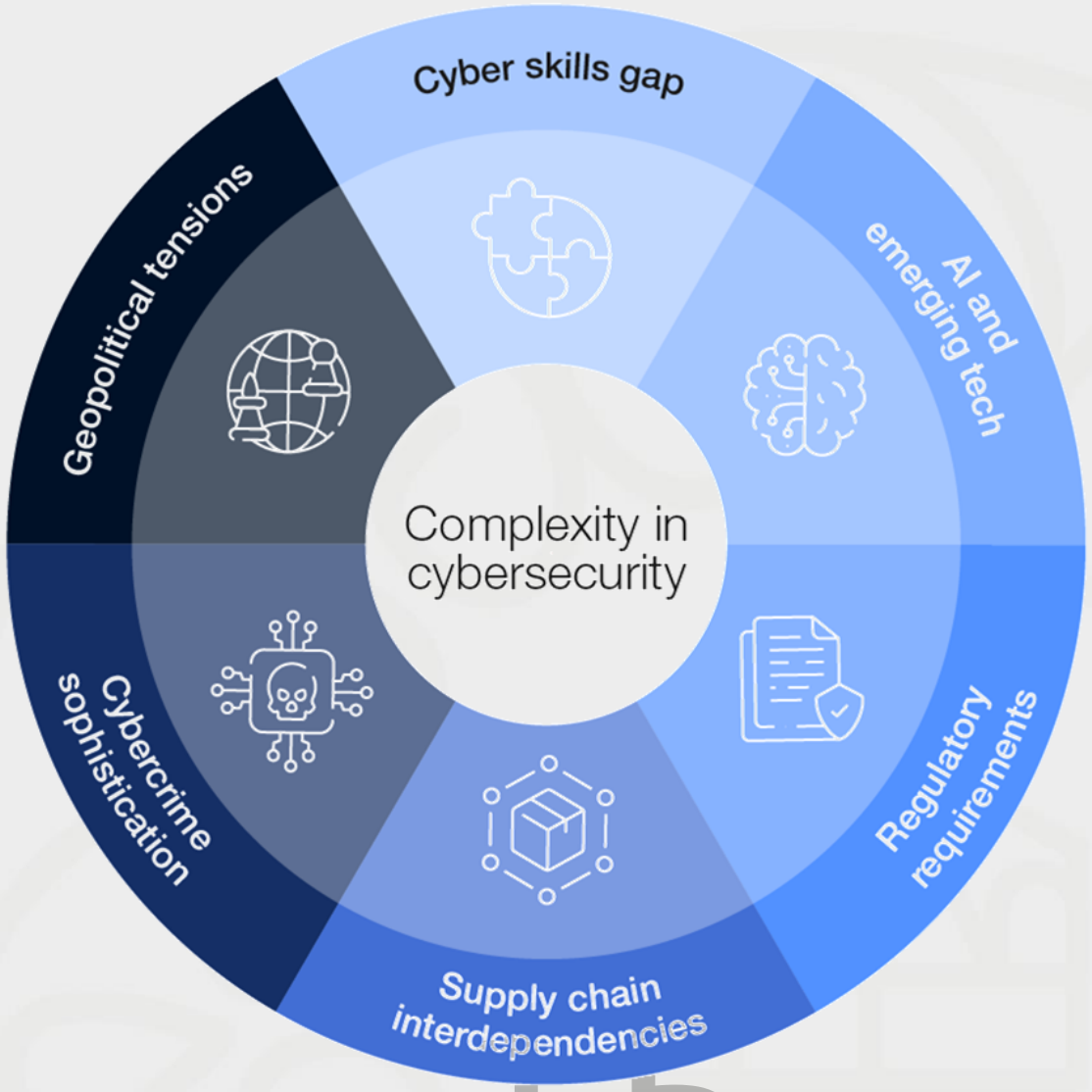
Lehetséges fenyegetések

Esettanulmány

Megelőzés

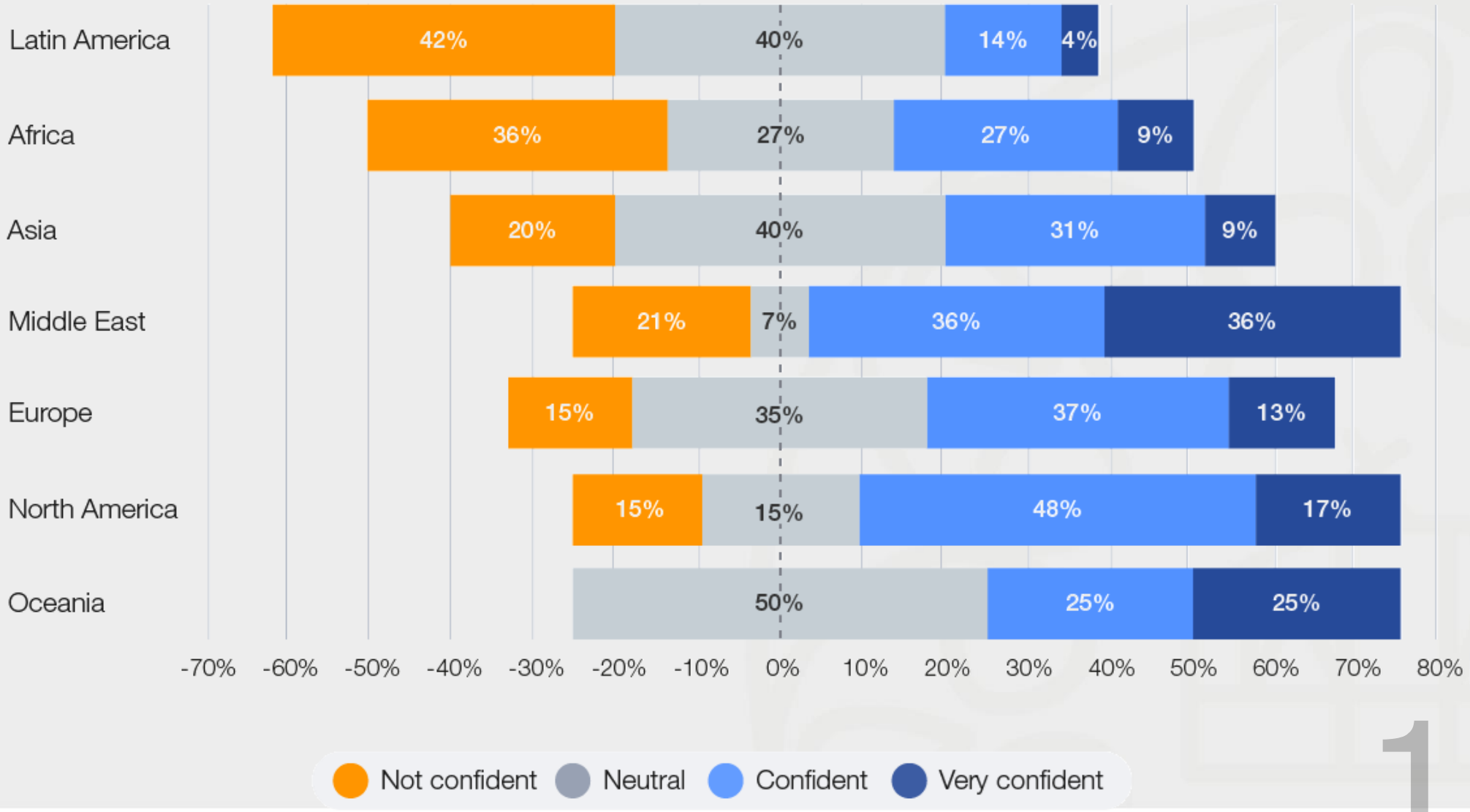
Kiberbiztonsági kihívások napjainkban

- Kiberbűnözés kifinomultabb
- Ellátási láncok – függés
- MI és feltörekvő tech
- Digitális szakadék
- Szabályozási hiányosságok
- Gopolitikai bizonytalanságok
- Quantum kriptográfia
- IT és OT konvergenciája



https://www.weforum.org/publications/global-cybersecurity-outlook-2025/digest/

How confident are you that the country in which your organization is based is well prepared to respond to major cyber incidents targeting critical infrastructure?



Az okos város biztonsági kihívásai

Az okos városok biztonsági szempontból speciális helyzet, mert egyszerre kell figyelembe vennie a következőket:

Kiberbiztonság:

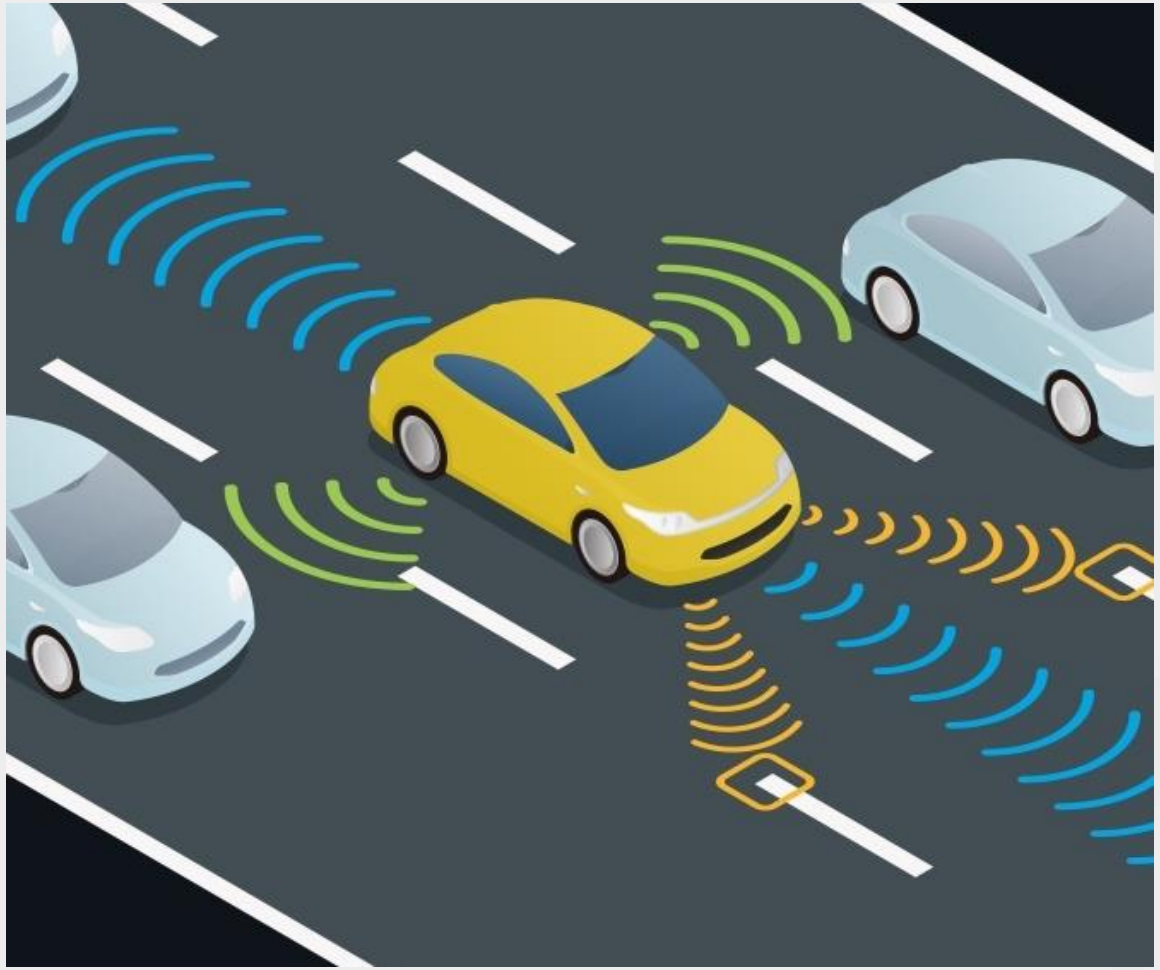
- Súlyos sebezhetőség az önvezető autóban
- A fertőzés percekben mérhető
- Azonnal frissíteni kell!

Üzembiztonság:

- Egy új patch előre nem látható gondokat okozhat
- Lehet-e menet közben frissíteni?
- Nézzük meg, merre jár áll-e az autó!

Adatvédelem:

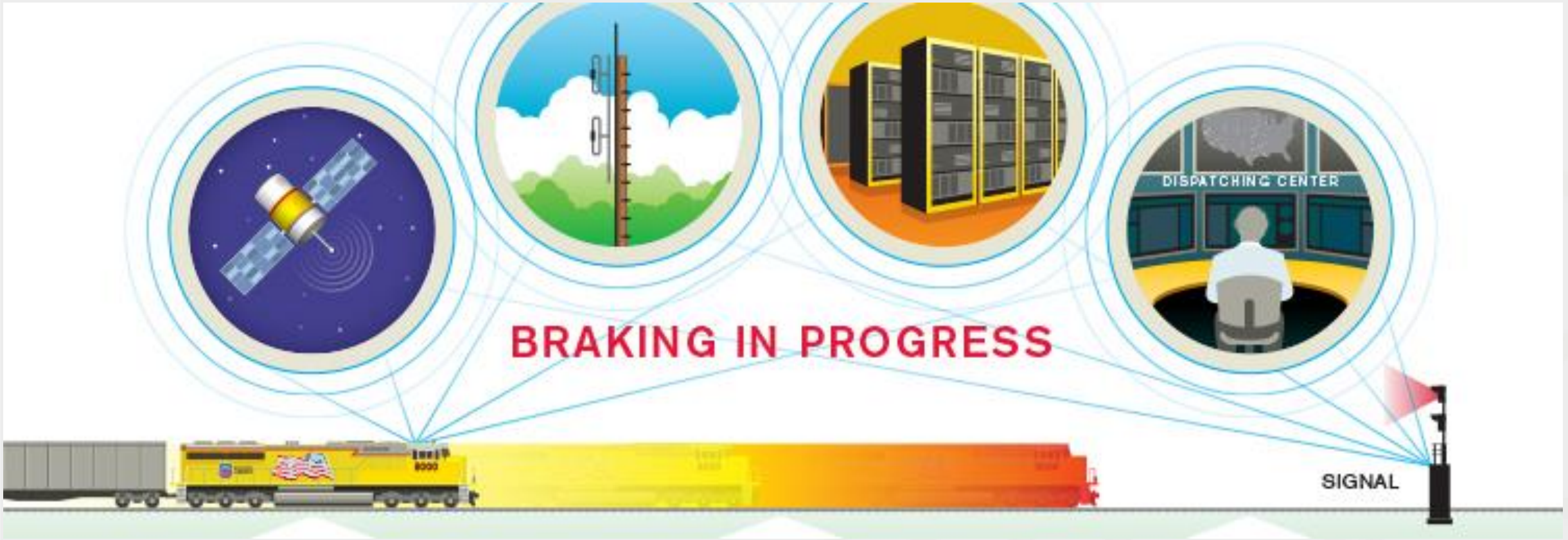
- A helyadatokból és a szenzorokból kiderül, hogy mozog-e az autó
- De figyelheti-e a gyártó az autó ezen paramétereit?



Autonóm közlekedés

Gépjárművek eltérítése

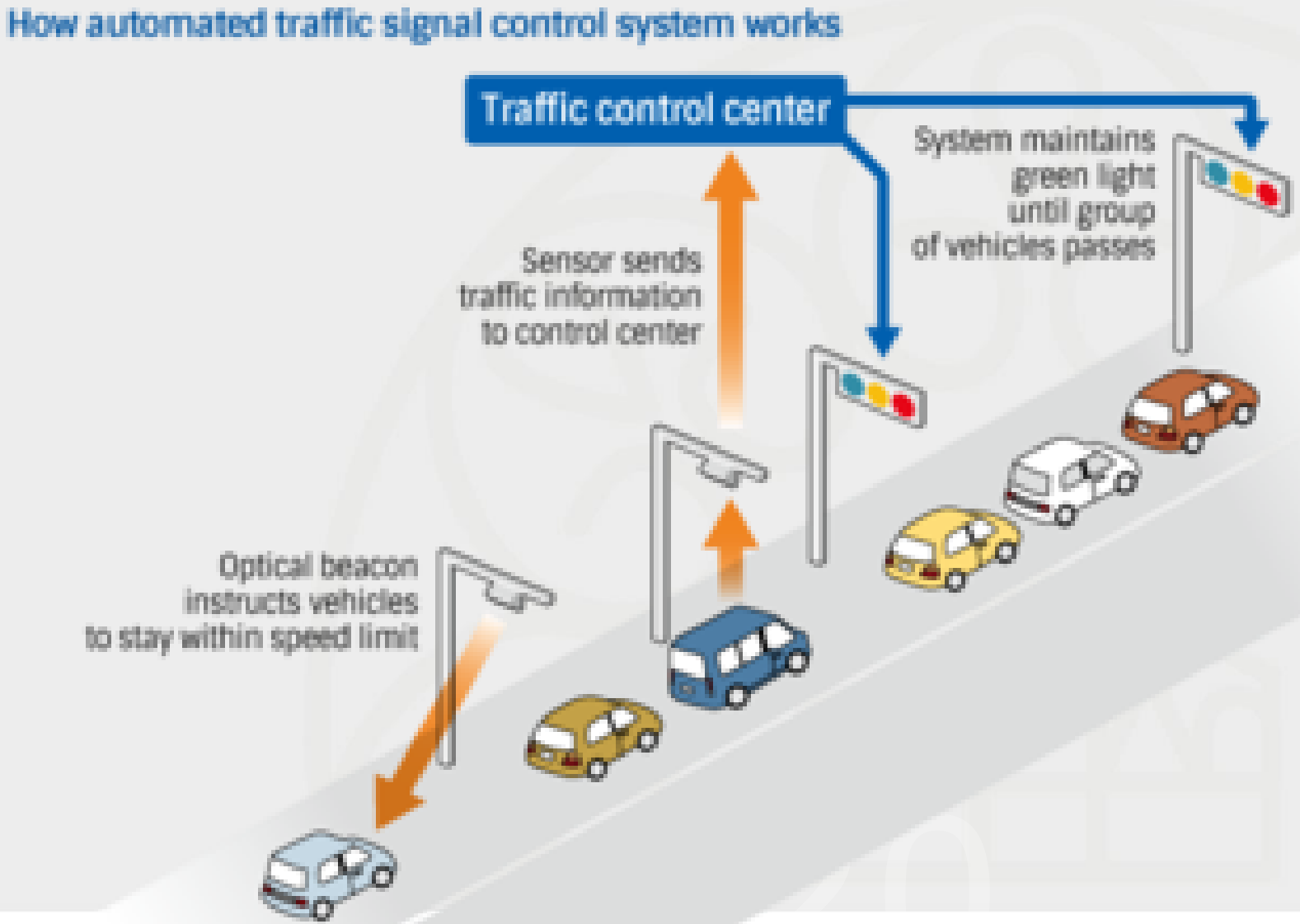
Egy kártékony kód tönkreteszi/befolyásolja a jármű szenzorokat



Vonatbefolyásolás (PTC)

- Egy rosszindulatú támadó bejut a PTC rendszerbe, ahol manipulálja az irányítást…
- Interoperabilitási problémák adódnak az egyes rendszerek között

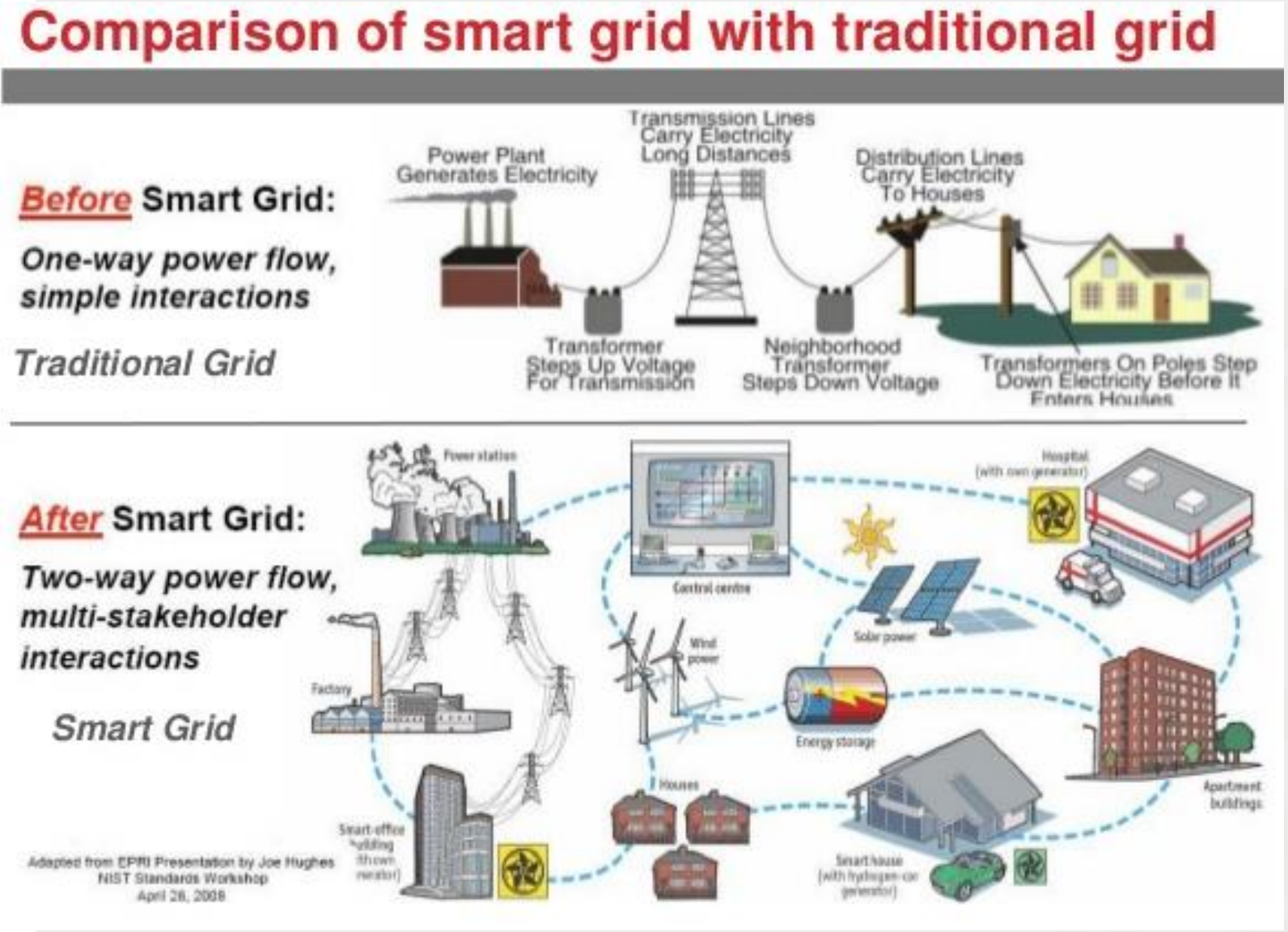
Közlekedésirányítási rendszerek



Egy rosszindulatú támadó manipulálja a V2V és V2I jeleket

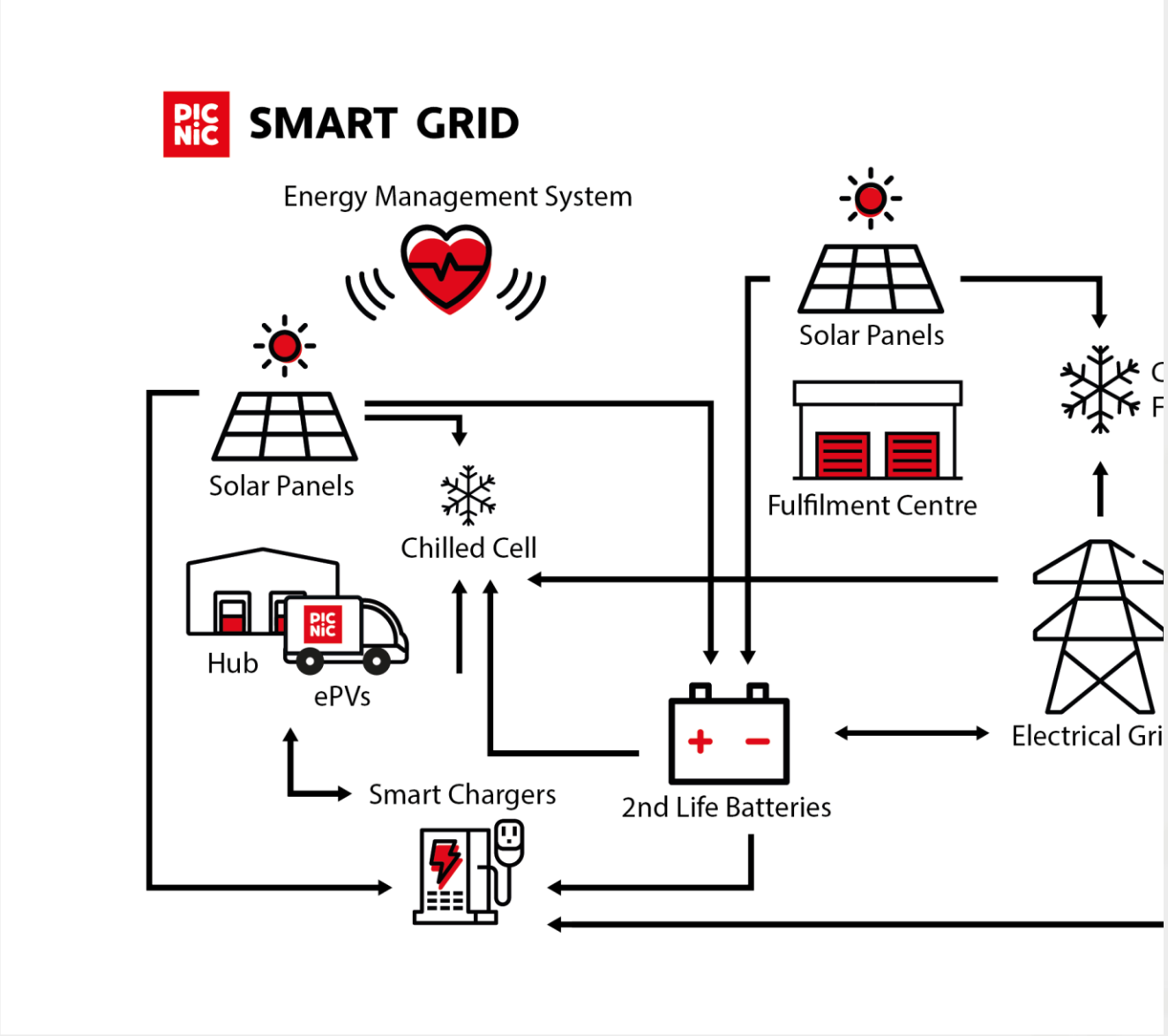
Egy rosszindulatú támadó megzsarolja a gépjármű-tulajdonosokat vagy gyártókat (pl. ransomware)

V2V és V2I kommunikáció



Okos energia elosztás és átvitel

- Egy rosszindulatú támadó hozzáférést szerez a SCADA rendszerhez
- Egy rosszindulatú támadó jogosulatlan hozzáférést szerez az erőmű hagyományos IT rendszereihez
- A „régi” és az „új” rendszerek találkozása előre nem látott problémákat okoz

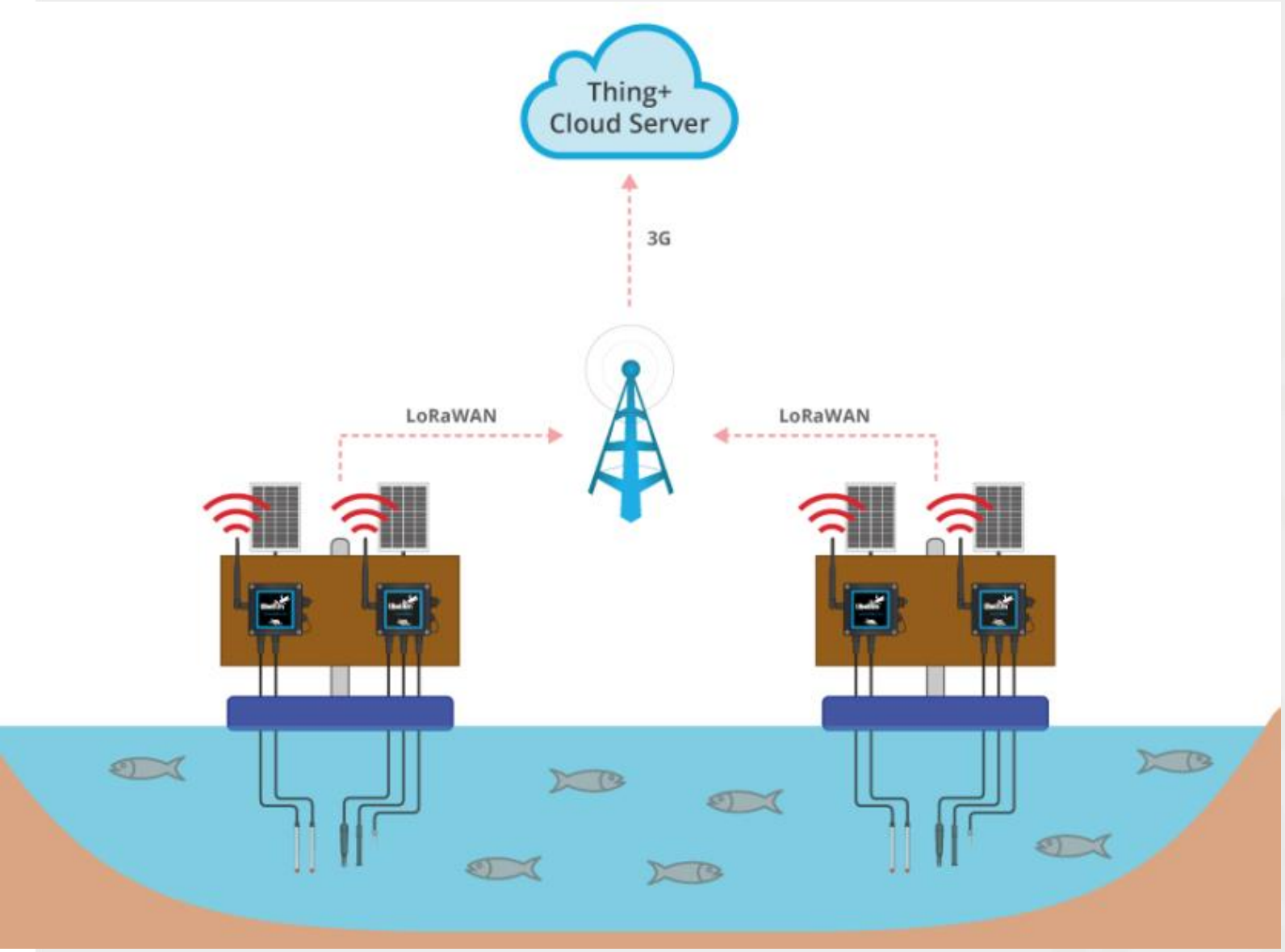


Okos energia elosztás és átvitel

- Egy rosszindulatú támadó kompromittálja az átviteli rendszert, ezzel megfosztva a felhasználókat az áramellátástól
- Egy rosszindulatú támadó manipulálja az energiaárakat mutató adatokat, emiatt a rendszer inkonzisztens módon irányítja a megtermelt energiát

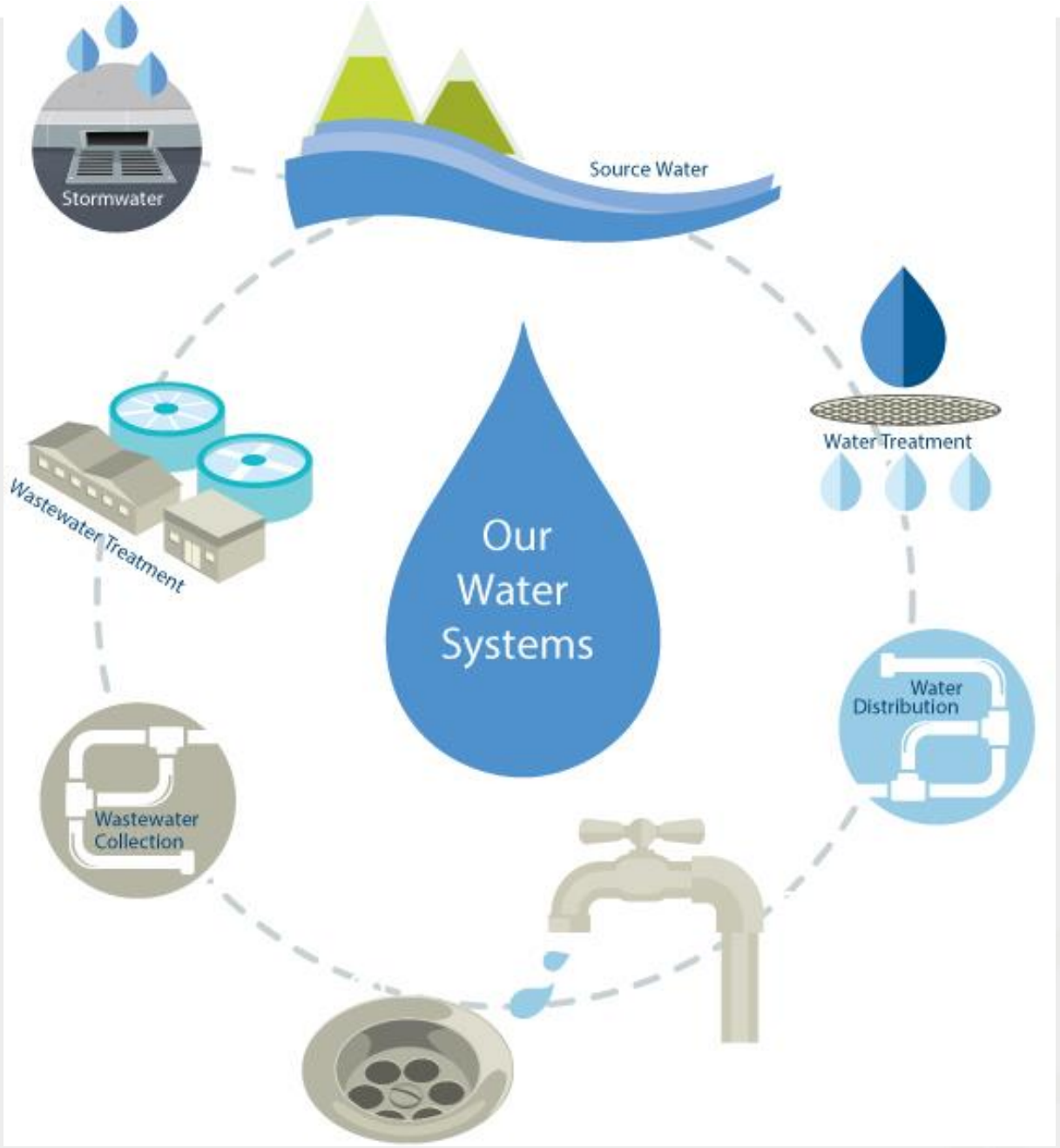
Okos mérőhelyek

- A mérőhelyek elleni támadással a támadó be tud jutni a háztartások belső informatikai hálózatába
- A mérőhelyek elleni támadással a háztartások áram nélkül maradnak



Okos vízkezelés

- Kibertámadás éri a vízkezelő központot, ezen keresztül olyan hatást érnek el, mely hat a közegészségügyre
- Az információs rendszeren keresztül teszi tönkre a támadó a vízbázist és okoz környezeti katasztrófát



Okos infrastruktúra

- A támadó rendkívüli időjárási helyzetben teszi lehetetlenné, pl. a felgyűlt csapadékvíz elvezetését
- Egy támadó távolról behatol a rendszerbe és lekapcsolja az érzékelő szenzorokat, így szennyezett víz kerülhet a háztartásokba
- Az előbbiekkel fenyeget

Okos infrastruktúra

- Egy rosszindulatú támadó távolról manipulálja a víztárolók berendezéseit, ezzel pl. áradást okoz
- Egy rosszindulatú támadó távolról manipulálja a biztonsági berendezéseket, ezzel fedve el a potenciális veszélyhelyzetet

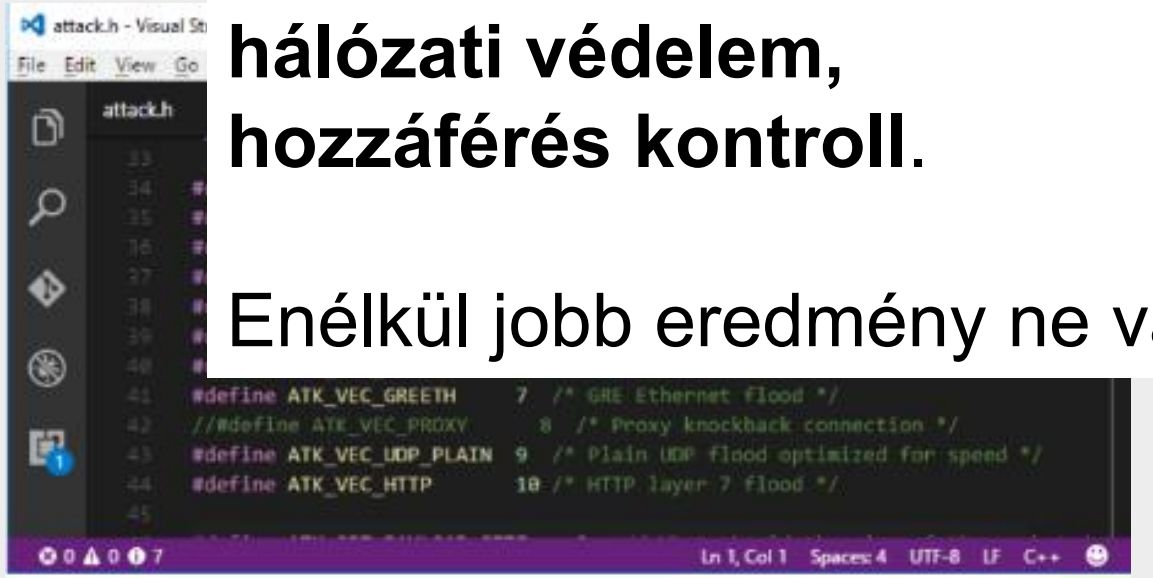
IoT esettanulmány: Mirai botnet

IoT esettanulmány: Mirai botnet

- Első megjelenés: 2016. augusztus
- Célpontok: régebbi Linux alapú IoT eszközök, elsősorban IP kamerák, routerek
- Fertőzési sorrend:
  - IP tartományok scannelése elérhető eszközök után
    Sebezhető eszközök esetén hozzáférés beégetett jelszavakkal
    A bot telepítése, a riválisbotok kiirtása
    Csatlakozás a C&C szerverhez
    Igény szerint támadás

Tanulság:
Frissítés,
hálózati védelem,
hozzáférés kontroll.

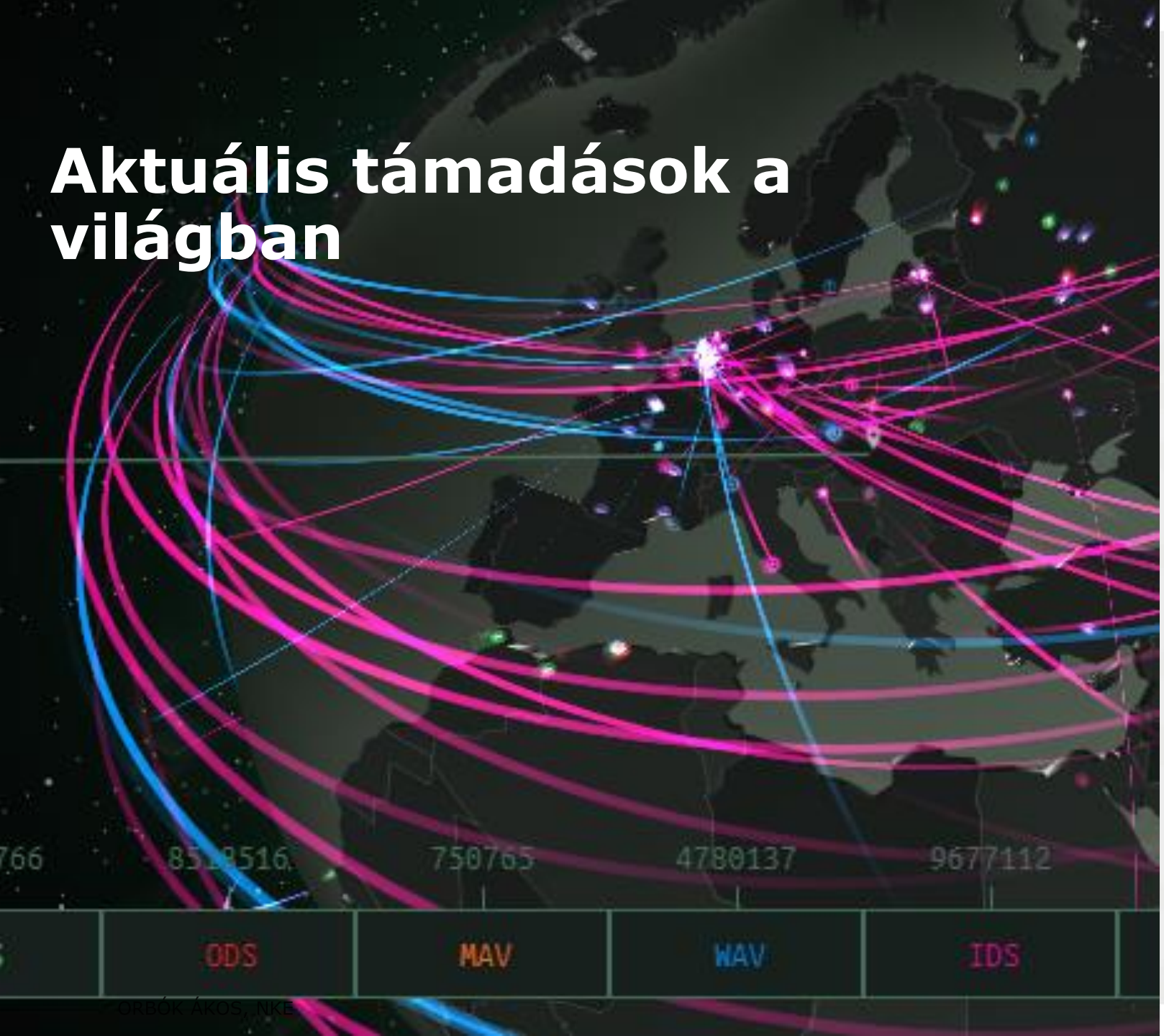
Enélkül jobb eredmény ne várjunk!



Forrás: Graham, R.: *Mirai and IoT Botnet Analysis*

- pont: DNS szolgáltatások, a legnagyobb a Dyn lgáltató ellen -> Port 53 UDP flood, ~600GBps ~1.2TBps között
- Számos szolgáltatás leállt, pl. Netflix

Aktuális támadások a világban



https://cybermap.kaspersky.com/

https://threatmap.checkpoint.com/

https://www.digitalattackmap.com

Megelőzés, mint a legolcsóbb kockázatkezelési megoldás

Irodalomjegyzék

Elmaghraby, A. S., Losavio, M. M.: *Cyber security challenges in Smart Cities: Safety, security and privacy*. Journal of Advanced Research. Volume 5, Issue 4, July 2014, Pages 491–497. http://www.sciencedirect.com/science/article/pii/S2090123214000290

Graham, R.: *Mirai and IoT Botnet Analysis*, RSA Conference 2017, https://www.rsaconference.com/writable/presentations/file_upload/hta-w10-mirai-and-iot-botnet-analysis.pdf

Orbók, Á.: *Challenges and Risks in The Smart Cities,* In: Eva Kellnerová, Kateřina Pochobradská, Kristýna Binková (ed.): New Approaches to the National Security : 11th PhD Conference Proceedings. 443 p.

US. Department of Homeland Security: *The Future of Smart Cities: Cyber-physical Infrastructure Risk*. August, 2015.

Zhu, Y., Zuo, J.: *Research on Security Construction of Smart City*. International Journal of Smart Home, Vol. 9, No. 8 (2015), pp. 197-204 http://www.sersc.org/journals/IJSH/vol9_no8_2015/21.pdf

KÖSZÖNÖM A FIGYELMET!

uni-nke.hu