A DRÓNOK KIBERBIZTONSÁGI ASPEKTUSA

INFORMÁCIÓVÉDELEM MENEDZSELÉSE CIII. SZAKMAI FÓRUM

2022. NOVEMBER 16.

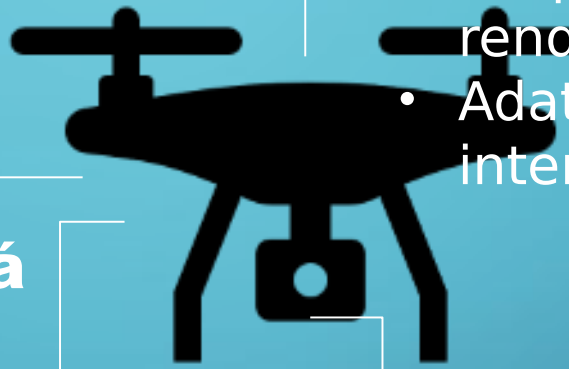
KÉSZÍTETTE: KATONA GERGŐ

DRÓN RENDSZER

GPS

Repülés vezérlő rendszer

- Központi vezérlő rendszer
- Adatkapcsolati interfész



Kommunikáció

Wi-Fi 802.11; Bluetooth

Irányítóközpont

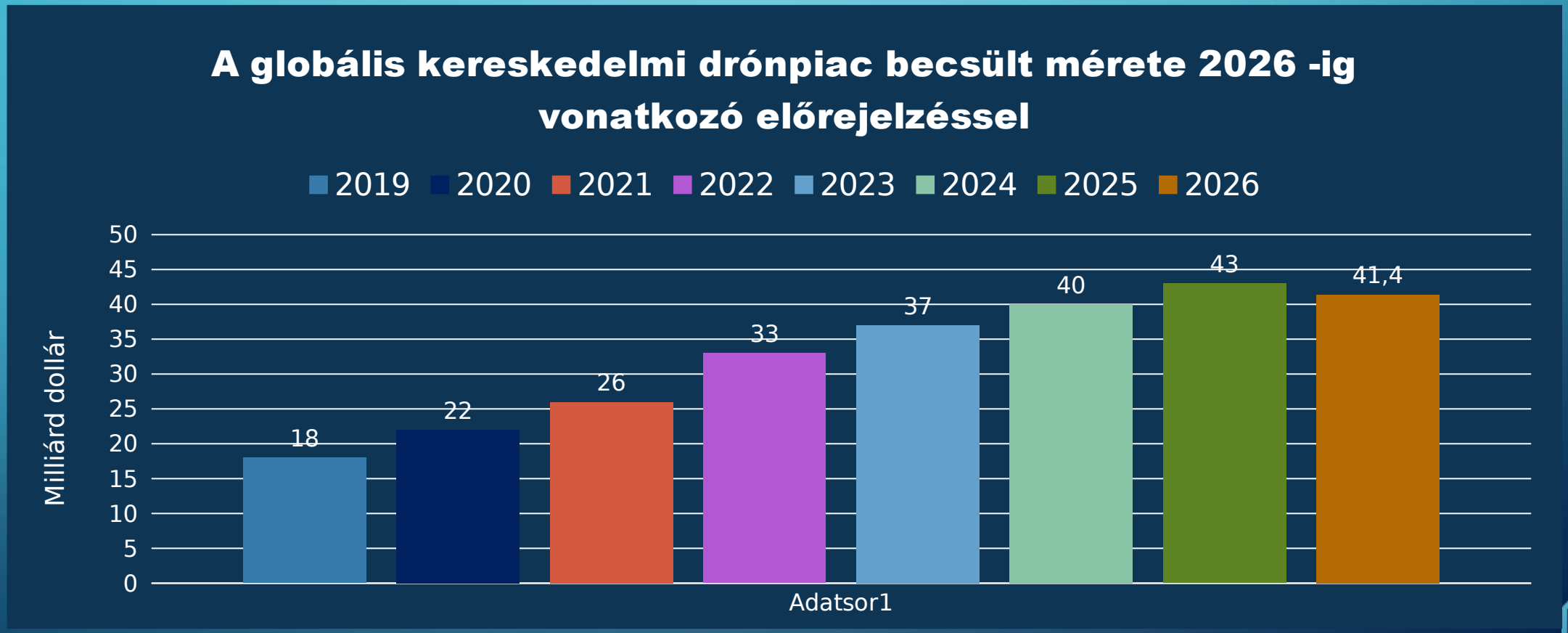
Személyzet

Hasznos teher

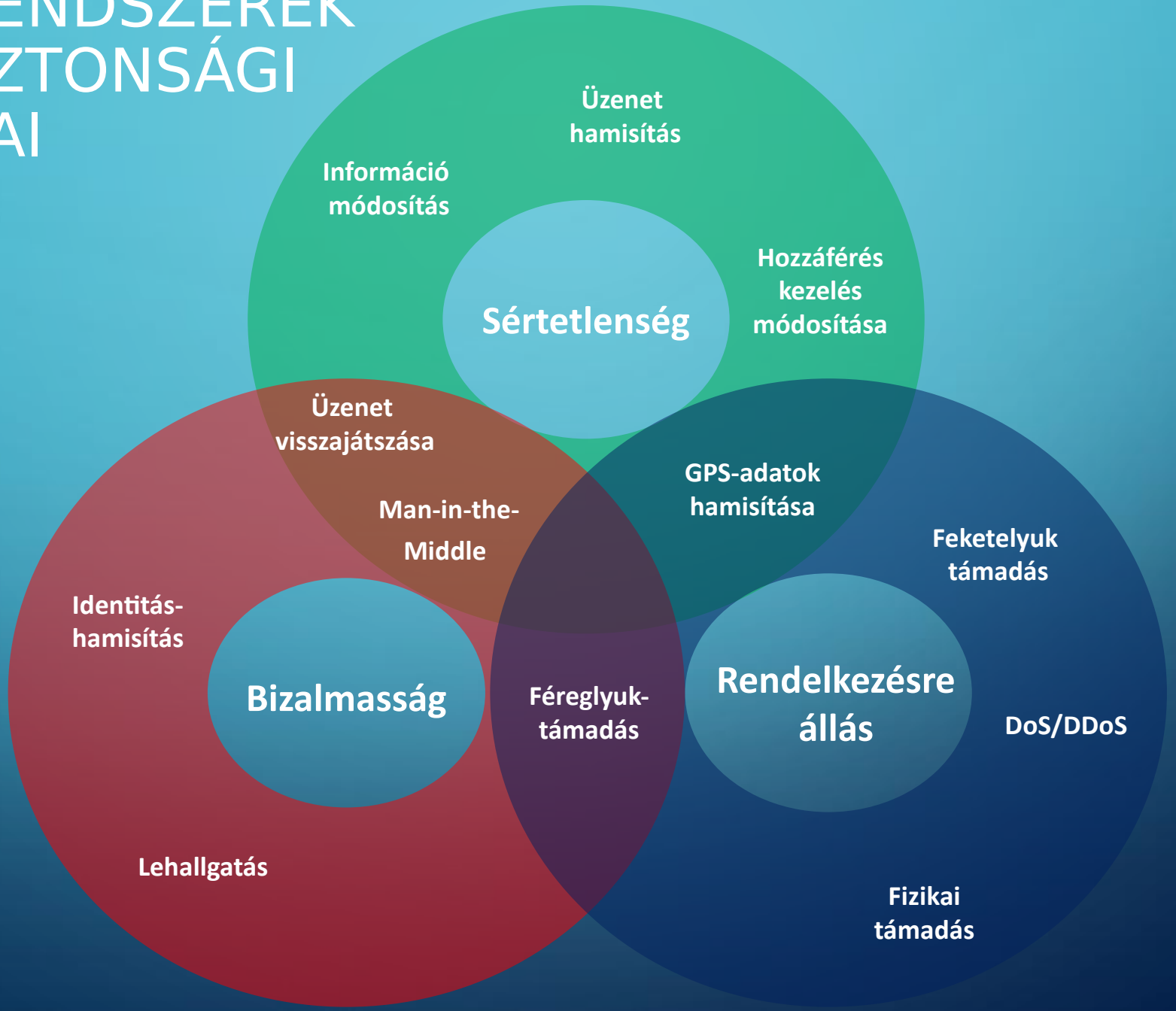
- **Távoli pilóta vezérlés**
- **Távoli felügyelt vezérlés**
- **Teljes autonóm**

Saját szerkesztés, Forrás: Statista

DRÓNOK SZÁMOKBAN



DRÓN RENDSZEREK KIBERBIZTONSÁGI KIHÍVÁSAI

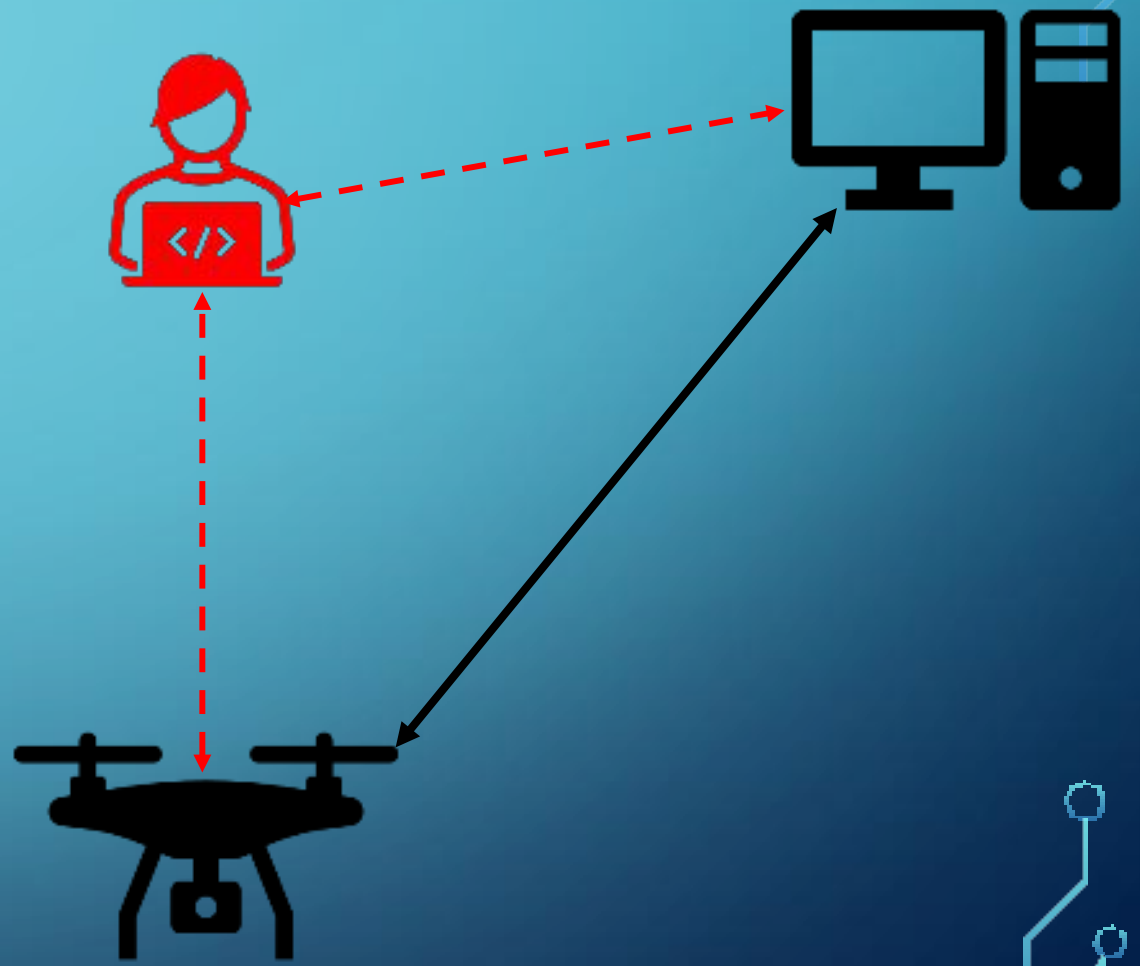


FENYEGETÉSEK

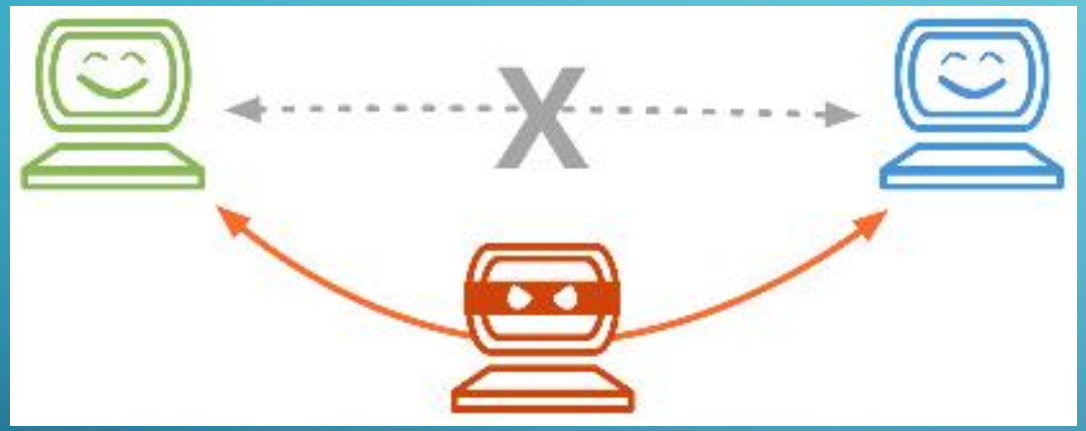
Identitás-hamisítás: lehetővé teszi a támadó számára, hogy olyan identitásnak álcázza magát, amely jogosan helyezkedik el a rendszerben, rendelkezik megfelelő jogosultsággal.

Üzenet visszajátszása: a jogos adatokat a támadó észleli, és elfogja, amit később újra és újra továbbít.

Lehallgatás: az UAV kommunikáció jogosulatlan valós idejű lehallgatását jelenti, amely lehetővé teszi a támadó számára, hogy lekérje az eszközök közötti bizalmas információkat.



FENYEGETÉSEK



Hozzáférés kezelés módosítása célja a hozzáférés kezelő rendszerek elérése

Man-in-the-Middle támadások: A Man-in-the-Middle támadások lehetővé teszik a támadók számára, hogy rögzítsék a drónok és vezérlő, érzékelők közötti kommunikáció adatait.

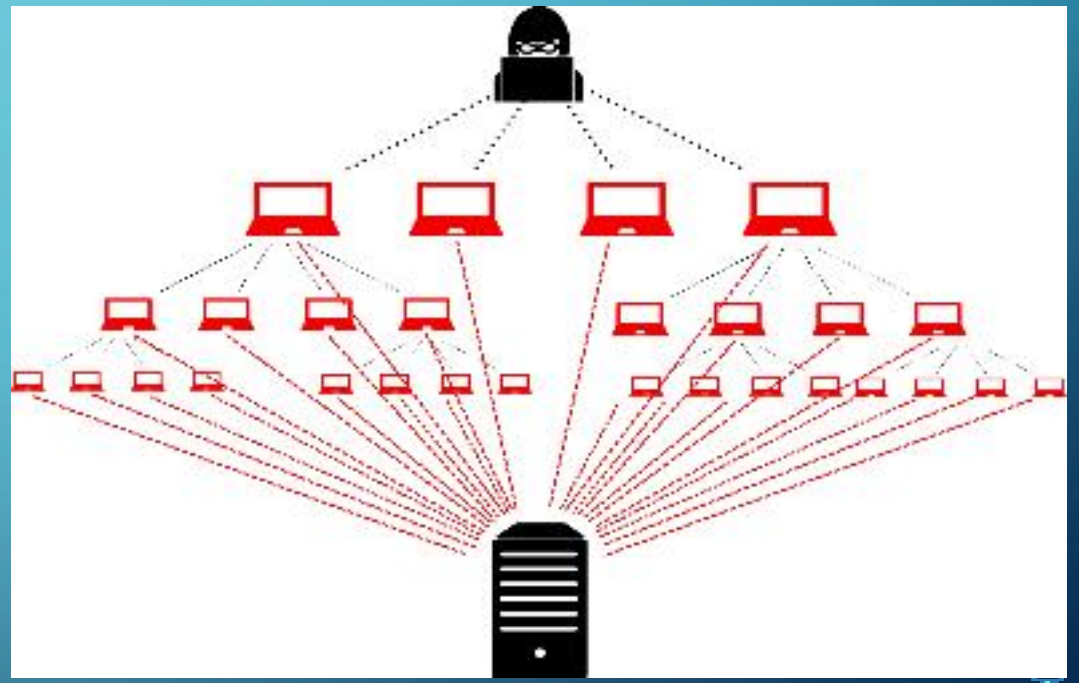
Üzenethamisítás A drón rendszerek üzenethamisító támadása alatt a nyilvános/nyitott csatornán végrehajtott korábbi munkamenetekben végrehajtott bejelentkezési kérelmet hamisítják a hitelesítési protokoll lefutása során. Ezt követően a támadó módosíthatja és továbbíthatja az üzenetet a felhasználónak.

FENYEGETÉSEK

- **A GPS-adatok zavarása vagy hamisítása**: A GPS adások szabadon hozzáférhetőek, titkosítatlan és nem hitelesített jelek. A GPS-jelek nyílt jellege lehetővé teszi a hamisítási támadásokat, ahol hamis jeleket lehet generálni. Ezenkívül a GPS-jelek könnyen elakadhatnak, így a drón nem képes GPS jelek alapján meghatározni a helyzetét.

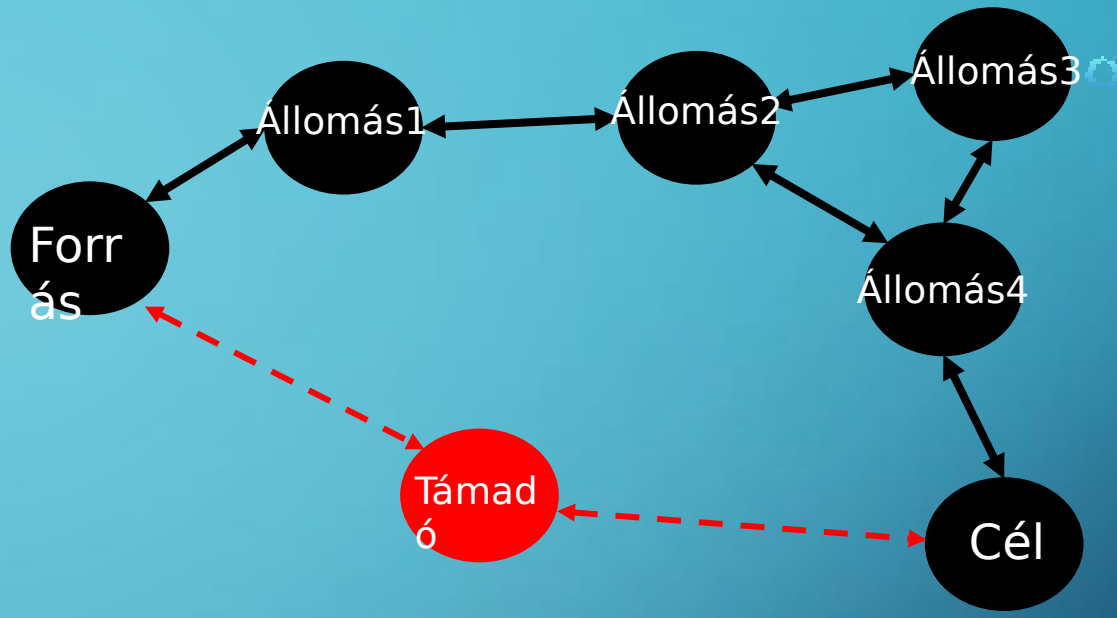
- **Fizikai támadás**: Ezen támadások a hardverek fizikai megkárosítását, illetve megsemmisítését helyezik a középpontba.

- **Szolgálatás megtagadás (DoS, DDoS)**: Mivel e drónok megfelelő működéséhez folyamatos kommunikáció szükséges, ezért ha ezen csatornákat egy támadó elárasztja akkor az eszközök elérhetetlenek lesznek.

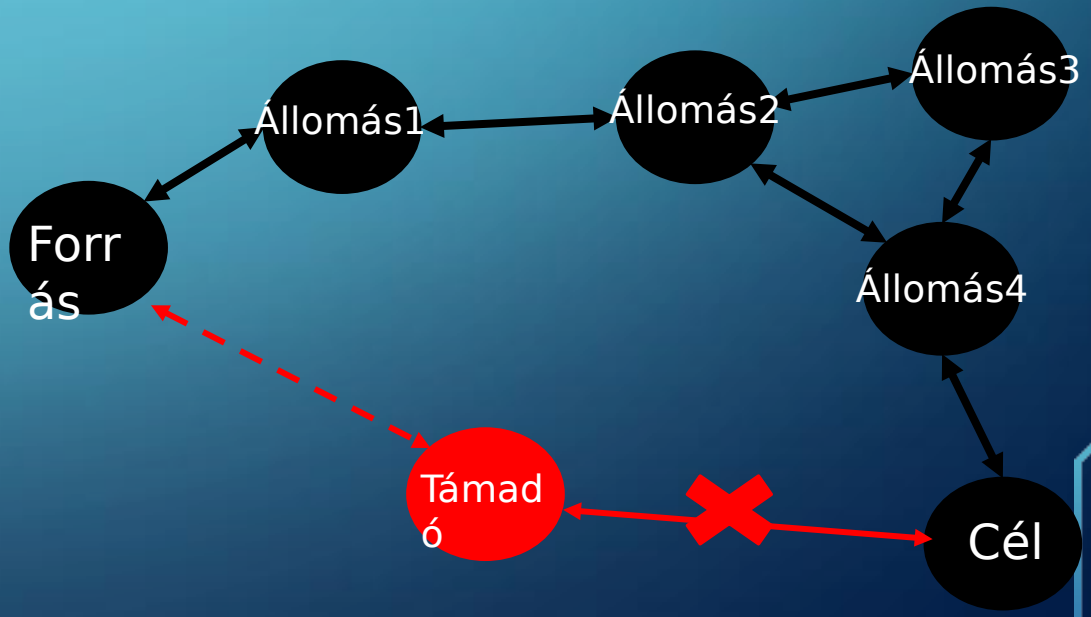


FENYEGETÉSEK

- **A féreglyuk-támadások**: amelyek úgy működnek, hogy kapcsolatot hoznak létre két csomópont között. Ez a kapcsolat olyan két csomópont között fordulhat elő, amelyek tipikusan nincsenek közel egymáshoz (más szóval több, mint egyetlen ugrás távolságra). A féreglyuk adatokat fogad a forráscsomóponttól és továbbítja a célállomásnak.



- **Feketelyuk támadás**: Ez abban különbözik a féreglyuk támadástól, hogy itt a támadó, mikor hálózati csomóponttá válik nem továbbítja a csomagokat, hanem eldobja azt.



ESETTANULMÁNYOK

- **Források:** Google Scholar, Scopus

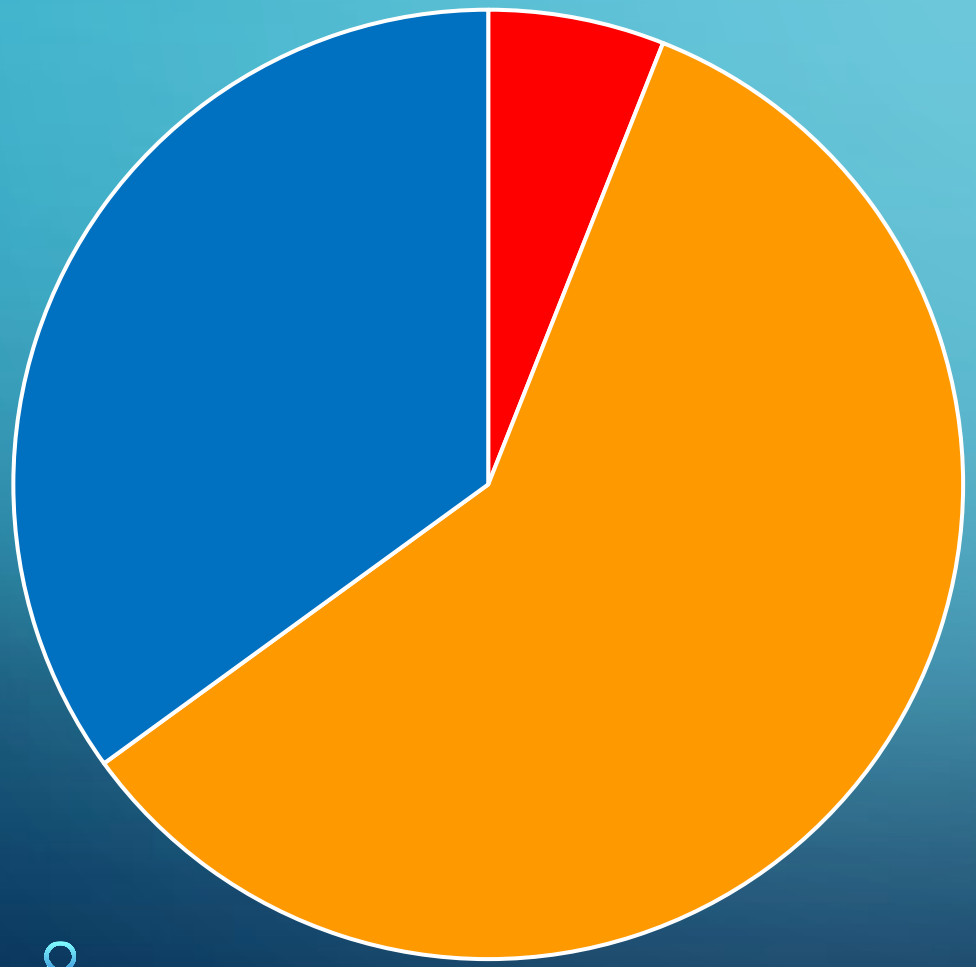
- **Vizsgált esetek száma:** 19 db

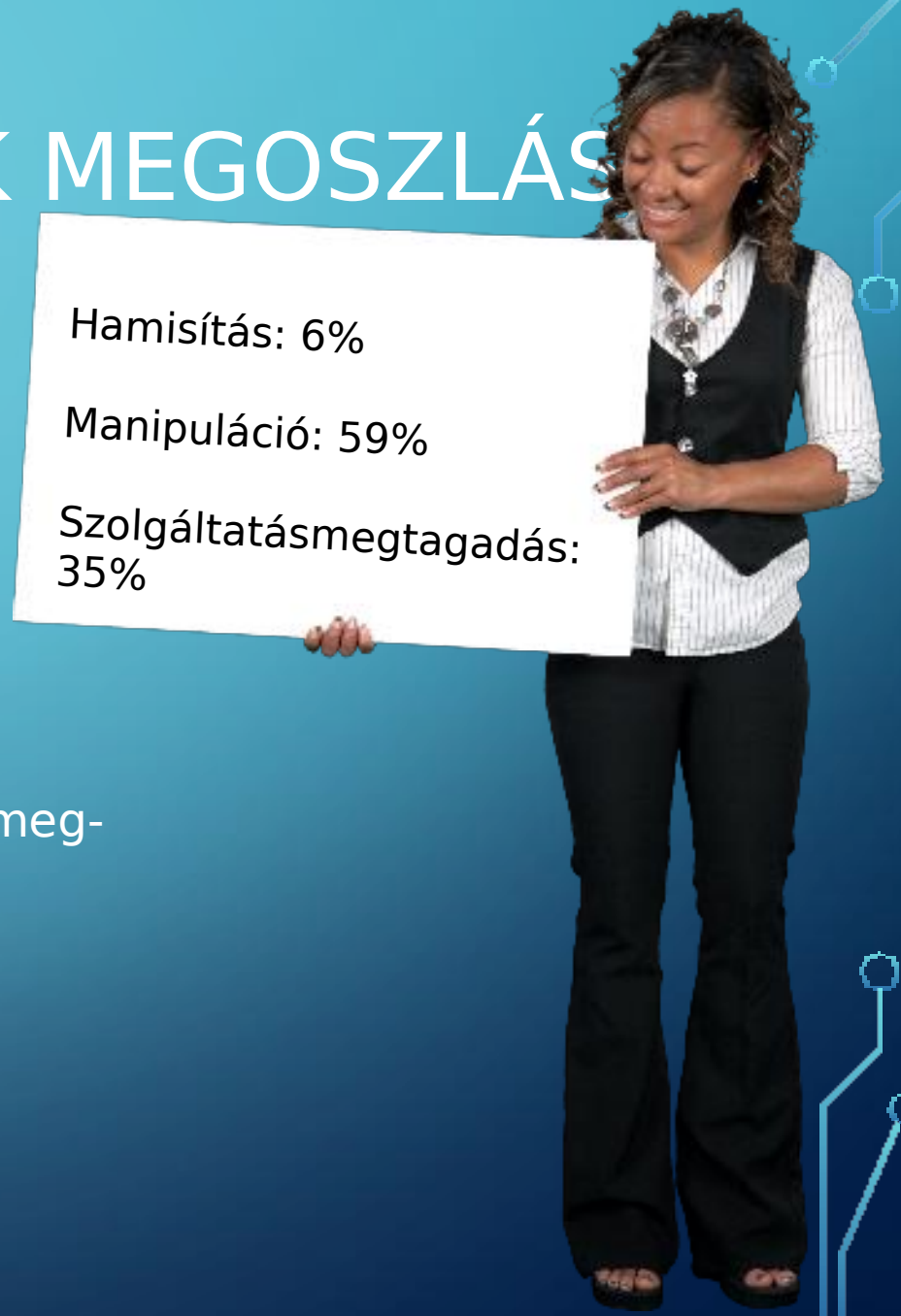
Scopus®

TÁMADÁSOK CSOPORTOSÍTÁSA ESETTANULMÁNYOK ALAPJÁN

- **Hamisítás**
  - **Üzenet hamisítás, GPS-adatok hamisítása, Személyazonosság-hamisítás**
- **Manipuláció**
  - **Üzenet visszajátszása, Információ módosítás, Man-in-the-Middle, Hozzáféréskezelés módosítás**
- **Szolgáltatásmegtagadás**
  - **DoS/DDoS, Feketelyuk támadás, Fizikai támadás, Féreglyuk támadás**

TÁMADÁSOK MÓDSZERÉNEK MEGOSZLÁS

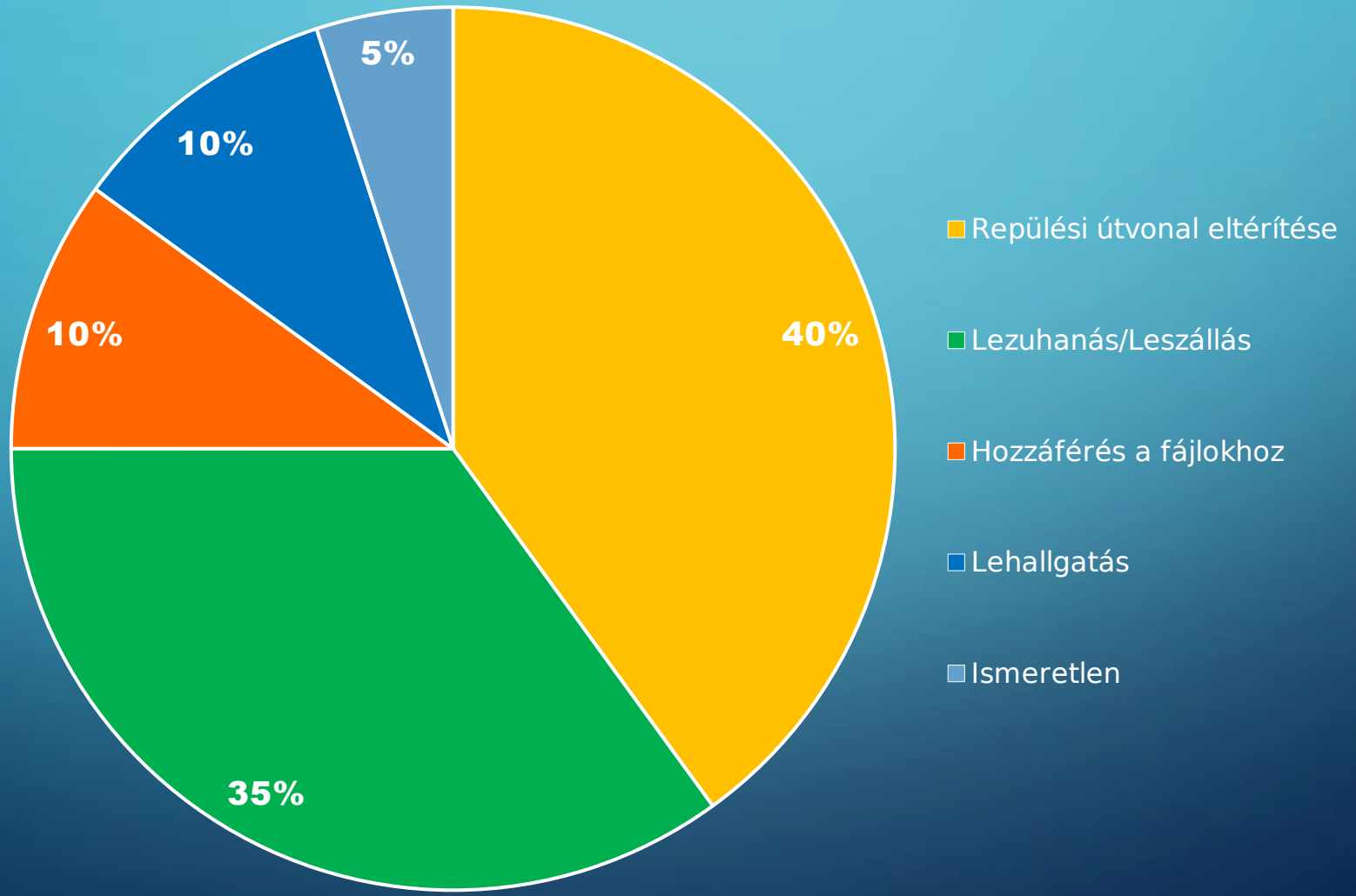




TÁMADÁSOK CÉLJAINAK CSOPORTOSÍTÁSA

- Repülési útvonal eltérítése
- Lezuhanás/Leszállás
- Hozzáférés a fájlokhoz
- Lehallgatás

TÁMADÁSOK CÉLJAINAK CSOPORTOSÍTÁSA



VÉDELMET ERŐSÍTŐ TÉNYEZŐK

- Külsős szolgáltatók megfelelése
- BCM kialakítása
- ISMS bevezetése
- Általános tudatosítás
- CISO kijelölés
- Hatékony incidens menedzsment
- IBSZ kialakítása
- Kockázat-menedzsment
- Szerep alapú biztonsági képzés
- Hozzáférés kezelés

- Fizikai hozzáférés ellenőrzés
- Tűz- és vízkár védelem
- Szállítás
- Áramellátás
- Karbantartás
- Hőmérséklet, páratartalom

- Tűzfalak és hálózati szegmentálás
- Alkalmazás biztonság és biztonságos tervezés
- Naplózás
- Az eszközök alapértelmezett adatainak módosítása
- Sérülékenység vizsgálat
- Adattitkosítás
- Szoftver- és hardverfrissítések
- Vírusírtó Rendszer
- Behatolásészlelő és megelőző rendszerek (IDS, IPS)
- Erős felhasználói hitelesítés

KÖSZÖNÖM A FIGYELMET!

KATONA.GERGO@UNI-NKE.HU