NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA

INFÓ ÉRA -2025

Zsakó László emlékkonferencia

EIVOK 61

Információbiztonsági szekció

Gondolatok a kiberbiztonság alapjairól

Oláh István c. egyetemi docens
EIVOK alelnök

- **Nemzeti Közszolgálati Egyetem (NKE):**

  Információs rendszerek és hálózatok biztonsága,

  Pénzintézeti információs rendszerek védelme,

  Szoftverfejlesztés biztonsági kérdései egy aktuális sebezhetőség tükrében,

  Bizalom a kiberbiztonságban.

- **Óbudai Egyetem (ÓE):**

  IT rendszerek üzemeltetésének logikai biztonsági követelményei

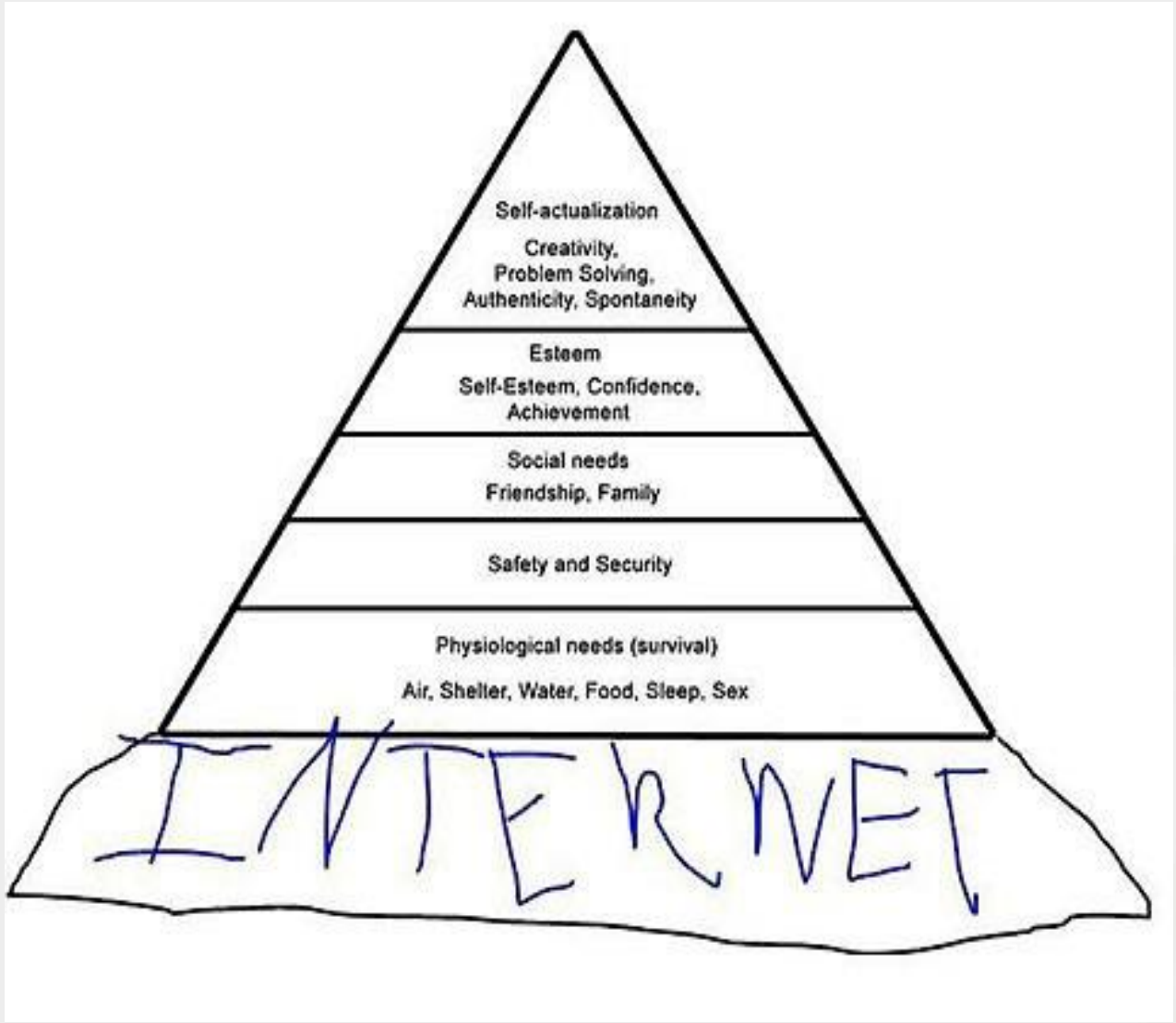
- **Hírközlési és Informatikai Tudományos Egyesület (HTE):**

  Információbiztonsági Szakosztály-EIVOK, alelnök

https://www.hte.hu/eivok

- eivok@hte.hu
- Istvan.olah@hte.hu

A Digitális Maslow



MIK EZEK?

A lehetséges válaszok.

- Kütyük, izék, masinák,
- Játékok,
- **Testrészeink, végtag kiegészítők,**
- Amikkel fekszünk, kelünk,
- **Amiket egész nap nézünk, avagy ki ural kit?** A használó a képernyőt, vagy a képernyő a használót, de ki is vezérli a képernyő tartalmát?
- Amiket már minden gyerek, unoka tud jól használni, de ez nem így van, mert a **használni és tudatosan használni nem ugyanaz!**
- **Munkaeszközök,**
- **Adathordozók,** rólunk, családunkról, ismerőseinkről, munkahelyünkről, etc. minden adat megtalálható rajtuk, vagy rajtuk keresztül, ma egy közepes közösségi szolgálató is többet tud rólunk mint bárki más, milyen jogalappal?
- **Tárgyi eszközök, adatvagyon probléma a számvitelben, és a mindennapokban,**
- **Veszélyforrások,**
- **……**


www.china-defense-mashup.com

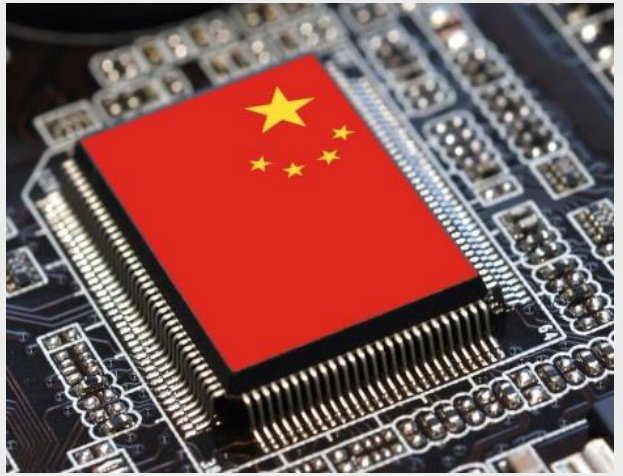
Hol lehet csatát vívni?

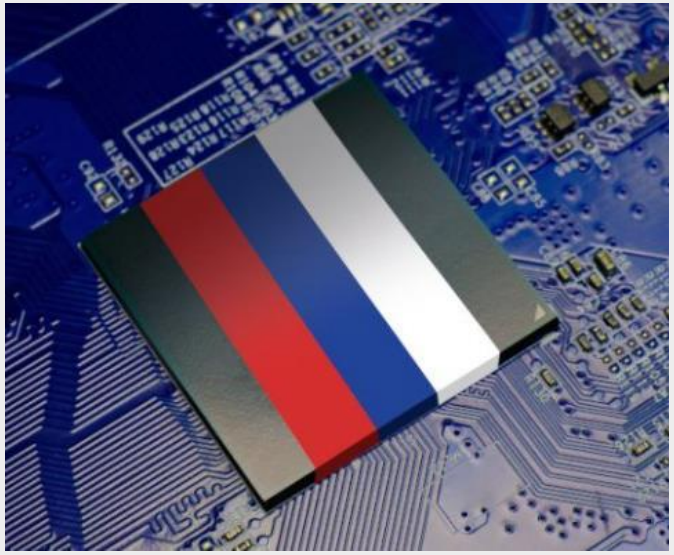
- **Föld,**
- **Víz,**
- **Levegő,**
- **Világűr,**

- **KIBERTÉR!!!!!**

MIK EZEK?

Benne van mindenben..??



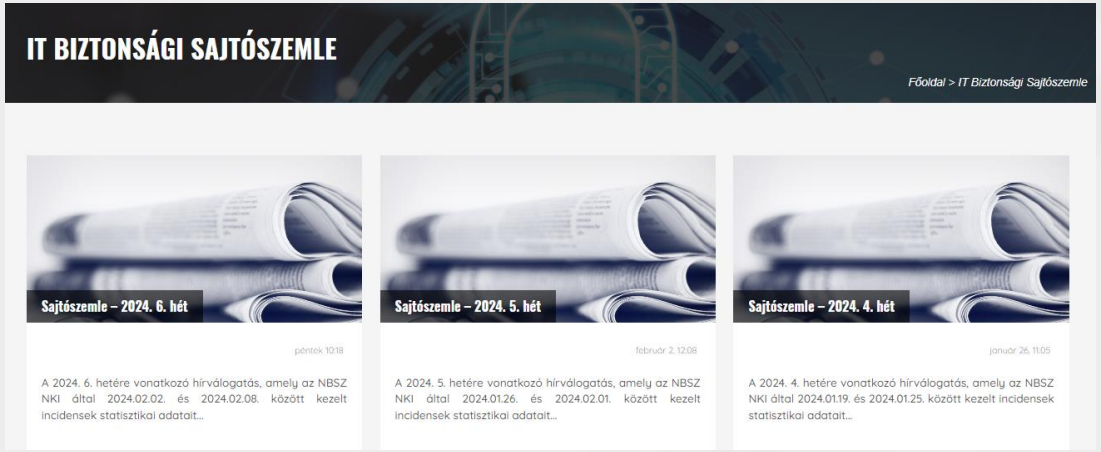


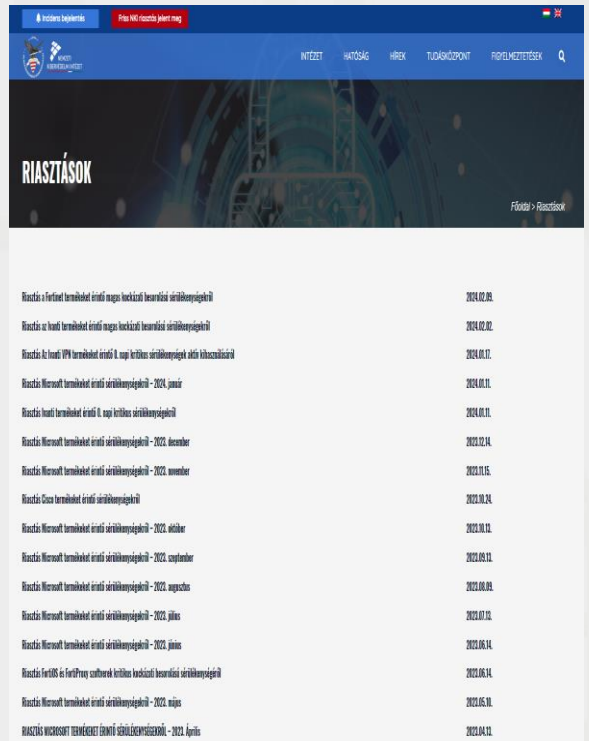
Mi van benne, mint képesség?

- Megfigyelés,
- Lehallgatás,
- Befolyásolás,
- Kémkedés,
- …
- Kik által birtokolva a képességek?
- Milyen jogszabályi, társadalmi, szervezeti, egyéni felhatalmazás alapján?
- A használat első pillanatától, okos-e mindent tiltani taktika?
- **A TUDATOS használat, mint TANULHATÓ KÉPESSÉG kiemelten fontos minden felhasználó esetében! A szervezetek vezetőinek a feladatai közt TOP1 szinten szükséges szerepeljen.**
- **Általános iskola 3. osztálytól: Digitális Kultúra tárgy (15 év múlva látjuk a hatást majd), lesz-e ECDL+ = IT-KIBERJOGSI?**

Honnan tudhatunk a fenyegetettségekről?

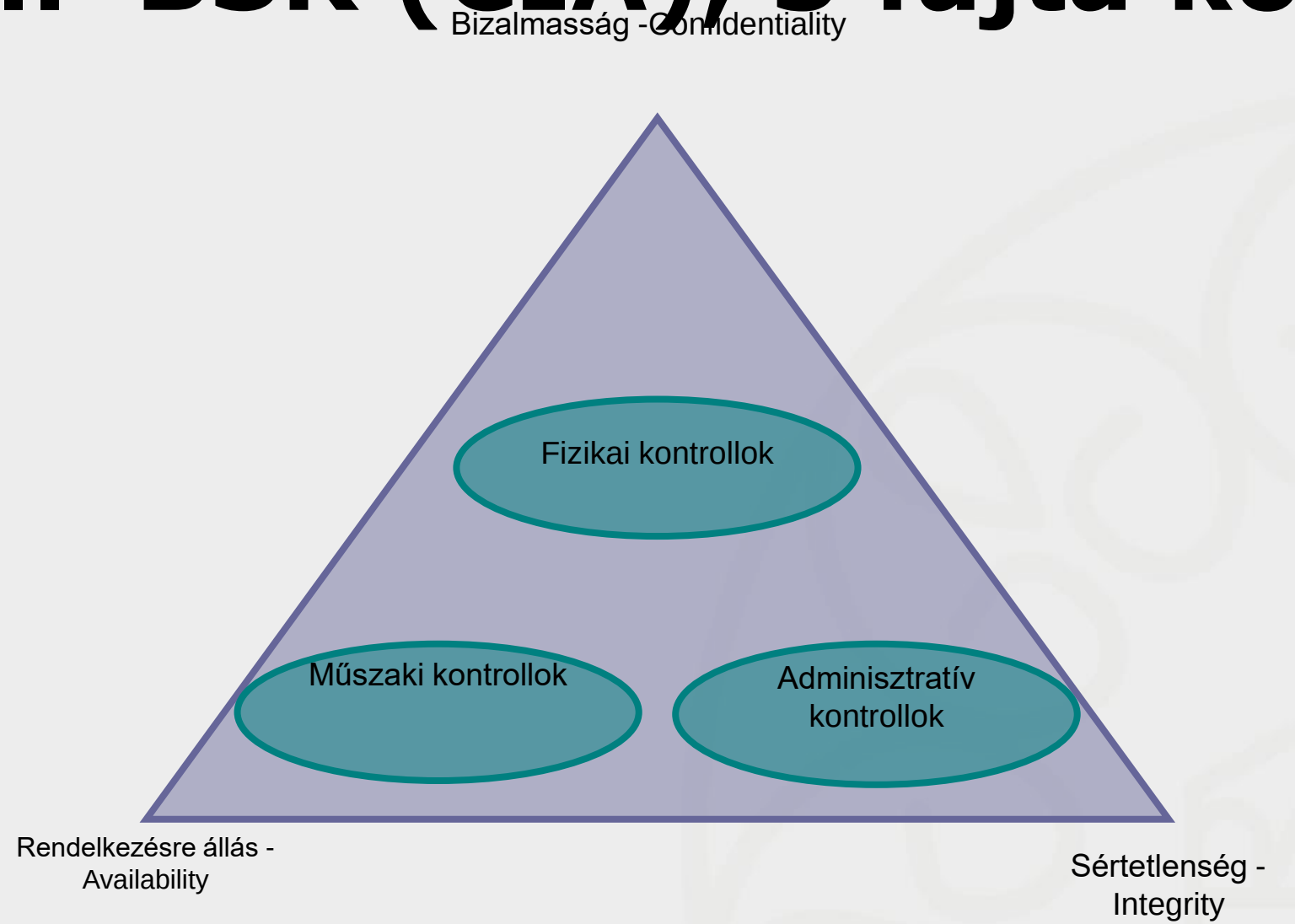
- Napi sajtó, minden nap 1-2 hír magyarul is, **de tegyük fel a kérdést**, hogy ez érint-e minket / családunkat / munkahelyünket
- Hazai, és nemzetközi szakmai portálok, hírlevek, vásárolható információk, elemzések, és az NKI:
- NKI weboldala:





https://nki.gov.hu/

3 szó.. BSR (CIA), 3 fajta kontroll.



A A A ! a klasszikus Ki, Mikor, Mit?

- **Authentication: felhasználó azonosítás**
- **Authorization: jogosultságkezelés**
- **Accounting: naplózás**

Forrás: Microsoft Copilot

Az adatvagyon

- Mérjük fel a szervezet adatait, soroljuk be az adatokat biztonsági osztályba!
- Hol érhetők el, hogy kezelhetők?
- Minden tárolási helyet gyűjtsünk össze, e-form, papír, fénykép, stb.!
- Kik férhetnek hozzájuk, szabályozzuk, és ezt mint elvárást érvényesítsük az IT rendszerekben és ne fordítva:
  - Szervezet munkavállalói, kiemelt figyelem a rendszergazdákra!
  - Szervezet partnereinek munkavállalói, külső üzemeltető,
  - Ügyfelek,
  - Hatóságok,
  - Köznyilvános adatok,
  - Akikre nem szoktak gondolni, távközlési cégek, felhő szolgáltatók, etc.,
- Mit nem lehet egy embernek, azaz a kizáró szerepkörök (SOD mátrix)?
- Az IT ökószisztéma összes eleme is értelemezhető adatként, azaz IT környezeteket (fejlesztői, teszt, oktatási, éles, etc.) ugyanúgy mentsük mint az adatokat,
- Az adatok mentéséről, archiválásáról úgy gondoskodjuk, ezeket ellenőrizzük, pl. hogy ne csupa nulla legyen a mentett állomány,
- Életciklus-menedzsment: létrehozás, használat, archív állapot, törlés,
- **Mindent naplózzunk, és a naplók BSR elemeiről gondoskodjuk, mert bizonyítékok!**
- Mindezeket a PDCA (tervezd, csináld, ellenőrizd, cselekedj, és kezd újra) elv szerint.

A Működés biztonsága

- Mérjük fel a szervezet működési folyamatait, soroljuk be a folyamatokat! pl. BIA módszertan,
- A besorolás szerint döntsünk arról, hogy szükséges-e egy incidens esetén a folyamatot fenntartani!
- Amennyiben igen, akkor erre legyen kész forgatókönyvünk, BCP,
- A forgatókönyveket teszteljük legalább évente!
- Egy BCP-hez határozzuk meg a szükséges IT-rendszereket és ne fordítva!
- Az IT-rendszereket e szerint soroljuk be a **rendelkezésre állás** szempontjából is (pl. SLA, OLA szintek),
- A besorolás alapján döntsünk arról, hogy szükséges-e többleterőforrás a rendszerben, készenléti tartalék rendszer, élesben folyamatosan rendelkezésre álló tartalék,
- Egy incidens (sok féle és fajta lehet) esetében legyen döntési szempontrendszerünk, **szereplőink,** és folyamatunk arra, hogy kell-e a tartalékra átállni,
- Az átállásra legyen kész és tesztet forgatókönyvünk (DR), amelyet a szervezetben minden szereplő begyakorolt,
- Rendelkezzünk naprakész kommunikációs tervvel és folyamattal (BCP itt is),
- Ha minta szükséges: „Az információszolgáltatásról szóló 54/2021. (XI. 23.) MNB rendelet 3. sz. mellékletében felsorolt technikai segédletek 2022,” **P-58**, **P-64**
- Mindezeket a PDCA (tervezd, csináld, ellenőrizd, cselekedj) elv szerint

Tudásmenedzsment, emberek

- Mérjük fel a szervezet érettségi szintjét, abból kiindulva készítsünk szervezeti és egyéni képzési terveket!
- Folyamatosan képezzük a legnagyobb kockázati forrást a FELHASZNÁLÓKAT, azaz saját magunkat, családtagjainkat, kollegáinkat,…., legalább évente egy alkalommal a munkaszervezetben!
- **A védelem feladatai során ne az IT-üzemeltetőkre, IT és információbiztonsági szakemberekre, hanem mindenkire gondoljunk, mert csakis a közös védelem lehet eredményes!** (leggyengébb láncszem),
- Időszakonként végezzünk próbát, ahogy pl. tűzriadó próba is van,
- A vezetőket külön készítsük fel az incidensek kezelésére,
- Mindezeket a PDCA szerint

Alapfogalmak

- **Artifical Intelligence:** a számítástechnika azon területe, amely olyan intelligens gépek létrehozására törekszik, amelyek képesek az emberi intelligenciát megismételni vagy meghaladni.

- **Machine Learning:** a mesterséges intelligencia olyan részhalmaza, amely lehetővé teszi a gépek számára, hogy a meglévő adatokból tanuljanak, és az adatok alapján döntéseket vagy előrejelzéseket hozzanak.

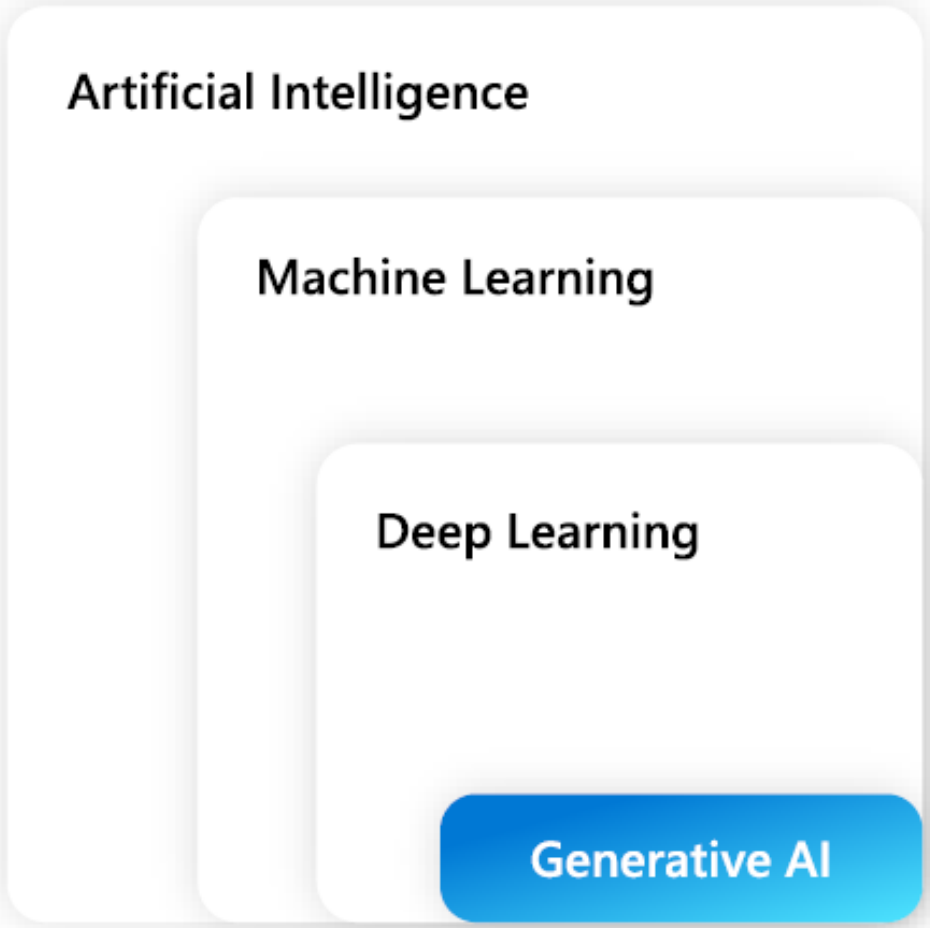
- **Deep Learning:** olyan gépi tanulási technika, amelyben neurális hálózatok rétegeit használják az adatok feldolgozására és a döntések meghozatalára.

- **Generative AI:** új írott, vizuális és auditív tartalmakat hoz létre kérések vagy meglévő adatok alapján

Forrás: Tóth Márton EIVOK-40

Vezetőknek

A brief history of AI



1950s

Artificial Intelligence

the field of computer science that seeks to create intelligent machines that can replicate or exceed human intelligence.

1959

Machine Learning

subset of AI that enables machines to learn from existing data and improve upon that data to make decisions or predictions.

2017

Deep Learning

a machine learning technique in which layers of neural networks are used to process data and make decisions.

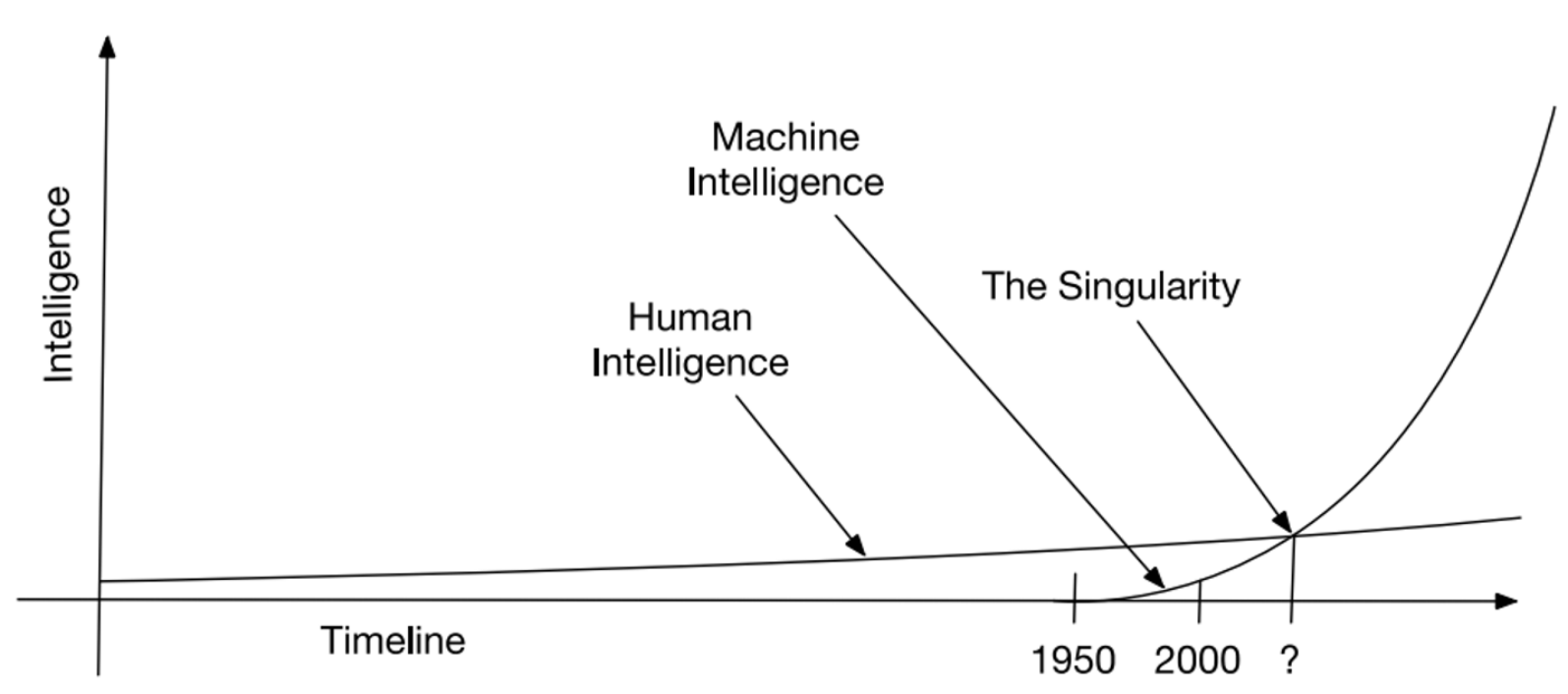
2021

Generative AI

create new written, visual, and auditory content given prompts or existing data.

Forrás: Microsoft

Szingularitás?



Forrás: Tóth Márton EIVOK-40

Forrás: Microsoft Copilot

Hol lehet a kontrollokat kialakítani?

MINDENHOL !

mert egy, egy kontroll nem szolgáltató és/vagy technológia függő!

KÖSZÖNÖM A FIGYELMET!

uni-nke.hu