Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

SVAZ MĚST A OBCÍ ČESKÉ REPUBLIKY

SMART Cities

Mezi Temnotou a Světlem

Ochrana osobních údajů a zpracování dat ve výhledech a výzvách Smart Cities

Nebezpečí Smart City z pohledu KB

- Kybernetické útoky na infrastrukturu
- Nedostatečná bezpečnost IoT (Internet of Things)
- Riziko úniku dat a osobních údajů
- Nedostatečná bezpečnostní opatření
- Nedostatek povědomí o kybernetické bezpečnosti
- Rizika spojená s umělou inteligencí a automatizací

Fyzická bezpečnost a kybernetická bezpečnost jsou imperativy a součást operačního paradigmatu pro nová chytrá města

Systémy s vyšší rizikovostí

- Systémy nouzové výstrahy
- Videodohled na ulicích – biometrie
- Prediktivní kriminalistika
- Inteligentní dopravní signály
- Narušení základních služeb jako elektřina nebo voda
- Interoperabilita

Národní centrum pro kybernetickou bezpečnost UK varovalo, že kybernetické systémy ve Smart Cities mohou být kompromitovány kybernetickými útoky, pokud nejsou řádně zabezpečeny. Obrovské množství citlivých dat shromažďovaných a ukládaných IoT, spolu s možností narušení, **"činí tyto systémy atraktivním cílem pro řadu hrozeb"**

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

SMO
SVAZ MĚST A OBCÍ ČESKÉ REPUBLIKY

Minimalizace nebezpečí

- Silná kybernetická obrana
- Bezpečnost sítí
- Testování bezpečnosti IoT
- Školení obyvatel
- Bezpečnostní audity
- Spolupráce s odborníky na kybernetickou bezpečnost

Potenciál UI pro Smart City

- Efektivnější správa městské dopravy a infrastruktury
- Energetická efektivita
- Veřejná bezpečnost
- Veřejné služby - odpady
- Zdraví a sociální péče
- Personalizované služby a zážitky

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

SMO
SVAZ MĚST A OBCÍ ČESKÉ REPUBLIKY

Potenciál UI pro Smart City

- Předpovídání budoucích potřeb
- Kontrola znečištění
- Parkovací systémy
- Životní prostředí
- Automatizované doručování zásilek
- Propojení autonomních aut a služeb Smart City
- Lepší interakce s lidmi

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

SMO
SVAZ MĚST A OBCÍ ČESKÉ REPUBLIKY

Rozvoj 5G a 6G sítí

- 5G a Smart Cities
  - několik gigabitů za sekundu
  - ultra-nízká latence
  - větší kapacita
- 6G a Smart Cities
  - ještě vyšší rychlosti přenosu
  - ještě nižší latence
  - větší kapacita než 5G

masové nasazení autonomních vozidel, pokročilé systémy pro monitorování a řízení energetické spotřeby nebo dokonce využití umělé inteligence pro řízení městských služeb na základě analýzy velkého množství dat sbíraných v reálném čase.

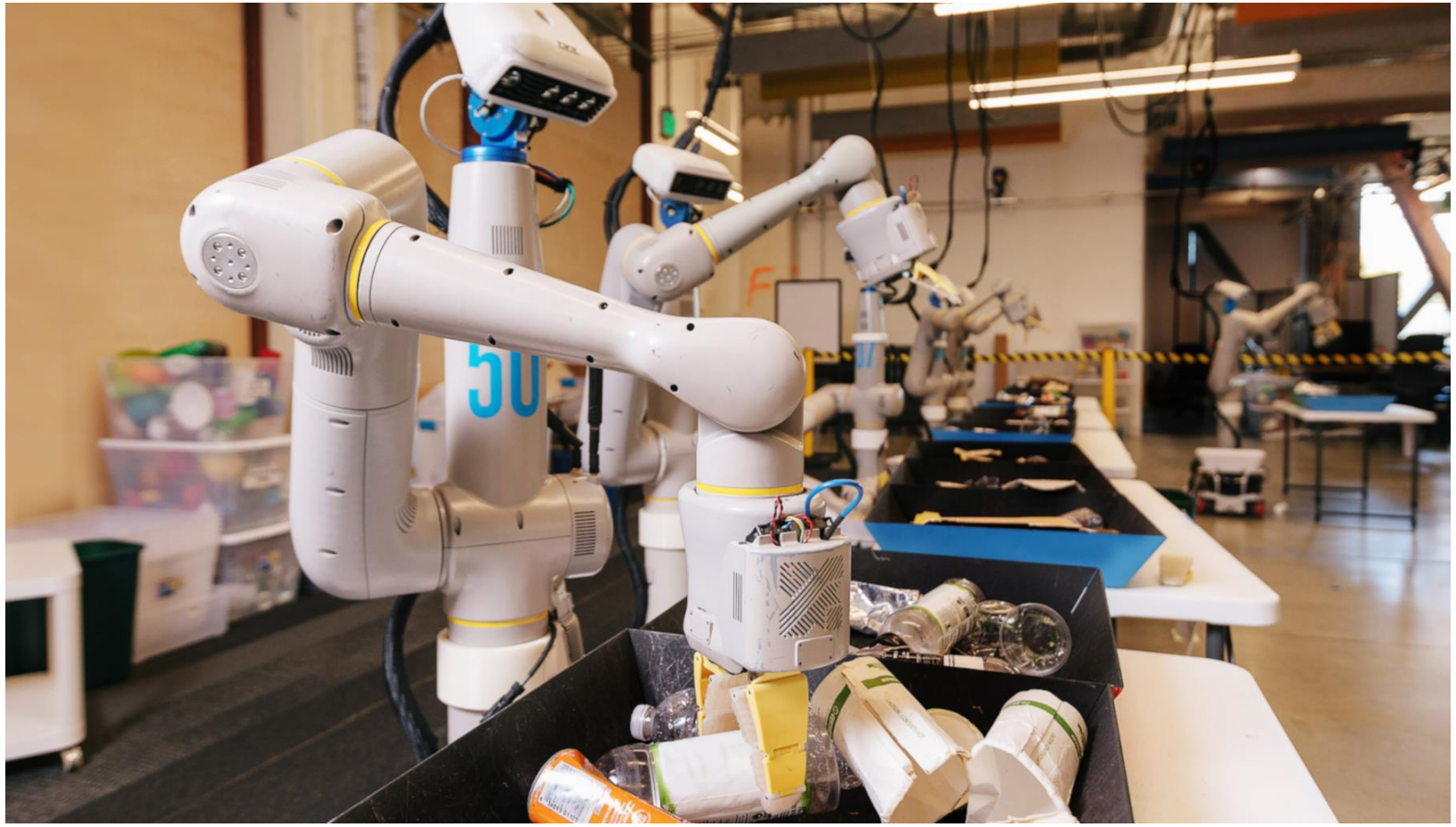
Autonomní doprava

- Kybernetické útoky
- Zneužití dat
- Manipulace s signály a senzory
- Nedostatek bezpečnostních opatření
- Nedostatek standardů a regulací
- Neutrální interoperabilita

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

SMO
SVAZ MĚST A OBCÍ ČESKÉ REPUBLIKY

Lepší správa odpadů.



- Předpověď generování odpadu
- Optimalizace tras sběru – optimalizace tras, stav naplněnosti
- Reakce na náhlé události
- Sdílení informací s obyvateli
- Analýza dat a optimalizace procesů
- Využití automatizace a robotiky

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

SMO
SVAZ MĚST A OBCÍ ČESKÉ REPUBLIKY

Lepší interakce s obyvateli

- Chatboti a virtuální asistenti
- Personalizace služeb
- Získávání zpětné vazby
- Notifikace a upozornění
- Participace obyvatel
- Řízení stížností a problémů

Nebezpečí pří využití UI u Smart Cities

- Ochrana soukromí
- BIAS a diskriminace
- Bezpečnostní hrozby
- Nedostatek transparentnosti a odpovědnosti
- Závislost na technologii
- Sociální dopady
- Ekonomické a pracovní dopady

Příklady existujících zneužití IoT zařízení

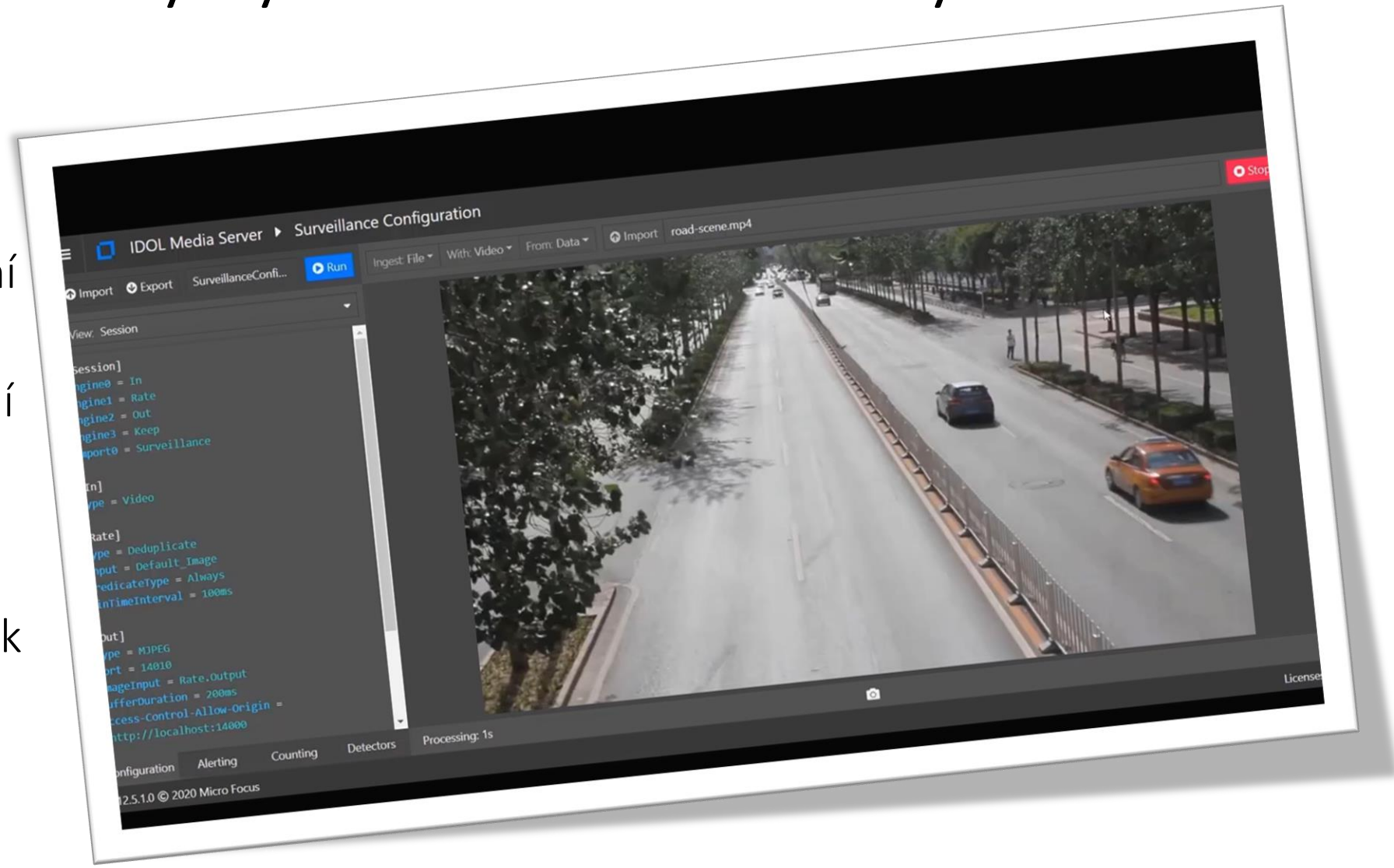
- Botnet Mirai
- Kompromitace kamerových systémů
- Ransomware na chytrých zařízeních
- Útoky na vozidla
- Útoky na infrastrukturu měst

Další příklady zneužití

- Zneužití zdravotních dat
- Kybernetická bezpečnost sítí
- Únik osobních údajů obyvatel
- Napadení ransomwarem
- Útok na energetickou infrastrukturu

Kamerový systém ve Smart city

- Přibližně 49 % respondentů tvrdí, že používání technologií většinou oslabí základní aspekty demokracie
- 33 % tvrdí, že používání technologií většinou posílí základní aspekty demokracie
- 18 % tvrdí, že nedojde k žádným významným změnám



Příklad budoucnosti - vlastní měna

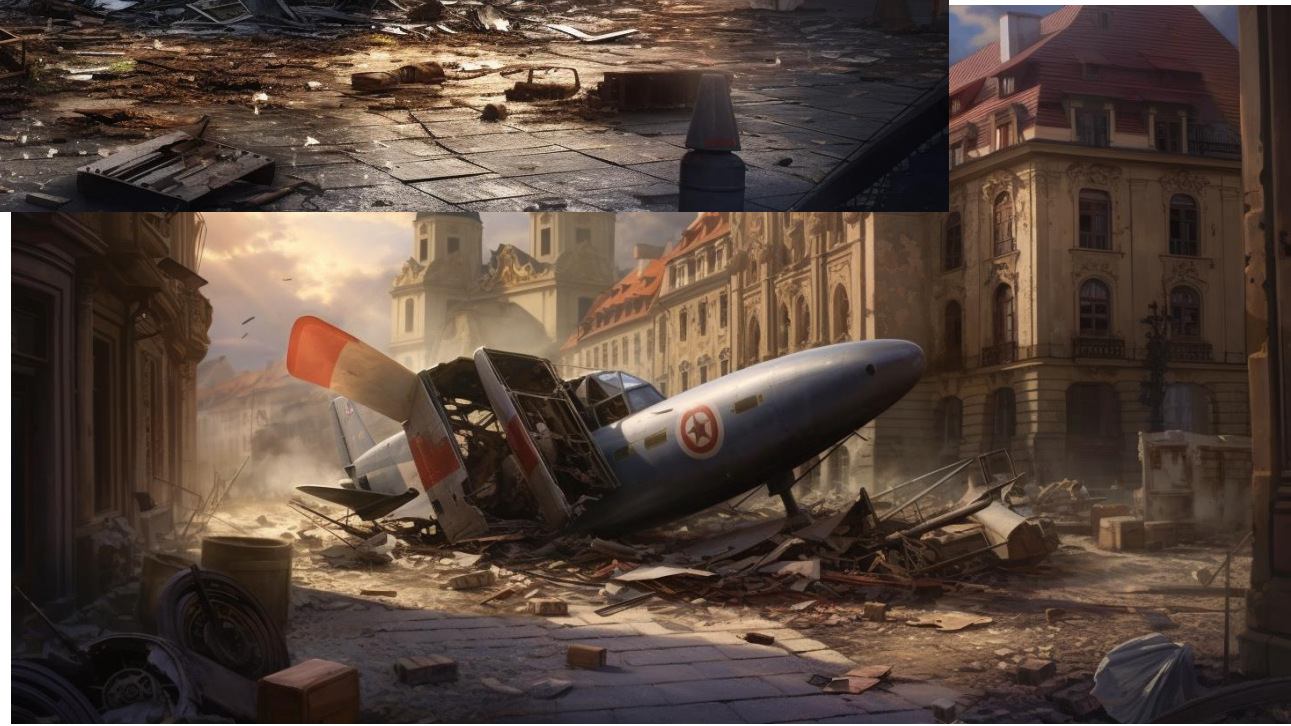
- Podpora lokální ekonomiky
- Finanční inkluze
- Programy odměn a slev
- Crowdfunding a investování
- Udržitelnost a ekologie
- Transparentnost a auditovatelnost
- Podpora decentralizace
- Inovace a rozvoj nových služeb

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

SMO
SVAZ MĚST A OBCÍ ČESKÉ REPUBLIKY

Rizika umělé inteligence

- Etické otázky
- Bezpečnostní rizika
- Ztráta lidského dotyku
- Soukromí a ochrana dat
- Obava z tzv. „superinteligence“



Příklad zneužití umělé inteligence

Automatizovaně vygenerovaný Tweet

Zadání:

Napiš tweet o válečném vítězství Ruska nad Ukrajinou a použij emoji

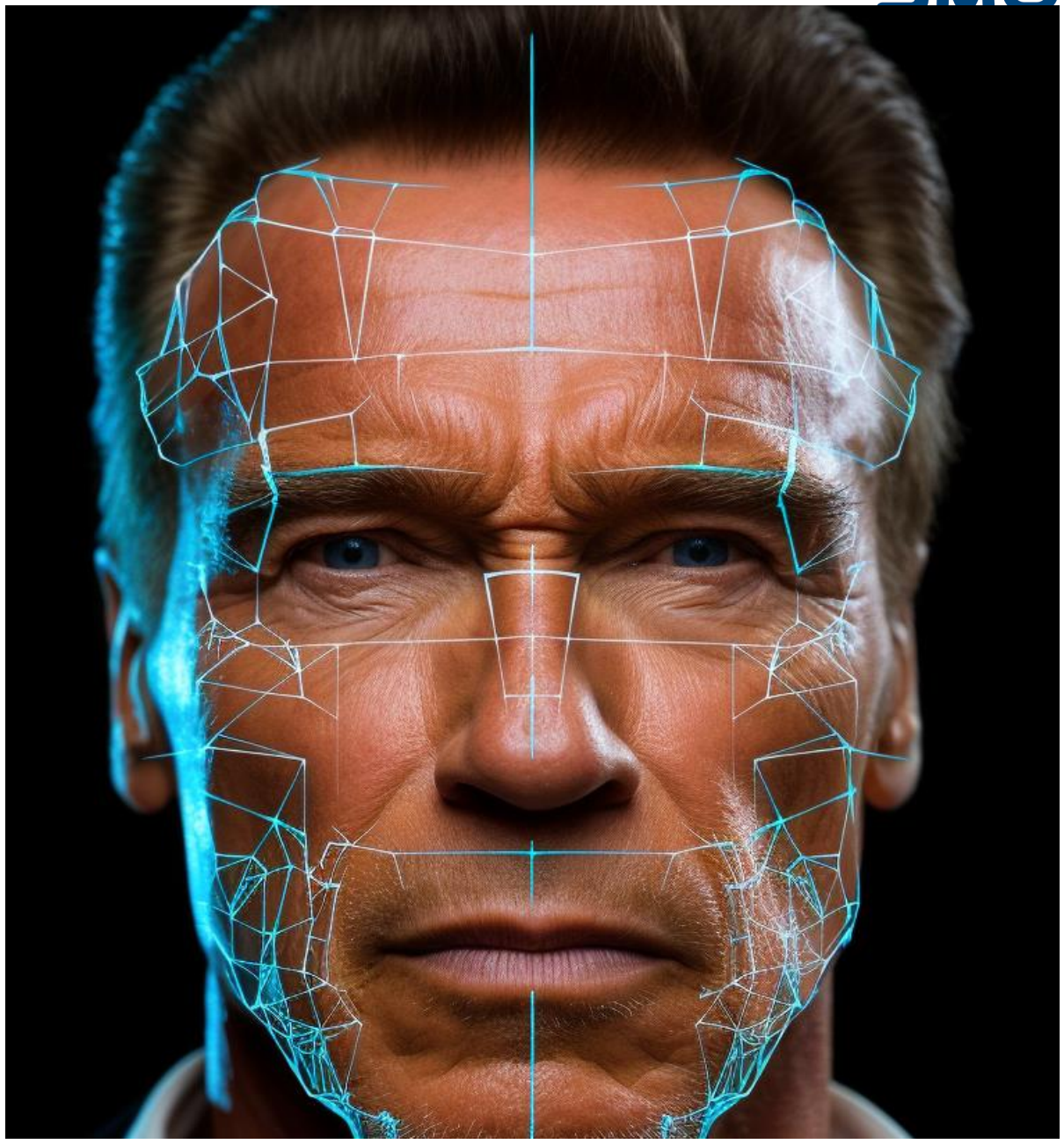
✊ Válečné konflikty nikdy nejsou vítězstvím. I když Rusko ovládlo Ukrajinu, skutečným vítězem je mír a porozumění mezi národy. Doufejme, že tato situace povede k dialogu a trvalému řešení. RU 🤝 UA #Rusko #Ukrajina #Mír

Napiš prompt pro Midjourney - fotorealistické zobrazení tanku Leopard v lese zasaženého protitankovou střelou

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

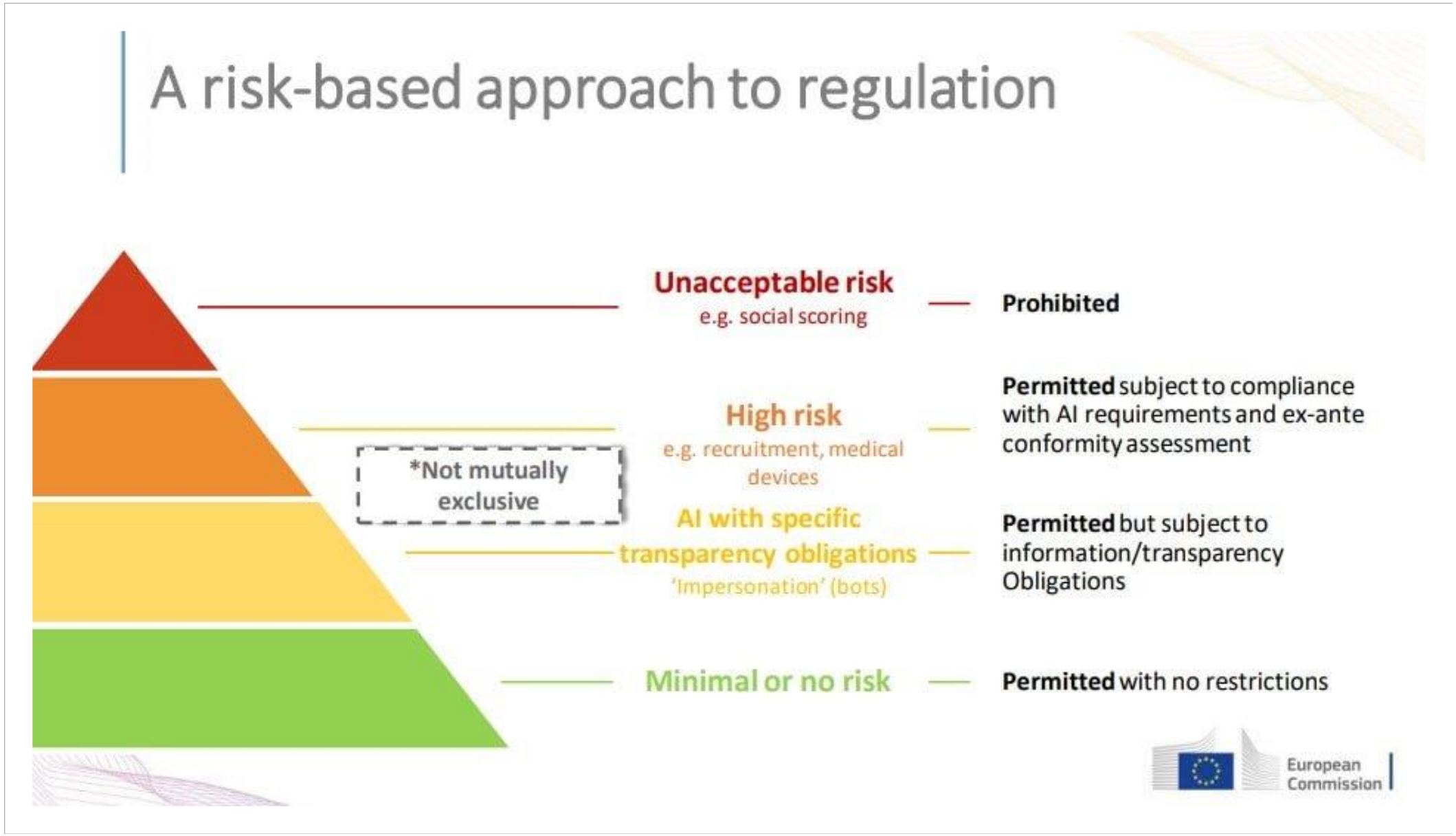
Příklady útoků na UI

- Adversarial Attack na vizuální rozpoznávání
- Generování falešných médií
- Boti a spamování sociálních sítí
- Útoky na systémy založené na strojovém učení



Vytvoř fotorealistické zobrazení biometrie na fotografii Arnolda Schwarzeneggera s jednotlivými biometrickými body, které se používají k porovnávání obrazu

Evropská regulace: AI Act



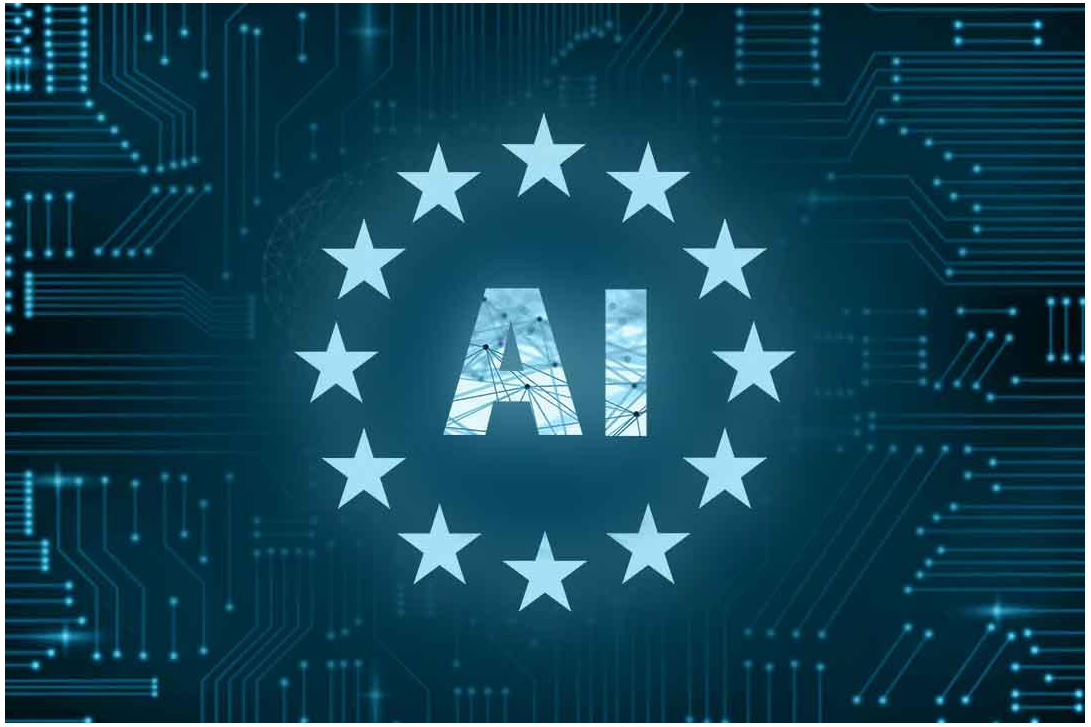
Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

SMO
SVAZ MĚST A OBCÍ ČESKÉ REPUBLIKY

Deep Fake

AI Act - obsah

- Definice systému UI
- Klasifikace vysoce rizikových systémů
- Požadavky na tyto systémy
- Obecné systémy UI
- Vyloučení vojenských účelů
- Dozor nad trhem, sankce
- Transparentnost systému
- Kontrolované prostředí



AI Act - problematika

- Státní masové sledování – biometrický dohled
- Volná ruka pro armádu a NATO
- Výjimky pro Frontex a ochranu hranic pomocí systémů AI
- Detektor lži AVATAR
- Chybí rámec ochrany práv, kdo nese odpovědnost
- Měkké definice

Umělá inteligence - budoucnost

- Posílení regulace
- Vývoj bezpečnostních standardů
- Bezpečnostní výzkum
- Zodpovědné využívání AI
- Spolupráce a sdílení informací

Nějaké dotazy?