Umělá inteligence pro síťovou bezpečnost

Od studentského
startupu do Silicon Valley
jako součást CISCO

Cognitive Security (COSE) vzniklo ze Skupiny agentových technologií FEL ČVUT

```
Is a Win32 executable
  Size of header       00045520h / 283936
  File size in header  FFFFFEE8h / 4294967016
  Entrypoint           000A5B23h / 678691
  Relocation entries   00005B00h / 23296
  Relocation offset    00000468h / 1128

  PE DLL at offset 000000F0h / 240
    Entrypoint              00061BC5h / 400325
    Entrypoint RVA          000627C5h
    Entrypoint section      .text
    Calculated PE EXE size  000B6A00h / 748032
    Image base              10000000h / 268435456
    Required CPU type       80386
    Required OS             5.00 - Win 98 or 2k
    Subsystem               Windows GUI
    Linker version          9.00
    Stack reserve           00100000h / 1048576
    Stack commit            00001000h / 4096
    Heap reserve            00100000h / 1048576
    Heap commit             00001000h / 4096
    Flags:
      File is executable
      Machine based on 32-bit-word architecture
      DLL file (library image)

    Sections according to section table (section align: 00001000h):
      Name      RVA         Virt size   Phys offs   Phys size   Phys end    Flags
      .text     00001000h   000757E8h   00000400h   00075800h   00075C00h   60000020h
      .rdata    00077000h   00025C6Ch   00075C00h   00025E00h   0009BA00h   40000040h
      .data     0009D000h   000166ECh   0009BA00h   00011400h   000ACE00h   C0000040h
      .reloc    000B4000h   00009AB2h   000ACE00h   00009C00h   000B6A00h   42000040h

    Listing of all used data directory entries (used: 5, total: 16):
                        Name   Phys offs   RVA         Phys size   Section
                Export Table   0009AF50h   0009C350h   0000091Ch   .rdata
                Import Table   0009A26Ch   0009B66Ch   00000064h   .rdata
```

Skupina úspěšně řešila projekty pro americkou armádu a námořnictvo:

- kooperace dronů
- hledání bezpečných plavebních tras

Síťová bezpečnost dnes staví na firewallech, antivirech, prevenci, sandboxech

COSE přináší Umělou inteligenci a Teorii her pro optimální obranné strategie

COSE realizuje technologii strojového učení na datech ze stovek tisíc počítačů

2006

- Agentový system detekce síťové nákazy
- Financování z Army Research Office, CERDEC US ARMY, AFRL,
- Martin Rehak PhD

2009

- COSE s.r.o.
- Financování Angel funding
- Lic. smlouva s ČVUT
- Financování DOD zdvojnásobeno
- CISCO partnerství

2010

- První zaměstnanec
- První zákazník
- společný vývoj s ČVUT

2011

- Early stage VC financování 1.4M
- částečný Angel buyout
- ESOP začleněn
- CISCO/COSE společný R&D kontrakt
- VP sales přijat

2012

- VP sales propuštěn
- Angel buyout dokončen
- CISCO/COSE společné R&D ukončeno
- CISCO/COSE OEM smlouva
- přípr. rouxrun tier1VC

2013

- COSE se stává součástí CISCO
- >25% do ESOP
- ČVUT/COSE lic. smlouva upravena na sml. o podporovaném výzkumu

2014

- ISO audit - “nejlepší integrace do CISCO”
- WebFlow detekční engine v produkci
- cloudová služba
- tým vzrostl o 100%
- první platící zákazníci

2015

- produkt CTA chrání >500k síťových uzlů
- >30 platících globálních zákazníků, >100 EFT
- rozšiřujeme pokrytí: WSA, BC

INOVACE V COSE

COGNITIVESECURITY

- **vytrvalé hledání disruptivních příležitostí**
- **vše stavěno na high-end vědeckých metodách (umělá inteligence, strojové učení)**
  - spolupráce s univerzitou, spoluřešitelství R&D projektu
- **extrémně rychlý postup od vědeckých výsledků → k dodání produktu**
- **investice do lidí a R&D upřednostněna před investicemi do rozvoje businessu**
  - umožněno přes Venture Capital,
  - tlak na rychlý růst technologie i businessu

INOVACE V CISCO

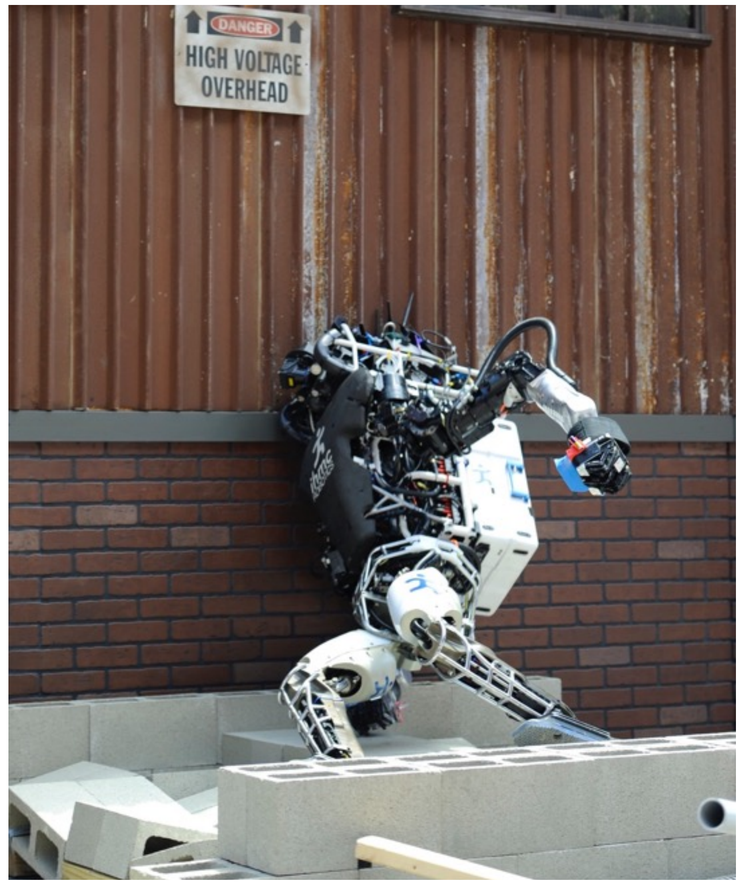
- příležitosti:
  - **zdroje k získání** (ještě výraznějšího) **talentu**
  - **dostupnost relevantních obrovských dat, a tím pádem příležitosí k uplatnění R&D zkušeností v širším rozsahu**
  - **unikátní znalosti a zkušenosti v síťové bezpečnosti**
  - **potenciál ovlivnit velmi rozsáhlý globální trh**
- výzvy:
  - **disruptivní postupy v tradičním zaběhlém prostředí**
  - **tlak na revenue**
  - **diversita talentu**

UMĚLÁ INTELIGENCE

- co to vlastně je ?

- je to bezpečné ?

- funguje to vůbec ?

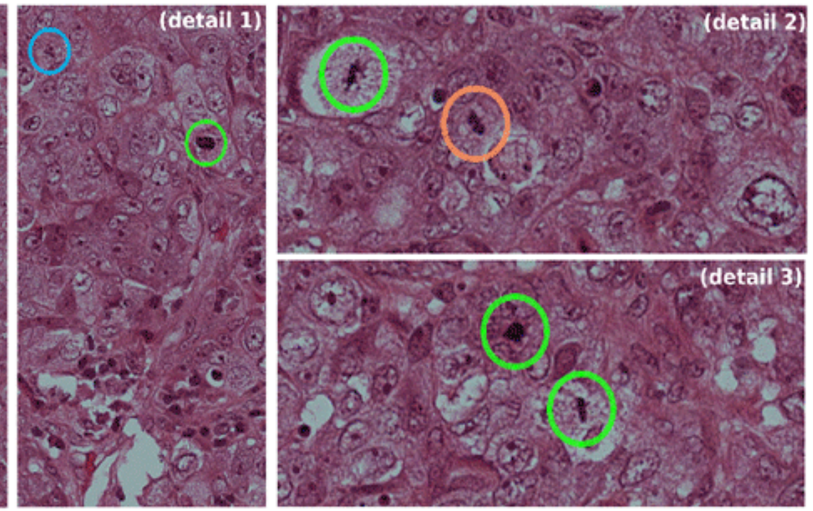


Umělá inteligence ?
Strojové učení ?

Rozpoznávání ?

Predikce ?

rozeznání nemocných buněk…



Alan Turing

1912–1954

Thomas Bayes

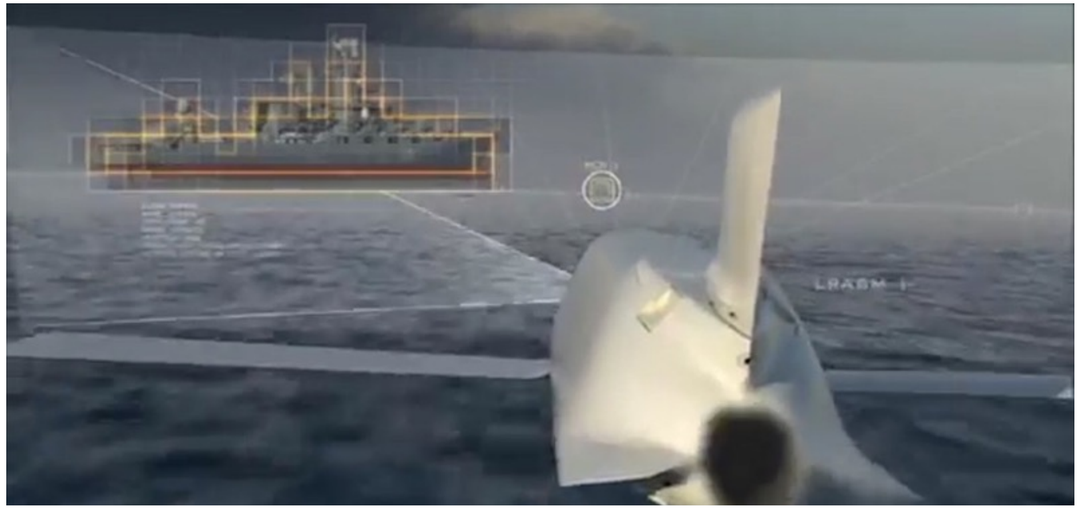
1701–1761

Claude Shannon

1916–2001

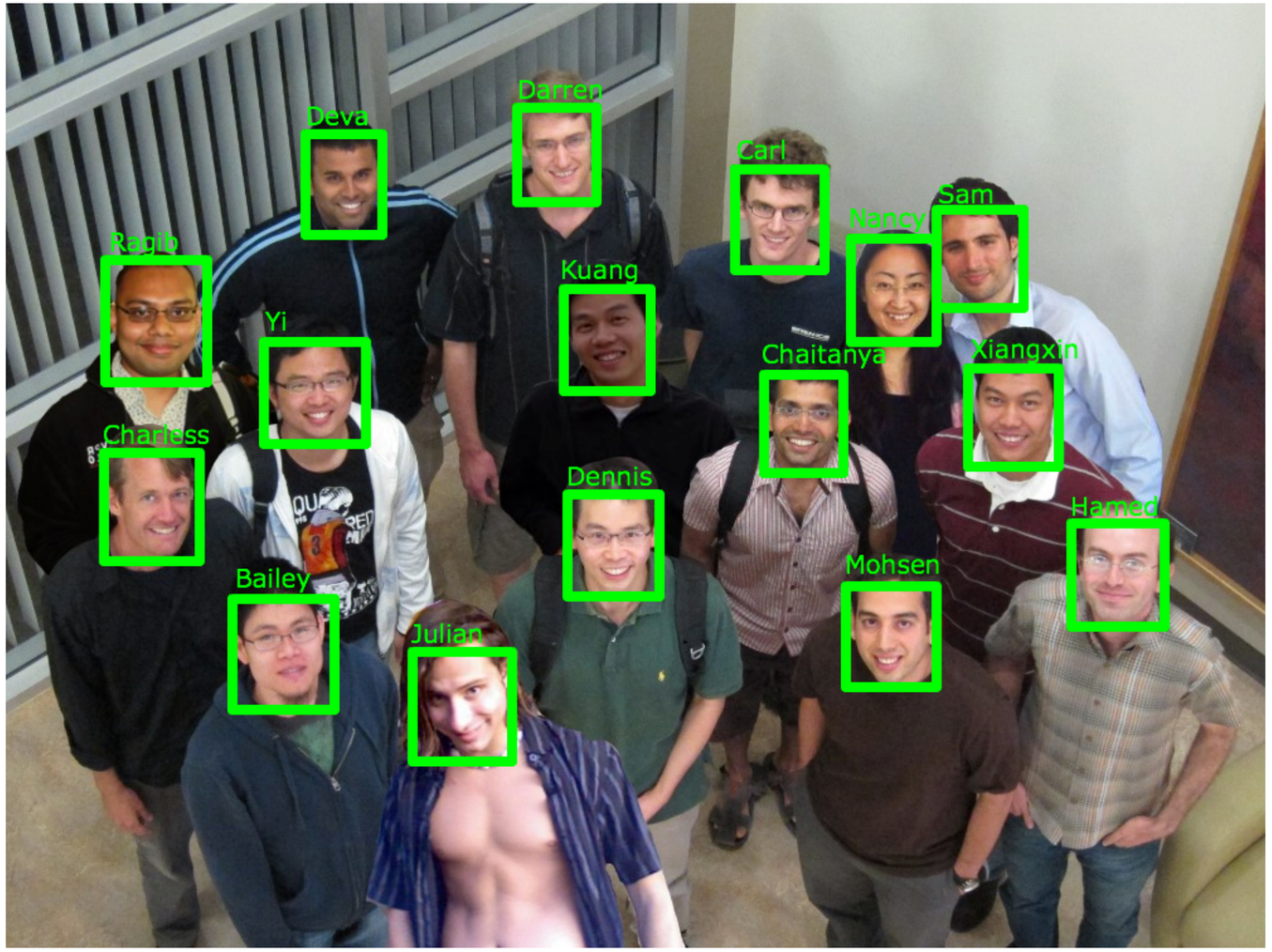
95% totéž

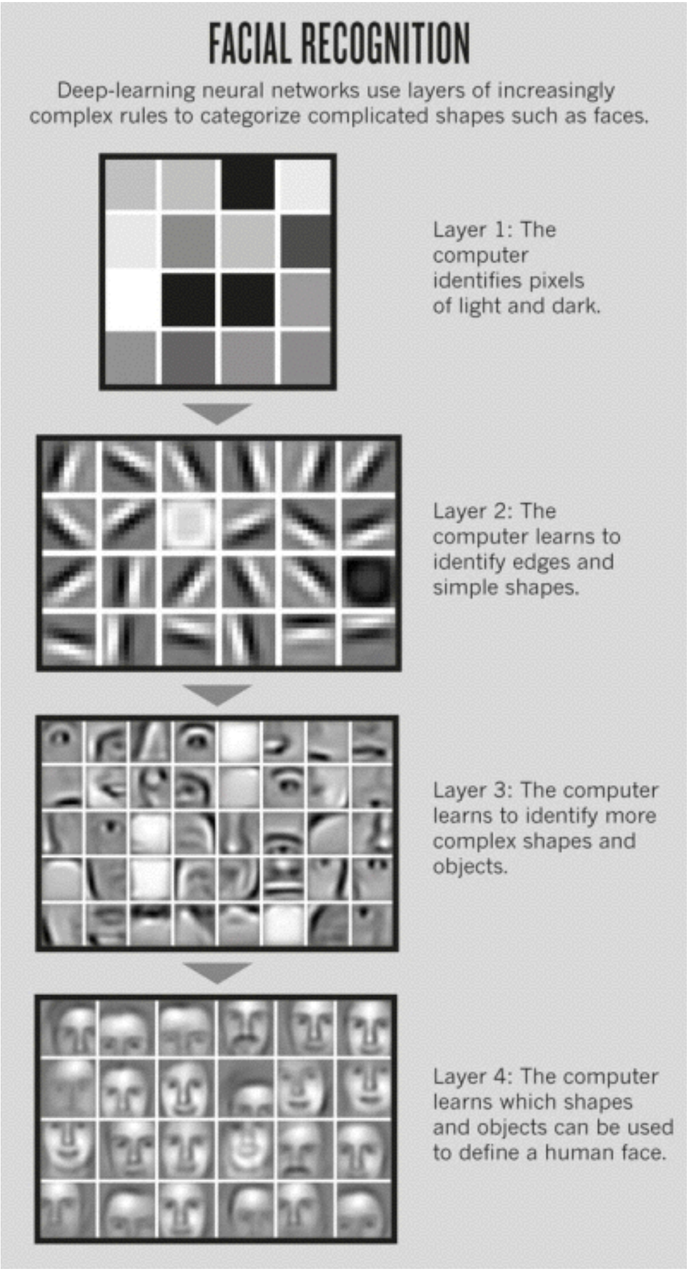
…rozeznání vojenských cílů



…nejtěžší je dekódovat obsah vstupních dat

Průlom po 2006 v rozeznávání obsahu obrazu





Průlom 2014: překonání hranice obraz-text

- Strojové učení do ~2010
  - _ učení z malých dat
  - _ učení navigováno člověkem
- "Deep Learning" po 2010
  - _ učení z masivních dat
  - _ automatické učení z dat v hierarchii různých úrovní detailu

Ale !

Umělá inteligence za 5, 10, 20 let

Bezprecedentní syntéza všech dostupných dat

“Prohledávači, připrav mi smlouvu s brazilským dodavatelem. Podle švýcarského práva. Trojjazyčně.”

- klesne hodnota lidské mechanické práce s daty

Budoucí ultimátní síťové bezpečnostní systémy

- kam směřujeme ?
  - _ k odstranění práce armády analytiků píšících signatury
  - _ k automatické kompletí reakci (zabezpečení, vyčištění, reporting) systému při objevení jediného příkladu doposud neznámé hrozby
  - _ k automatickému rozeznávání lidmi nerozeznatelných událostí na síti
  - _ k systému neomezenému velikostí síťě (IoT zvětší provoz o několik řádů)
- kde jsme ?
  - _ stále ještě na začátku - ale nikdo na světě neumí víc

Samořídící vůz vs. síťová behaviorální analýza

podobná komplexita

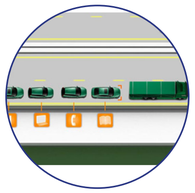
Self-Driving Car

Surprising number of problems...

- Occlusion
- Sudden obstacles
- Unexpected conditions
- ...

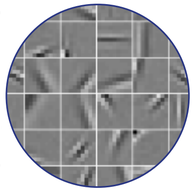
Not entirely there yet... (20+ years)

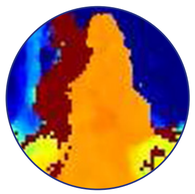
- Assisting park house
- Virtual car trains
- Sensors in roads ?!?
- ...

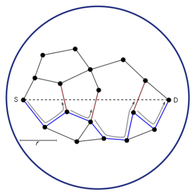


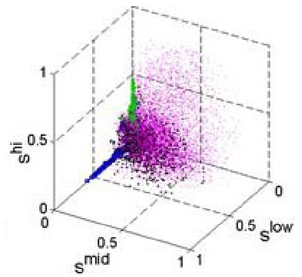
Various methods combined...

- Img analysis
- Radar
- Location analysis
- ...



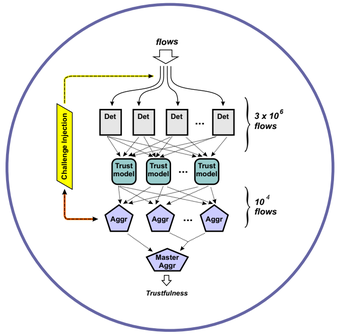






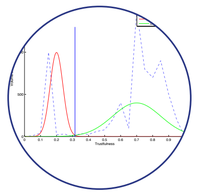
The Same Machine Learning Background

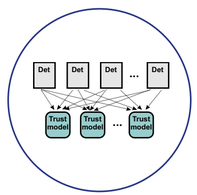
Network Behavior Analysis



Various methods combined...

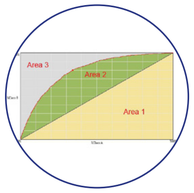
- Detectors
- Trust modeling
- Game Theory
- ...

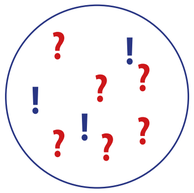


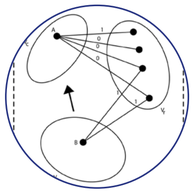


Not entirely there yet... (after 4+ years)

- Efficacy reserves
- Zero-Day coverage
- Explanation & simplicity
- ...

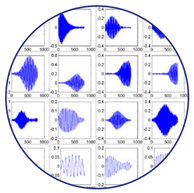


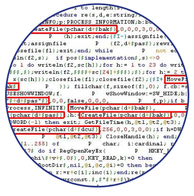


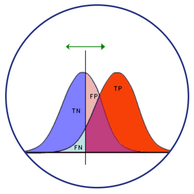


Surprising number of problems...

- Feature extraction
- What is malicious ?
- Limited information
- ...








THE MAGIC ROUNDABOUT
Ring road
Cirencester
A4289
(M4)
Marlborough
Burford
Oxford
Town
centre
H
A&E
A4312

Swindon, UK

UMĚLÁ INTELIGENCE JE VÍC HROZBOU NEBO PŘÍLEŽITOSTÍ ?

- **Brzdy**
  - techniky umělé inteligence je těžké implementovat, selhání jsou běžná
  - žádná skutečná technologie (zatím) nevede ke strojům s vlastním vědomím
  - všechno zdánlivě inteligentní chování strojů je zakódováno lidmi, kteří chybují
- **Příležitosti**
  - masivní zrychlení CPUs umožní nepředstavitelné změny ve společnosti
  - jsme na začátku datově-informační revoluce
  - přijde série průlomů v technologii. Každý bude disruptivní. Každý bude hrozbou ale i příležitostí !


COSE
COGNITIVESECURITY
CISCO
TM