

# Nástroje umělé inteligence a jejich využití v ochraně obyvatelstva

Jana Martinková

---

Bakalářská práce  
2024



Univerzita Tomáše Bati ve Zlíně  
Fakulta logistiky a krizového řízení

---

Univerzita Tomáše Bati ve Zlíně

Fakulta logistiky a krizového řízení

Ústav ochrany obyvatelstva

Akademický rok: 2023/2024

# ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	Jana Martinková
Osobní číslo:	L21445
Studijní program:	B1032A020002 Ochrana obyvatelstva
Forma studia:	Kombinovaná
Téma práce:	Nástroje umělé inteligence a jejich využití v ochraně obyvatelstva

## Zásady pro vypracování

- Zpracujte literární rešerzi nasazení umělé inteligence v oblasti bezpečnosti se zaměřením na ochranu obyvatelstva.
- Zhodnoťte nástroje umělé inteligence a jejich nasazení v bezpečnostních aplikacích.
- Vyhodnoťte využitelnost nástrojů umělé inteligence v ochraně obyvatelstva a identifikujte oblasti vhodné pro implementaci nástrojů umělé inteligence.

Forma zpracování bakalářské práce: **tištěná/elektronická**

**Seznam doporučené literatury:**

1. AL-SUQRI, Mohammed Nasser a Maryam GILLANI. *A Comparative Analysis of Information and Artificial Intelligence Toward National Security*. IEEE Access [online]. 2022, 10, 64420-64434 [cit. 2023-12-07]. ISSN 2169-3536. Dostupné z: doi:10.1109/ACCESS.2022.3183642.
2. RUSSELL, Stuart J. a Peter NORVIG, 2010. *Artificial intelligence: a modern approach*. 3rd ed. Upper Saddle River: Prentice Hall. Prentice Hall series in artificial intelligence. ISBN 978-0136042594.
3. TECUCI, Gheorghe, 2012. *Artificial intelligence*. WIREs Computational Statistics [online]. 4(2), 168-180 [cit. 2023-12-06]. ISSN 1939-5108. Dostupné z: doi:10.1002/wics.200

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **Ing. Jakub Rak, Ph.D.**  
Ústav ochrany obyvatelstva

Datum zadání bakalářské práce: **1. prosince 2023**

Termín odevzdání bakalářské práce: **3. května 2024**

L.S.

---

**doc. Ing. Zuzana Tučková, Ph.D.**  
děkanka

---

**prof. Ing. Dušan Vičar, CSc.**  
ředitel ústavu

## PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

**Prohlašuji,**

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 3.5.2024

Jméno a příjmení studenta: Jana Martinková

.....  
podpis studenta



## **ABSTRAKT**

Tato bakalářská práce pojednává o využití nástrojů umělé inteligence v ochraně obyvatelstva. Práce se zaměřuje na historii a vývoj umělé inteligence, od jejích počátků v 40. letech 20. století, přes jednoduché algoritmy až po složité systémy využívající strojové učení, počítačové vidění, expertní systémy a zpracování přirozeného jazyka a jejich využití v oblasti ochrany obyvatelstva. Práce dále zkoumá specifické příklady využití umělé inteligence, jako je nasazení chatbotů pro komunikaci s veřejností v krizových situacích a implementaci systémů jako Digital Fire pro detekci a správu požárů. Práce využívá metodu analýzy dostupných zdrojů a SWOT analýzu pro zhodnocení využitelnosti nástrojů umělé inteligence v oblasti bezpečnosti a ochrany obyvatelstva. Provedeným výzkumem jsem zjistila, že využití těchto nástrojů v oblasti bezpečnosti je má vysoký potenciál, je však potřeba další výzkum a vývoj, stejně jako zajištění, že tyto technologie budou implementovány eticky a s ohledem na ochranu soukromí a bezpečnost dat.

Klíčová slova: umělá inteligence, nástroje umělé inteligence, ochrana obyvatelstva, strojové učení, porozumění přirozeného jazyka, expertní systémy, počítačové vidění

## **ABSTRACT**

This bachelor's thesis discusses the utilization of artificial intelligence tools in population protection. It focuses on the history and development of artificial intelligence, from its origins in the 1940s, through simple algorithms to complex systems utilizing machine learning, computer vision, expert systems, and natural language processing, and their application in population protection. The thesis also examines specific examples of artificial intelligence utilization, such as deploying chatbots for communication with the public in crisis situations and implementing systems like Digital Fire for fire detection and management. The work employs a method of analyzing available resources and SWOT analysis to evaluate the usability of artificial intelligence tools in the field of security and population protection. Through the conducted research, it has been found that the utilization of these tools in security has high potential, but further research and development are needed, as well as ensuring that these technologies are implemented ethically and with regard to privacy protection and data security.

Keywords: artificial intelligence, artificial intelligence tools, population protection, machine learning, natural language understanding, expert systems, computer vision

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

# OBSAH

ÚVOD.....	9
<b>I TEORETICKÁ ČÁST .....</b>	<b>11</b>
<b>1 UMĚLÁ INTELIGENCE.....</b>	<b>12</b>
1.2 HISTORIE.....	13
1.3 TECHNIKY UMĚLÉ INTELIGENCE .....	15
1.3.1 Strojové učení.....	15
1.3.2 Zpracování přirozeného jazyka .....	17
1.3.3 Počítačové vidění .....	18
1.3.4 Expertní systémy .....	19
<b>2 OCHRANA OBYVATELSTVA .....</b>	<b>21</b>
2.1 AKTUÁLNÍ BEZPEČNOSTNÍ HROZBY .....	21
<b>3 VYUŽITÍ UMĚLÉ INTELIGENCE V OBLASTI BEZPEČNOSTI.....</b>	<b>23</b>
3.1 APLIKACE STROJOVÉHO UČENÍ V OBLASTI BEZPEČNOSTI.....	24
3.2 APLIKACE POČÍTAČOVÉHO VIDĚNÍ V OBLASTI BEZPEČNOSTI .....	26
3.3 APLIKACE EXPERTNÍCH SYSTÉMŮ V OBLASTI BEZPEČNOSTI .....	28
3.4 APLIKACE ZPRACOVÁNÍ PŘIROZENÉHO JAZYKA V OBLASTI BEZPEČNOSTI .....	29
<b>DÍLČÍ ZÁVĚR.....</b>	<b>32</b>
<b>II PRAKTICKÁ ČÁST .....</b>	<b>33</b>
<b>4 NÁSTROJE UMĚLÉ INTELIGENCE A JEJICH NAsAZENÍ V BEZPEČNOSTNÍCH APLIKACÍCH.....</b>	<b>34</b>
4.1 NAsAZENÍ CHATBOTŮ V BEZPEČNOSTNÍCH APLIKACÍCH .....	34
4.1.1 Zhodnocení využití Chatbota v oblasti bezpečnosti.....	35
4.1.2 Chatbot Clara .....	36
4.1.3 FloodBot.....	40
4.2 NAsAZENÍ OSTATNÍCH NÁSTROJŮ UMĚLÉ INTELIGENCE V BEZPEČNOSTNÍCH APLIKACÍCH.....	43
4.2.1 FloodHub.....	43
4.2.2 Digital Fire .....	46
<b>5 OBLASTI VHODNÉ PRO IMPLEMENTACI NÁSTROJŮ UMĚLÉ INTELIGENCE.....</b>	<b>51</b>
<b>DÍLČÍ ZÁVĚR.....</b>	<b>54</b>
<b>ZÁVĚR .....</b>	<b>55</b>
<b>SEZNAM POUŽITÉ LITERATURY.....</b>	<b>57</b>
<b>SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....</b>	<b>61</b>
<b>SEZNAM OBRÁZKŮ .....</b>	<b>62</b>
<b>SEZNAM TABULEK.....</b>	<b>63</b>



## ÚVOD

V současné době se svět potýká s celou řadou výzev, které ohrožují bezpečnost a pohodu obyvatelstva. Tyto výzvy zahrnují přírodní katastrofy, kybernetické útoky, terorismus a šíření infekčních nemocí. V reakci na tyto hrozby se stále více obracíme k pokročilým technologiím, aby nám pomohly chránit obyvatelstvo a zlepšit reakce na krizové situace. Proto se umělá inteligence stává nezbytným nástrojem v mnoha oblastech lidské činnosti, přičemž jednou z klíčových oblastí je ochrana obyvatelstva. Umělá inteligence, definovaná jako schopnost počítačů řešit problémy spojené s vyššími intelektuálními schopnostmi lidí, se stala klíčovým prvkem v mnoha aspektech našeho života. Schopnost počítačů a algoritmů simulovat vyšší intelektuální schopnosti člověka, jako je učení, rozhodování a vizuální vnímání, otevírá nové možnosti pro zlepšení bezpečnosti a reakce na krizové situace. Tato bakalářská práce se zaměřuje na využití umělé inteligence v ochraně obyvatelstva, zkoumá její historii, aplikaci jejich nástrojů a potenciál pro budoucí rozvoj. Historie umělé inteligence sahá až do 40. let 20. století, kdy byly počítače poprvé použity k simulaci inteligentního chování. Od té doby prošla umělá inteligence významným vývojem, od jednoduchých algoritmů po složité systémy schopné učení, analýzy a autonomního rozhodování. Dále práce představí termín ochrana obyvatelstva a jaké jsou aktuální bezpečnostní hrozby pro svět a Českou republiku. Cílem práce je zhodnotit nástroje umělé inteligence a jejich nasazení v bezpečnostních aplikacích. Dílčím cílem práce je zpracování literární rešerše nasazení umělé inteligence v oblasti bezpečnosti se zaměřením na ochranu obyvatelstva a identifikování oblasti vhodné pro implementaci nástrojů umělé inteligence. V této práci budou prozkoumány různé techniky umělé inteligence včetně strojového učení, počítačového vidění, expertních systémů a zpracování přirozeného jazyka a jejich využití v oblasti bezpečnosti a ochrany obyvatelstva. Dále se práce zaměří na výzvy a omezení spojená s implementací těchto technologií v praxi. Práce se zabývá analýzou a hodnocením využití nástrojů umělé inteligence v oblasti bezpečnosti se zaměřením na ochranu obyvatelstva. Bude se zkoumat, jak může umělá inteligence přispět k rychlejšímu a přesnějšímu šíření informací, zlepšení koordinace záchranných operací a podpoře obětí katastrof. Zvláštní pozornost bude věnována využití chatbotů, jako jsou FloodBot a Clara, které mohou být využity pro poskytování informací a podpory v krizových situacích. Práce se bude zabývat otázkou co je to umělá inteligence, jaké máme její metody, jak lze tyto metody aplikovat v bezpečnostních aplikacích. Dále se bude zabývat otázkou, jak mohou být chatboti a další nástroje umělé inteligence efektivně

využity ke zlepšení připravenosti na katastrofy a reakce na ně, a jak mohou pomoci v koordinaci záchranných operací a podpoře obětí katastrof. Jako vědecká metoda je v práci využita analýza dostupných zdrojů a v kapitole Nástroje umělé inteligence a jejich nasazení v bezpečnostních aplikacích je pro zhodnocení jednotlivých nástrojů využita SWOT analýza.

## **I. TEORETICKÁ ČÁST**

## 1 UMĚLÁ INTELIGENCE

Umělá inteligence má mezinárodní zkratku AI, která plyne z jejího anglického názvu Artificial Intelligence. (Zelinka, 2003) Na otázku, co je to umělá inteligence neexistuje jedna ustálená definice. V minulosti definoval umělou inteligenci McCarthy jako: „snahu vyvinout stroje, které se budou chovat jako by byly inteligentní.“ V encyklopedii Britannica je definována jako: „schopnost digitálních počítačů řešit problémy, které jsou normálně spojené s vyššími intelektuálními schopnostmi lidí.“ S další definicí přišel s Elaine Rich, který říká, že umělá inteligence je: „studium toho, jak přimět počítače dělat věci, ve kterých jsou lidé v tuto chvíli lepší.“ (Ertel, 2017)

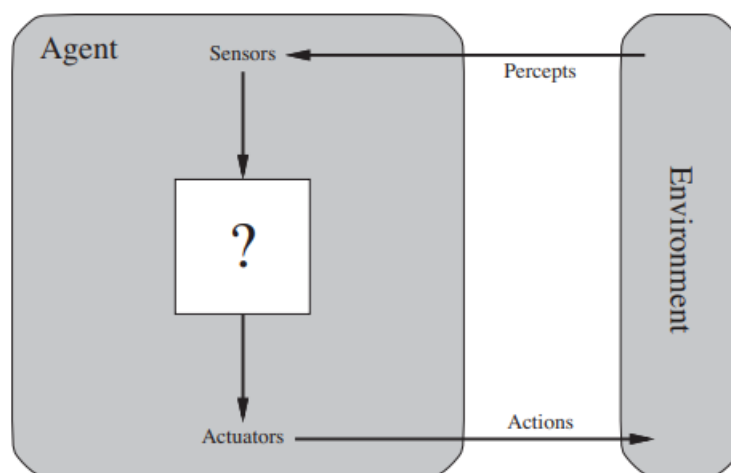
Tvrdí se, že umělá inteligence hraje významnou roli v oblasti řízení a operačního výzkumu. Inteligence je běžně považována za schopnost shromažďovat vědomosti a znalosti k řešení složitých problémů. V blízké budoucnosti mohou inteligentní stroje nahradit schopnosti člověka v mnoha oblastech. Umělá inteligence se zaměřuje na vývoj a implementaci inteligentních agentů. Jedná se o studium a vývoj inteligentních strojů a softwarů, které dokážou uvažovat, učit se, shromažďovat znalosti, komunikovat, manipulovat a vnímat předměty. Jde o studium výpočtů, které umožňují vnímat a jednat. Liší se od psychologie, protože klade důraz na výpočetní techniky a liší se i od informatiky kvůli důrazu na vnímání, uvažování a akce. (Pannu, 2015) Jedná se o vědní disciplínu, která je postupně formována na základě dalších disciplín, mezi které patří kybernetika, informatika, psychologie, neurologie, matematická logika, teorie her nebo teorie rozhodování. (Zelinka, 2003) Dnes je tato disciplína bohatě aplikovaná v nejrůznějších oblastech jako je zdravotnictví, průmyslová výroba, speciální pedagogika, vzdělávání, sociální práce nebo kybernetická bezpečnost. (Abiodun et al., 2018)

Umělá inteligence může být rozdělena na úzkou umělou inteligenci (ANI) a obecnou umělou inteligenci (AGI). Úzká umělá inteligence dokáže překonat člověka v definovaných a úzce strukturovaných úkolech. Byla navržena tak, aby dokázala vykonávat pouze jednu funkci. Aplikace ANI na základě parametrů, kontextu a pravidel stimulují lidské chování. Mezi nejvíce běžné techniky úzké umělé inteligence patří strojové učení, počítačové vidění a zpracování přirozeného jazyka. Příkladem takových funkcí může být rozpoznávání obličeje nebo systémy doporučení. Na druhou stranu obecná umělá inteligence umožňuje strojům aplikaci znalostí a dovedností v různých kontextech. Cílem obecné umělé inteligence je vytvoření stroje, který bude myslet a uvažovat jako člověk.

Mezi příklady AGI patří Chatbot, který dokáže zpracovat přirozený jazyk, který zanalyzuje a poté vytvoří odpověď. (Larkin, 2022).

## 1.1 Inteligentní agent

Slovem agent lze nazvat cokoliv, co je schopné vnímat okolní prostředí pomocí senzorů a následně působit na prostředí pomocí aktuátorů (Obr.1). Lidský agent má jako senzory své smysly a jako aktuátory používá ruce, nohy nebo hlas. Robotický agent může mít kamery a infračervené zaměřovače jako senzory a jako aktuátory různé motory pro jejich pohon. Softwarový agent přijímá stisknuté klávesy, obsah souboru a síťové pakety jako senzorické vstupy a působí na prostředí zobrazením na obrazovce, psaním souborů a odesíláním síťových paketů. Matematicky řečeno je chování agenta popsáno jeho funkcí mapovat jakoukoliv danou sekvenci vnímání na akci. (Russel and Norvig, 2012)



Obrázek 1- Agent a prostředí (Russel and Norvig, 2012)

## 1.2 Historie

Výzkumné cíle v oblasti umělé inteligence se v průběhu let měnily. Po vynálezu počítače ve 40. letech 20. století si lidé uvědomili, že jeho schopnosti nejsou omezeny pouze na numerické výpočty, ale lze jej použít k provádění mnoha intelektuálních úkolů, které jsou příliš složité pro lidskou inteligenci. Počítačům se říkalo „obří elektronické mozky“ a několik vizionářských výzkumníků navrhlo teorie, které zdůrazňují společné rysy strojů a lidské mysli. Mezi tyto vizionáře patřili McCullocha a Pittsa (1943), Wienera (1948), Shannona a Weavera (1949), Turing (1950) a von Neumann (1958). (Wang, 2019)

Koncept použití počítačů k simulaci inteligentního chování a kritického myšlení poprvé popsal právě Alan Turing v roce 1950. Ve své knize *Computers and Intelligence*, Turing popsal jednoduchý test, který později se stal známým jako „Turingův test“ k určení, zda byly počítače schopny lidské inteligence. (Kaul, 2020)

Ačkoli výše uvedené vědce lze považovat za průkopníky výzkumu umělé inteligence a jejich práce ovlivnily další generace, založili výzkumný obor dnes známý jako AI především McCarthy, Minsky, Newell, and Simon. Právě tyto vědci se zúčastnili vědecké konference v Dartmouthu v roce 1956, kde byl vytvořen název umělá inteligence, založili tři přední výzkumná centra a jejich myšlenky do značné míry utvářely cestu, kterou se ubírala umělá inteligence po celá desetiletí. (Wang, 2019)

Nejprve umělá inteligence začala jako jednoduchá série „když, pak“ a o několik desítek let později už zahrnovala složitější algoritmy, které fungují podobně jako lidský mozek. (Kaul, 2020)

Raná práce v oblasti umělé inteligence se zaměřovala na jednoduché domény „hraček“ a přinesla některé velmi působivé výsledky. Arthur Samuel vyvinul šachový herní program, který byl trénován hraním proti sobě, hraním proti lidem a hraním podle knih. Po tréninku obsahovala paměť zhruba 53 000 pozic a program se stal „spíše lepším než průměrným nováčkem, ale rozhodně ne odborníkem“, což dokazuje že samotné učení se na z paměť může mít za výsledek měřitelný pokrok. Minskyho studenti vyvinuli systémy, které demonstrovaly několik typů inteligentního chování pro řešení problémů, porozumění přirozenému jazyku, učení a plánování, ve zjednodušených oblastech známých jako „mikrosvěty“. Tyto úspěchy vyvolaly velké nadšení a očekávání v oblasti umělé inteligence. Lidé věřili, že brzy vytvoří stroje, které budou myslet, učit se a tvořit na úrovních překonávajících dokonce i lidskou inteligenci. Pokusy aplikovat vyvinuté metody na složité problémy reálného světa však soustavně končily velkolepými neúspěchy. K řešení složitých problémů reálného světa by totiž systém potřeboval obrovské množství znalostí a heuristiku. To vedlo k úpadku AI, kdy byly dříve štědré finance na její výzkum výrazně omezeny. Časem bylo zjištěno, že vytvoření inteligentního agenta je velmi obtížné, protože kognitivní funkce, které mají být automatizovány, nejsou dostatečně pochopeny. To vedlo výzkumníky AI k tomu, aby se zaměřili na jednotlivé kognitivní procesy, jako je učení, a na hloubkové studium základních problémů, jako je učení konceptů. Důsledkem bylo rozdělení umělé inteligence do mnoha různých oblastí, včetně reprezentace znalostí, vyhledávání, hraní her, dokazování teorémů, plánování,

pravděpodobnostního usuzování, učení, zpracování přirozeného jazyka, vizualizace, robotiky, neuronových sítí, genetických algoritmů a dalších. Každá z těchto oblastí si vytvořila vlastní výzkumnou komunitu s vlastními konferencemi a časopisy a omezenou komunikací s výzkumnými komunitami v jiných oblastech. (Tecuci, 2012)

### 1.3 Techniky umělé inteligence

Techniky umělé inteligence jsou technologie a systémy, které simulují inteligentní chování, aby vykonávaly úkoly, které obvykle vyžadují lidskou inteligenci. Tyto techniky mohou zahrnovat strojové učení, zpracování přirozeného jazyka, expertní systémy, počítačové vidění a další. Cílem AI je zlepšit efektivitu, přesnost a rychlost rozhodovacích procesů a úkolů, které by jinak mohly být pro lidi časově náročné nebo příliš složité (Tecuci, 2012).

AI techniky se využívají v široké škále aplikací, od automatizace výrobních procesů, přes analýzu velkých dat, až po rozvoj autonomních vozidel. Umožňují systémům, aby se učily z dat, rozpoznávaly vzory, dělaly predikce a autonomně reagovaly na nové situace (Krishnamoorthy and Rajeev, 2018).

#### 1.3.1 Strojové učení

Strojové učení (ML) je disciplínou, která se zabývá vytvářením algoritmů, jež umožňují umělým objektům automaticky se učit. Učení v tomto kontextu znamená schopnost těchto objektů zlepšovat své výkony na základě získaných zkušeností. Strojové učení se zaměřuje primárně na využití matematických postupů, které slouží k technické implementaci cílů definovaných oblastí umělé inteligence. Nezahrnuje však algoritmy, které se týkají vztahu k lidskému chápání nebo další filozofické reflexe. (Russel and Norvig, 2012)

Strojové učení se používá k tomu, aby stroje naučilo, jak lépe zpracovávat data. Někdy po prohlédnutí dat nemůžeme extrahovat informace. V takovém případě používáme strojové učení. S dostupností bohatých datových sad roste poptávka po strojovém učení. Mnoho odvětví aplikuje strojové učení k extrakci relevantních dat. Účelem strojového učení je učit se z dat. Bylo provedeno mnoho studií o tom, jak stroje naučit, aby se učily samy, aniž by byly explicitně programovány. Neexistuje žádný univerzální algoritmus, který by byl nejlepší pro řešení všech problémů. Typ algoritmu, který se použije, závisí na druhu

problému, který chcete řešit, na počtu proměnných, na druhu modelu, který by mu nejlépe vyhovoval, a tak dále. Zde je rychlý přehled několika běžně používaných algoritmů ve strojovém učení: (Mahesh, 2018)

### 1. Supervized learning (učení pod dohledem)

V tomto strojovém učení agent pozoruje některé příkladné dvojice vstupů a výstupů a naučí se funkci, která mapuje vstupy na výstupy. (Russel and Norvig, 2012)

Vyvozuje funkci z označených školících dat, která zahrnuje sadu školících příkladů. Algoritmy dohledového strojového učení jsou ty algoritmy, které vyžadují externí pomoc. Vstupní soubor dat je rozdělen na školící a testovací soubor dat. Školící soubor dat obsahuje výstupní proměnnou, která má být předpovězena nebo klasifikována. Všechny algoritmy se učí nějaké druhy vzorů ze školící souboru dat a aplikují je na testovací soubor dat pro předpověď nebo klasifikaci. (Mahesh, 2018)

### 2. Unsupervised learning (učení bez dohledu)

Při učení bez dozoru se agent učí vzorce ve vstupu, i když není poskytnuta žádná explicitní zpětná vazba. Nejběžnějším učebním úkolem bez dozoru je shlukování: detekce potenciálně užitečných shluků vstupních příkladů. (Russel and Norvig, 2012)

Algoritmy jsou ponechány svému vlastnímu zařízení, aby objevily a prezentovaly zajímavou strukturu v datech. Algoritmy nedohledového učení se učí několik rysů z dat. Když jsou představena nová data, používá předchozí naučené rysy k rozpoznání třídy dat. (Mahesh, 2018)

### 3. Semi-supervised learning (polo-dohledové učení)

Kombinuje prvky dohledového a nedohledového učení. Agent má k dispozici některé označené příklady a velkou kolekci neoznačených příkladů, ze kterých musí vytěžit co nejvíce informací. Příkladem může být systém, který se snaží odhadnout věk z fotografie. Nejprve je potřeba shromáždit několik označených příkladů, vyfotit lidi a zeptat se na jejich věk. To je dohledové učení. Ale ve skutečnosti někteří lidé lhali o svém věku. Nejde jen o náhodný šum ve datech; spíše jsou nepřesnosti systematické, a odhalit tyto nepřesnosti je problém nesupervizního učení zahrnující obrazy, samo-hlášené věky a skutečné (neznámé) věky. Takže jak šum, tak nedostatek štítků vytváří kontinuum mezi dohledovým a nedohledovým učáním. (Russel and Norvig, 2012)



#### 4. Reinforcement learning (odměňovací učení)

Odkazuje se na cílově orientované algoritmy, které se učí, jak dosáhnout složitějšího cíle nebo maximalizovat určitý rozměr během mnoha kroků; například maximalizovat získané body ve hře během mnoha tahů. Mohou začít s prázdným plátnem, a za správných podmínek dosáhnou nadlidského výkonu. Podobně jako dítě motivované výprasky a cukrovinkami, tyto algoritmy jsou penalizovány, když udělají špatná rozhodnutí, a odměňovány, když udělají ta správná. Strojové učení může analyzovat velké množství dat a identifikovat neobvyklé vzory. Tato schopnost může být velkým přínosem i v ochraně obyvatelstva. (Mahesh, 2018)

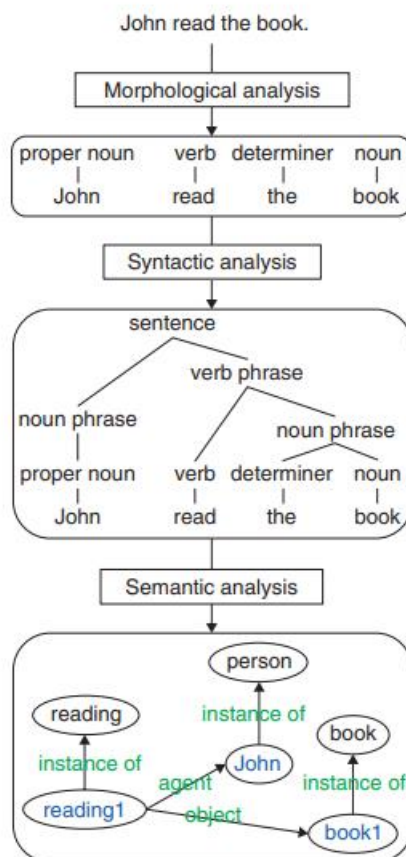
### 1.3.2 Zpracování přirozeného jazyka

Schopnost strojů porozumět a interpretovat a generovat přirozený jazyk. Přeložit mluvenou řeč do psané podoby a překládat z jednoho přirozeného jazyka do druhého. (Pannu, 2015)

Zpracování přirozeného jazyka je označováno zkratkou NLP podle anglického názvu natural language processing. Jazyk můžeme rozdělit na přirozený a umělý. Přirozený jazyk se vyvíjel za účelem komunikace současně s lidskou rasou. Příkladem takového jazyka je angličtina nebo čeština. Oproti tomu umělý jazyk nebyl součástí přirozeného vývoje a má přesně definovanou gramatiku a pravidla. NLP je jeden z hlavních pilířů umělé inteligence. Skládá se z několika dalších dílčích aplikací, mezi které patří extrakce informací, strojové překládání nebo rozpoznávání řeči. Pro pochopení lidského jazyka jej musí program nejprve analyzovat. Taková analýza se skládá z několika kroků. (Kumar, 2011)

1. Fonologická analýza – zaměřená na zpracování zvuku, rozpoznání a tvorbu řeči.
2. Morfologická analýza – zaměřená na rozlišování a generování správných gramatických tvarů. Nejprve dojde k rozdělení slova na dílčí části jako jsou předpony a přípony, a poté lze identifikovat o jaký se jedná slovní druh, jakého je rodu, pádu aj.
3. Lexikální analýza – přepisuje zdrojový kód do lexémů (identifikátorů, symbolů apod.)
4. Syntaktická analýza – převádí data z lexikální analýzy a v rámci dané věty analyzuje vztahy mezi jednotlivými slovy.

5. Sémantická analýza – určuje na základě pořadí, uskupení a významu slov a znaků ze syntaktické analýzy celkový význam daného textu
6. Pragmatická a diskurzivní analýza – přisuzuje rozdílnou váhu jednotlivým slovům a zkoumá jejich kontext. (D. Saffah a Hameed Al-Hindawi, 2021)



Obrázek 2-Stádia porozumění přirozeného jazyka (Tecuci, 2011)

### 1.3.3 Počítačové vidění

Počítačové vidění je odvětvím umělé inteligence, které se zaměřuje na umožnění počítačům interpretovat a porozumět vizuálnímu světu. Zahrnuje vývoj algoritmů a technik umožňujících počítačům extrahovat informace z obrázků nebo videí. (Russel and Norvig, 2012)

Cílem počítačového vidění je umožnit počítačům "vidět" a porozumět vizuálním informacím, jako jsou fotografie, videa, a 3D scény. Tento obor zahrnuje techniky jako detekce objektů, rozpoznávání obličejů, segmentace obrazu, a mnoho dalších aplikací, které mohou být využity v různých odvětvích, včetně bezpečnosti, zdravotnictví, průmyslu, a autonomních systémů. (Al-squiri and Gillani, 2022)

- **Klasifikace Obrázků:** Tato úloha zahrnuje zařazování obrázků do předdefinovaných tříd nebo kategorií. Například klasifikace obrázků zvířat do různých druhů nebo rozlišování mezi různými objekty.
- **Detekce Objektů:** Detekce objektů se zaměřuje na lokalizaci a identifikaci konkrétních objektů v obrázku nebo videu. Obvykle zahrnuje vytváření ohraničujících rámečků kolem objektů zájmu.
- **Sémantická Segmentace:** Sémantická segmentace zahrnuje přiřazování sémantických štítků každému pixelu v obrázku k odlišení různých objektů nebo oblastí. Poskytuje podrobné porozumění obrázku na úrovni pixelu.
- **Instance Segmentace:** Instance segmentace jde o krok dále než sémantická segmentace tím, že nejen přiřazuje sémantické štítky, ale také rozlišuje mezi jednotlivými instancemi objektů v obrázku.
- **Sledování Objektů:** Sledování objektů si klade za cíl sledovat pohyb objektů napříč několika snímky ve video sekvenci. Je obzvláště užitečné v aplikacích jako dohled nebo autonomní vozidla.
- **Odhad Pózy:** Odhad pózy spočívá v určování poloh a orientací objektů nebo konkrétních částí těla v obrázku nebo videu. Často se používá v aplikacích týkajících se analýzy lidské pózy nebo robotiky.
- **Generování Obrázků:** Generování obrázků zahrnuje vytváření nových obrázků, které mají specifické vlastnosti nebo sdílí podobnosti s daným souborem tréninkových obrázků. Techniky jako generativně adversární sítě (GANs) jsou často používány k tomuto účelu.
- **Vizuální Rozpoznání:** Vizuální rozpoznání zahrnuje širokou škálu úkolů, včetně klasifikace obrázků, detekce objektů a porozumění scéně. Jde o celkové porozumění a interpretaci vizuálního obsahu. (Szeliski, 2022)

#### 1.3.4 Expertní systémy

Expertní systémy jsou počítačové systémy, které simulují rozhodovací procesy a znalosti lidského odborníka v určitém oboru. Tyto systémy využívají znalostní bázi a pravidla

inferenčního mechanismu k řešení problémů a poskytování doporučení. Expertní systémy jsou často využívány v oblastech, kde je potřeba rychlého a přesného rozhodování na základě komplexních znalostí, jako je lékařství, finančnictví nebo inženýrství. (Russel and Norvig, 2012)

Podle povahy řešených úkolů lze aplikace rozdělit do následujících kategorií:

- Diagnostika: Identifikace chyb či nedostatků ve fungování systému, bez ohledu na to, zda se jedná o živé organismy či neživé entity.
- Interpretace: Analýza dat s cílem porozumět jejich významu a souvislostem.
- Monitorování: Nepřetržité sledování signálů a dat s cílem identifikovat okamžiky, kdy je nutná intervence.
- Plánování: Vytváření strategií a sekvencí kroků, které vedou k dosažení určeného cíle.
- Návrh: Navrhování konfigurací objektů nebo systémů, které odpovídají daným požadavkům či podmínkám.
- Predikce: Předpovídání budoucího vývoje událostí na základě analýzy minulosti a současnosti pomocí modelů. (Giarratano, 1998)

## 2 OCHRANA OBYVATELSTVA

Lindhart a Roudný definují ochranu obyvatelstva takto: „*Pojem ochrana obyvatelstva je často používán pro označení určitého sdruženého (integrovaného) systému vztahů, vazeb a konkrétních opatření k ochraně obyvatelstva a jeho majetku v nejrůznějších situacích, kdy může dojít k jejich ohrožení, počínaje „každodenními“ negativními událostmi, přes nejrůznější katastrofy a nouzové situace až po ozbrojený konflikt.*“ (Roudný, Linhart 2005)

### 2.1 Aktuální bezpečnostní hrozby

Největšími globálními bezpečnostními hrozbami podle The global risk report z roku 2023 jsou:

- **Kybernetická nejistota a rozšířená kyberkriminalita:** S rostoucí závislostí na digitálních technologiích a informačních systémech se zvyšuje riziko kybernetických útoků, které mohou ohrozit kritickou infrastrukturu, finanční systémy a osobní data.
- **Geoekonomické konfrontace:** Zvyšující se geopolitické napětí a ekonomické konfrontace mezi velmocemi, jako jsou USA a Čína, mohou vést k obchodním válkám, sankcím a dalším ekonomickým omezením, které mají dopad na globální ekonomiku.
- **Rozšíření nelegální ekonomické aktivity:** Proliferace nelegálních ekonomických aktivit, včetně obchodu s drogami, pašování a finančního podvodu, podkopává právní stát a přispívá k nestabilitě.
- **Terorismus a radikalizace:** Teroristické útoky a radikalizace jednotlivců a skupin představují vážnou hrozbu pro bezpečnost států i jednotlivců. Terorismus může mít mnoho podob, od mezinárodního džihádistického terorismu po domácí extremismus.
- **Pandemie a infekční nemoci:** Jak ukázala pandemie COVID-19, globální šíření infekčních nemocí může mít devastující dopad na zdraví, ekonomiku a společnost jako celek. Riziko nových pandemií zůstává vysoké.
- **Masová migrace a uprchlické krize:** Konflikty, ekonomická nestabilita, změna klimatu a další faktory mohou vést k masové migraci a uprchlickým krizím, které představují výzvy pro země původu, tranzitu i destinace.

- Rozpad států a občanské konflikty: Nestabilita, konflikty a rozpad státních struktur mohou vést k občanským válkám a dlouhodobé nestabilitě, což má dopad na regionální i globální bezpečnost.
- Zbrojení a šíření zbraní hromadného ničení: Zbrojení a šíření jaderných, biologických a chemických zbraní představují vážnou hrozbu pro globální bezpečnost. Zvláště znepokojivé je riziko, že tyto zbraně padnou do rukou teroristických skupin.
- Geoeconomické konfrontace: Zvyšující se geopolitické napětí a ekonomické konfrontace mezi velmocemi, jako jsou USA a Čína, mohou vést k obchodním válkám, sankcím a dalším ekonomickým omezením, které mají dopad na globální ekonomiku. (WEF, 2023)

Pro Českou republiku podle Koncepce ochrany obyvatelstva do roku 2025 s výhledem do roku 2030 nejvýznamnější hrozbou zůstává riziko vzniku povodní. Avšak pozornost by se měla zaměřit i na události související se suchem, narušením dodávek pitné vody, epidemiemi velkého rozsahu, rozsáhlé a dlouhotrvající výpadky elektrické energie, kybernetické útoky, rozsáhlé migrace a teroristické útoky. (Česko, 2023)

V Bezpečnostní strategii České republiky jsou za největší hrozby pro Českou republiku považovány:

- *„Výrazně zhoršené mezinárodní prostředí, které ohrožuje bezpečnost země.*
- *Válka Ruska proti Ukrajině, která ukončila období míru, stability a spolupráce v Evropě.*
- *Rusko, které záměrně působí proti politické, ekonomické a společenské stabilitě v Česku a je považováno za zásadní hrozbu pro bezpečnost země.*
- *Čína, která zpochybňuje mezinárodní řád a jejíž akce mají negativní důsledky pro euroatlantickou bezpečnost.*
- *Společný zájem Ruska a Číny oslabit vliv a jednotu demokratických zemí.* „(Česko, 2023)

### 3 VYUŽITÍ UMĚLÉ INTELIGENCE V OBLASTI BEZPEČNOSTI

Umělá inteligence má v oblasti bezpečnosti a ochraně obyvatelstva široké využití. Může být využita k predikci přírodních katastrof a havárií prostřednictvím analýzy rozsáhlých datových sad a identifikace vzorců a trendů, které mohou naznačovat blížící se nebezpečí. Například k analýze geografických dat, meteorologických informací, historických záznamů o přírodních katastrofách a dalších relevantních informací k predikci možných rizikových oblastí a časových okamžiků. Také může vytvářet modely pro simulaci a predikci chování přírodních jevů, jako jsou například zemětřesení, povodně nebo hurikány. (Al-suqri and Guillani, 2022)

AI může být dále použita k předpovídání trajektorií hurikánů a bouří, což umožňuje efektivnější přípravu a reakci na tyto události. Na základě analýzy tisíců datových proudů ze senzorů může být použita k detekci abnormálního chování hrází na základě, což umožňuje včasné varování před záplavami. Může pomoci energetickým společnostem odhadnout pravděpodobná místa poškození a dobu trvání výpadků služeb, aby se mohly připravit předem a efektivně reagovat na extrémní události. (Borisova and Nikolov, 2023)

Další možností využití AI je monitorování sociálních médií a dalších zdrojů informací pro detekci varovných signálů a rychlou reakci na blížící se katastrofy. AI může být využita k analýze textových dat a obrazových informací k identifikaci varovných signálů a informování veřejnosti a záchranných složek. Algoritmy AI mohou analyzovat data získaná z různých senzorů a sociálních médií, aby odhadly polohu zemětřesení a rychle vyvinuly systémy pro varování před zemětřesením, které mohou být rychlejší než tradiční metody. (Al-suqri and Guillani, 2022)

Umělá inteligence má široké využití také v armádě. Například může být využita k vývoji autonomních systémů, jako jsou bezpilotní letouny, pozemní vozidla a námořní plavidla, které mohou být využity k průzkumu, monitorování a bojovým operacím. (Tecuci, 2011)

Dále může být využita k analýze rozsáhlých datových sad a predikci chování nepřátelských sil, což může pomoci s plánováním a strategií vojenských operací. V oblasti kybernetické bezpečnosti, může být umělá inteligence využita k detekci a prevenci kybernetických útoků a ochraně vojenských informačních systémů. (Li, 2018)

V neposlední řadě, AI může být využita k vývoji inteligentních systémů pro rozpoznávání a identifikaci cílů, což může zlepšit přesnost a efektivitu vojenských operací. (Al-suqri and Guillani, 2022)

Umělá inteligence může být využita i v prevenci kriminality prostřednictvím analýzy rozsáhlých datových sad a identifikace vzorců a trendů, které mohou naznačovat možné kriminální aktivity. Může být využita například k analýze sociálních médií a dalších zdrojů informací k detekci varovných signálů a rizikových oblastí, což může pomoci s prevencí kriminality a rychlou reakcí na potenciální hrozby. V oblasti kybernetické bezpečnosti, AI může být využita k detekci a prevenci kybernetických útoků a ochraně informačních systémů před kriminálními aktivitami. (Li, 2018)

Dále může být využita k vytváření prediktivních modelů pro identifikaci oblastí s vysokým rizikem kriminality a přidělení zdrojů a opatření pro prevenci těchto aktivit. Může pomoci bezpečnostním agenturám a policistům v rozhodovacím procesu tím, že poskytuje analýzy rizik a doporučení založené na velkém množství dat. To umožňuje efektivnější alokaci zdrojů a lepší předvídání potenciálních hrozeb. Dále může pomoci v analýze historických dat o kriminalitě a vytváření prediktivních modelů, které předpovídají, kde a kdy může dojít k nárůstu kriminálních aktivit. To umožňuje efektivnější plánování a nasazení policejních hlídek. (Tecuci, 2011)

AI může být také využita k vývoji pokročilých bezpečnostních systémů, které mohou autonomně monitorovat veřejné prostory, detekovat podezřelé chování a automaticky upozornit bezpečnostní služby. Tyto systémy mohou být vybaveny schopností rozpoznávat specifické vzorce chování, které jsou typické pro přípravu nebo provádění kriminálních činů. (Lipton et al., 2003)

### **3.1 Aplikace strojového učení v oblasti bezpečnosti**

Strojové učení a umělá inteligence nabízejí řadu možností, jak výrazně zlepšit bezpečnost a ochranu obyvatelstva před různými hrozbami, včetně přírodních katastrof, kriminality, nebo kybernetických útoků. Zde jsou některé způsoby, jak lze strojové učení aplikovat v oblasti bezpečnosti:

1. **Predikce a včasná varování před přírodními katastrofami:** Strojové učení může být využito k analýze velkého množství dat z meteorologických stanic, satelitů a senzorů pro předpověď přírodních katastrof, jako jsou záplavy, zemětřesení nebo hurikány. Tato technologie umožňuje vytvářet přesnější modely pro predikci těchto



událostí a poskytovat včasné varování, což může zachránit životy a omezit materiální škody. (Pyayt et al., 2011)

2. **Zlepšení kybernetické bezpečnosti:** Strojové učení může identifikovat a reagovat na kybernetické hrozby rychleji a efektivněji než tradiční metody. Analýza vzorců síťového provozu a detekce anomálií pomáhá včas odhalit pokusy o neoprávněný přístup, malware a další kybernetické útoky, čímž chrání citlivé informace a infrastrukturu. (Li, 2018)
3. **Podpora rozhodování v krizových situacích:** AI a ML mohou analyzovat velké množství dat z různých zdrojů, jako jsou sociální média, zpravodajské kanály a vládní zprávy, aby identifikovaly vzorce a indikátory, které mohou naznačovat vznik krizových situací. Tato analýza umožňuje vládám a záchranným týmům lépe se připravit a reagovat na krizové situace, což může zahrnovat přírodní katastrofy, teroristické útoky nebo epidemie. (Lipton et al., 2003)
4. **Zlepšení komunikace v krizových situacích:** Strojové učení může být využito k analýze a optimalizaci komunikačních kanálů během krizových situací. Analýza dat získaných z komunikace mezi obyvatelstvem a záchrannými službami může pomoci identifikovat slabá místa v komunikačních sítích a zlepšit distribuci důležitých informací mezi obyvatelstvem. (Tecuci, 2011)
5. **Detekce a prevence šíření nemocí:** Strojové učení může být využito k analýze vzorců šíření nemocí a identifikaci potenciálních ohnisek nákazy. Modely strojového učení mohou pomoci předpovídat šíření infekčních nemocí na základě různých faktorů, včetně cestovních dat, klimatických podmínek a demografických informací, což umožňuje rychlejší a cílenější reakci. (Tecuci, 2011)
6. **Zlepšení monitorování a reakce na environmentální hrozby:** Strojové učení může být využito k monitorování změn v životním prostředí a detekci potenciálních hrozeb, jako jsou úniky toxických látek, znečištění vody nebo vzduchu a degradace ekosystémů. Modely strojového učení mohou analyzovat data získaná z satelitů, senzorů a dalších monitorovacích zařízení, aby rychle identifikovaly problémy a umožnily rychlou reakci na ochranu veřejného zdraví a životního prostředí. (Tecuci, 2011)
7. **Optimalizace rozdělení zdrojů a pomoci v krizových situacích:** Strojové učení může pomoci optimalizovat rozdělení zdrojů a pomoci v krizových situacích tím,

že předpovídá potřeby obyvatelstva a identifikuje nejefektivnější způsoby distribuce pomoci. Modely strojového učení mohou analyzovat data z minulých událostí, aktuální situace a dostupných zdrojů, aby navrhly optimální plány pro distribuci potravin, vody, léků a dalších zásob. Tato technologie může také pomoci koordinovat logistiku a zajištění, že pomoc dorazí tam, kde je nejvíce potřeba, což zvyšuje efektivitu humanitárních operací. (Al-suqri and Guillani, 2022)

Využití strojového učení v oblasti bezpečnosti a ochrany obyvatelstva je rozsáhlé. Za klíčové aspekty můžeme považovat hlavně predikci přírodních katastrof a včasné varování nebo podporu rozhodování a zlepšení komunikace v krizových situacích.

### 3.2 Aplikace počítačového vidění v oblasti bezpečnosti

Počítačové vidění lze aplikovat v oblasti bezpečnosti a ochraně obyvatelstva několika způsoby, které zvyšují bezpečnost a efektivitu reakce na potenciální hrozby:

1. **Detekce a identifikace osob:** Aplikace počítačového vidění mohou detekovat tváře lidí a registrační značky vozidel z obrazů zachycených kamerami. Tato schopnost je velmi cenná v bezpečnostních systémech, protože umožňuje snadno identifikovat místa trestné činnosti a zlepšit veřejnou bezpečnost. (Abdulhussein et al., 2020)
2. **Zlepšení bezpečnostního dohledu:** Počítačové vidění může spravovat detekci pohybu, identifikaci osob, sledování, kontrolu přístupu a interpretaci pohybu. Tyto úkoly mohou být využity k vylepšení bezpečnostního dohledu. Integrované počítačové systémy mohou identifikovat neobvyklé chování a pomáhat v řízení bezpečnosti. (Abdulhussein et al., 2020)
3. **Monitorování a ochrana kritické infrastruktury:** Systémy počítačového vidění mohou být nasazeny pro monitorování kritické infrastruktury, jako jsou elektrárny, přehrady a mosty, aby se včas identifikovaly potenciální hrozby nebo poškození. Tím se zvyšuje bezpečnost a minimalizuje riziko katastrofických událostí. (Abdulhussein et al., 2020)
4. **Rychlá a přesná reakce na přírodní katastrofy:** Počítačové vidění může být využito pro analýzu obrazů a videí z dronů nebo satelitů, aby se rychle identifikovaly oblasti postižené přírodními katastrofami, jako jsou zemětřesení, povodně nebo lesní požáry. Tato rychlá identifikace umožňuje efektivnější nasazení záchranných týmů a distribuci pomoci. (Lipton et al., 2003)

5. **Zlepšení evakuačních a záchranných operací:** Algoritmy počítačového vidění mohou analyzovat obrazová data z různých zdrojů, aby identifikovaly nejbezpečnější a nejefektivnější cesty pro evakuaci obyvatelstva z ohrožených oblastí. Tato analýza může zahrnovat identifikaci překážek, hodnocení stavu infrastruktury a analyzování dostupných únikových tras a zajištění nejrychlejšího a nejbezpečnějšího přesunu osob z ohrožených oblastí. (Lipton et al., 2003)
6. **Analýza škod po katastrofách:** Počítačové vidění může být použito k rychlé a přesné analýze škod způsobených přírodními katastrofami nebo nehodami. Tato analýza pomáhá určit priority při obnově a zajišťuje efektivní rozdělení zdrojů pro opravy a obnovu. (Lipton et al., 2003)
7. **Podpora při hledání a záchraně:** Využití počítačového vidění v bezpilotních letounů (dronů) umožňuje efektivnější hledání a záchranu osob v rozsáhlých nebo obtížně přístupných oblastech. Drony vybavené kamerami mohou prohledávat velké oblasti a identifikovat osoby potřebující pomoc, což značně zrychluje záchranné operace. (Jain et al., 2020)
8. **Vzdělávání a trénink:** Simulační systémy využívající počítačové vidění mohou poskytovat realistické tréninkové prostředí pro záchranné týmy a bezpečnostní složky. Tyto systémy umožňují simulaci různých scénářů a krizových situací, což zlepšuje připravenost a reakční schopnosti týmů. (Tecuci, 2011)
9. **Detekce a analýza požárů:** Systémy počítačového vidění mohou detekovat počátek požárů v rané fázi, což umožňuje rychlejší a efektivnější reakci hasičských jednotek. Díky analýze obrazu z kamer může systém identifikovat zdroje ohně nebo kouře dříve, než jsou viditelné pro lidské oko, což umožňuje rychlejší evakuaci a minimalizaci škod. (Tecuci, 2011)
10. **Zlepšení dopravní bezpečnosti:** Počítačové vidění může být využito k monitorování dopravních toků a detekci potenciálně nebezpečných situací na silnicích, jako jsou nehody, překážky na vozovce nebo nebezpečné řídicí chování. Tato technologie může pomoci předcházet dopravním nehodám a zlepšit bezpečnost na silnicích. (Tecuci, 2011)
11. **Podpora veřejného zdraví:** V oblasti veřejného zdraví může počítačové vidění pomoci v rané detekci a monitorování epidemických onemocnění prostřednictvím analýzy obrazových dat. Například, systémy mohou být využity k monitorování

teploty těla ve velkých skupinách lidí nebo k identifikaci osob s příznaky respiračních onemocnění. (Xin and Yiliang, 2018)

Počítačové vidění může být v oblasti bezpečnosti a ochrany obyvatelstva velkým přínosem, zejména díky možnosti detekce a identifikace osob, které mohou být využity v pro zlepšení bezpečnostního dohledu nebo podporu při hledání a záchraně osob.

### 3.3 Aplikace expertních systémů v oblasti bezpečnosti

Expertní systémy lze v oblasti bezpečnosti a ochrany obyvatelstva využít k řadě účelů, které zahrnují predikci a řízení krizových situací, podporu rozhodování v náročných podmínkách a zlepšení reakce na přírodní a lidské katastrofy. Níže jsou uvedeny některé způsoby, jakými lze expertní systémy využít v ochraně obyvatelstva:

1. **Predikce přírodních katastrof:** Expertní systémy mohou analyzovat velké množství dat z různých zdrojů, včetně meteorologických a geologických senzorů, k predikci přírodních katastrof, jako jsou zemětřesení, povodně a hurikány. Tato predikce umožňuje včasnou evakuaci a přípravu na nadcházející události, čímž se minimalizuje riziko pro životy a majetek. (Abdulhussein et al., 2020)
2. **Analýza a řízení dopravních toků:** V oblasti dopravy mohou expertní systémy analyzovat dopravní toky a předpovídat dopravní zátěže, identifikovat potenciální problémy a navrhnout optimalizace pro zlepšení plynulosti a bezpečnosti dopravy. Tato analýza a řízení mohou být klíčové při evakuaci obyvatelstva v případě katastrof. (Abdulhussein et al., 2020) (Abdulhussein et al., 2020)
3. **Podpora veřejného zdraví a epidemiologického sledování:** V oblasti veřejného zdraví mohou expertní systémy pomoci při sledování a reakci na epidemie nemocí. Analýzou dat z různých zdrojů, včetně sociálních médií, zdravotnických záznamů a vzorců pohybu obyvatelstva, mohou tyto systémy pomoci identifikovat a předvídat šíření infekčních nemocí. S využitím algoritmů strojového učení a umělé inteligence mohou tyto systémy identifikovat vzorce šíření nemocí, předpovídat budoucí vývoj a navrhnout preventivní opatření nebo reakce na epidemie. (Abdulhussein et al., 2020)
4. **Podpora rozhodování v krizovém managementu:** Expertní systémy mohou poskytovat doporučení pro rozhodování v krizových situacích tím, že integrují a analyzují informace z různých zdrojů, včetně historických dat, aktuálních zpráv a

modelů rizik. Tím pomáhají krizovým manažerům lépe pochopit situaci a vybrat nejvhodnější opatření. (Lipton et al., 2003)

5. **Řízení a koordinace záchranných operací:** Expertní systémy mohou být využity k optimalizaci nasazení záchranných týmů a zdrojů během katastrof. Systémy mohou analyzovat dostupné informace o situaci, počtu postižených, dostupných záchranných týmech a jejich vybavení, a na základě toho navrhnout nejefektivnější způsob nasazení. (Lipton et al., 2003)
6. **Vzdělávání a školení pro krizové situace:** Expertní systémy mohou být také využity pro vzdělávání a školení personálu zabývajícím se ochranou obyvatelstva. Simulace krizových situací s využitím expertních systémů umožňuje personálu lépe se připravit na reálné situace, rozvíjet dovednosti rozhodování a testovat různé reakční strategie v bezpečném prostředí. (Lipton et al., 2003)
7. **Detekce a reakce na chemické, biologické, radiologické a jaderné hrozby (CBRN):** Expertní systémy mohou být využity k rychlé identifikaci a analýze CBRN hrozeb, což umožňuje rychlou a cílenou reakci. Systémy mohou analyzovat vzorky v reálném čase a poskytovat doporučení pro evakuaci, dekontaminaci a další opatření. (Tecuci, 2011)
8. **Informování a komunikace s veřejností:** Expertní systémy mohou být využity k efektivnímu šíření informací mezi veřejností v případě krizových situací. Systémy mohou automaticky generovat a distribuovat upozornění a doporučení pro obyvatelstvo na základě aktuální situace a dostupných dat. Tím se zvyšuje informovanost veřejnosti a podporuje se přijímání preventivních opatření. (Jain, 2020)

Expertní systémy simulují rozhodovací procesy a znalosti lidského odborníka v určitém oboru. Díky tomuto mohou být přínosem v oblasti bezpečnosti a ochrany obyvatelstva zejména při detekci a reakci na chemické, biologické, radiologické a jaderné hrozby a také při řízení a koordinaci záchranných operací.

### 3.4 Aplikace zpracování přirozeného jazyka v oblasti bezpečnosti

Zpracování přirozeného jazyka lze v ochraně obyvatelstva využít několika způsoby, které zahrnují analýzu a interpretaci dat získaných z různých zdrojů, automatizaci komunikace a

zlepšení přístupu k informacím. Níže jsou uvedeny některé konkrétní příklady využití NLP v ochraně obyvatelstva:

1. **Monitorování a analýza sociálních médií a zpráv:** NLP může být využito k monitorování sociálních médií a zpravodajských kanálů pro rychlou identifikaci informací o nadcházejících nebo probíhajících krizích, jako jsou přírodní katastrofy nebo epidemie. Analýza obsahu umožňuje identifikovat klíčová slova a trendy, které mohou naznačovat potřebu rychlé reakce.
2. **Detekce dezinformací a fake news:** V době krize je šíření přesných a ověřených informací klíčové. NLP může pomoci identifikovat a filtrovat dezinformace a tzv. „fake news“, což je zásadní pro udržení veřejného klidu a zajištění, že obyvatelstvo má přístup k pravdivým a užitečným informacím. (Luccioni et al., 2021)
3. **Automatizace komunikace s veřejností:** Chatboty a virtuální asistenti využívající NLP mohou poskytovat okamžité odpovědi na dotazy veřejnosti, což je zvláště užitečné během krizových situací, kdy může dojít k zatížení zdravotnických a záchranných služeb. NLP technologie mohou automatizovat odpovědi na často kladené dotazy, čímž uvolní lidské zdroje pro kritičtější úkoly.
4. **Rozpoznávání a klasifikace důležitých informací v textových datech:** NLP může být použito k rozpoznávání a klasifikaci důležitých informací v textových datech, jako jsou zprávy o incidentech, zdravotní zprávy nebo vědecké články. Tím se usnadňuje rychlé získání a analýzu důležitých informací, což je klíčové pro rychlou a efektivní reakci na krizové situace. (Li, 2018)
5. **Zlepšení přístupnosti a srozumitelnosti informací:** NLP může být využito k překladu a zjednodušení složitých oznámení a instrukcí do formy, která je srozumitelnější pro širokou veřejnost nebo pro osoby s omezenými jazykovými dovednostmi. To zahrnuje automatické generování srozumitelných shrnutí dlouhých textů nebo překlady do různých jazyků. (Jain et al., 2020)
6. **Podpora při zpracování a analýze velkých objemů textových dat:** V oblasti ochrany obyvatelstva se generuje obrovské množství textových dat, včetně zpráv o incidentech, zdravotních záznamech a vědeckých studií. NLP může pomoci automatizovat procesy extrakce, zpracování a analýzy těchto dat, což umožňuje rychlejší získávání poznatků a informací potřebných pro rozhodování a plánování.

7. **Vzdělávání a školení:** NLP může být také využito pro vytváření vzdělávacích a školicích materiálů pro obyvatelstvo i profesionály. Automatizované generování přizpůsobených školicích modulů nebo simulací na základě aktuálních potřeb a situací může zlepšit připravenost na krizové situace. (Lipton et al., 2003)
8. **Vytváření a šíření varování a instrukcí pro obyvatelstvo:** NLP technologie mohou být využity k automatickému generování a šíření varování a instrukcí pro obyvatelstvo v případě krizových situací. To zahrnuje přizpůsobení komunikace pro různé demografické skupiny a jazykové verze, což zvyšuje efektivitu a dosah těchto zpráv.
9. **Zlepšení přesnosti a relevanci vyhledávání informací:** V době krize je rychlý přístup k relevantním informacím klíčový. NLP může zlepšit vyhledávací systémy tím, že umožní sofistikovanější dotazy a lepší porozumění kontextu a potřeb uživatelů, což vede k rychlejšímu a přesnějšímu nalezení potřebných informací. (Tecuci, 2011)
10. **Analýza a generování zpráv:** NLP může automatizovat procesy analýzy dat a generování zpráv, což umožňuje rychlejší a efektivnější sdílení informací s veřejností i mezi různými agenturami a organizacemi zapojenými do ochrany obyvatelstva. Tím se zvyšuje schopnost rychle reagovat na vzniklé situace a efektivně koordinovat záchranné a pomocné akce. (Al-suqri and Guillani, 2022)
11. **Podpora rozhodování a plánování:** NLP může poskytovat podporu při rozhodování a plánování tím, že umožní rychlou analýzu velkých objemů textových dat a extrakci relevantních informací. To může zahrnovat analýzu trendů, predikci vývoje situací nebo identifikaci potřebných zdrojů a kapacit. (Abdulhussein et al., 2020)

Zpracování přirozeného jazyka je v oblasti bezpečnosti a ochrany obyvatelstva přínosem zejména díky možnosti zlepšení přesnosti a relevanci vyhledávání informací a rozpoznávání a klasifikace důležitých informací v textových datech. Velkým přínosem je také využití speciálních chatbotů a virtuálních asistentů, které mohou poskytovat okamžité odpovědi na dotazy veřejnosti.

## DÍLČÍ ZÁVĚR

Umělá inteligence a její subdisciplíny, jako jsou strojové učení, počítačové vidění, zpracování přirozeného jazyka a expertní systémy, nabízejí značný potenciál pro zlepšení bezpečnosti a ochrany obyvatelstva. Tyto technologie mohou být využity k řešení široké škály bezpečnostních výzev, včetně predikce přírodních katastrof, detekce kybernetických hrozeb, podpory rozhodování v krizových situacích, zlepšení komunikace během krizí a monitorování a reakce na environmentální hrozby. Kromě toho umožňují efektivnější využívání zdrojů, zlepšení veřejného zdraví a zvýšení dopravní bezpečnosti. Vývoj a implementace AI v oblasti bezpečnosti a ochrany obyvatelstva vyžaduje multidisciplinární přístup, který spojuje odborníky z oblasti umělé inteligence, počítačové vědy, psychologie, neurovědy a dalších relevantních oborů. Tento přístup umožňuje vývojářům a výzkumníkům lépe pochopit a modelovat složité kognitivní procesy, což vede k vytváření efektivnějších a přesnějších AI systémů. Jedním z klíčových aspektů využití AI v oblasti bezpečnosti a ochrany obyvatelstva je schopnost těchto systémů adaptovat se na měnící se podmínky a výzvy. Například v oblasti předpovídání a reakce na přírodní katastrofy mohou AI systémy analyzovat velké množství dat z různých zdrojů, jako jsou meteorologické stanice, družicové snímky a sociální média, aby rychle identifikovaly vzory a předpověděly možné katastrofy. Tato schopnost rychlé analýzy a reakce může značně zlepšit připravenost a reakční časy, což může zachránit životy a omezit škody. Dalším příkladem je využití AI v boji proti kybernetickým hrozbám. S rostoucím počtem sofistikovaných kybernetických útoků je nezbytné mít systémy, které mohou tyto hrozby rychle detekovat a reagovat na ně. AI systémy mohou analyzovat vzorce chování v síťovém provozu a identifikovat anomálie, které mohou naznačovat pokus o útok, což umožňuje efektivní obranu proti nim. Tento adaptivní přístup je zásadní pro zajištění kybernetické bezpečnosti v dynamickém a neustále se měnícím kyberprostoru. V kontextu zlepšování reakcí na krizové situace a katastrofy, AI a její aplikace nabízejí významný potenciál pro zvýšení efektivity a účinnosti záchranných a bezpečnostních operací. Například, využití AI pro automatizované generování školicích materiálů a simulací může zlepšit připravenost na krizové situace pro obyvatelstvo i profesionály. Kromě toho, využití technologií počítačového vidění pro detekci a analýzu požárů v rané fázi umožňuje rychlejší a efektivnější reakci hasičských jednotek, což může významně snížit škody a ztráty na životech.



## **II. PRAKTICKÁ ČÁST**

## 4 NÁSTROJE UMĚLÉ INTELIGENCE A JEJICH NASAZENÍ V BEZPEČNOSTNÍCH APLIKACÍCH

Nasazení umělé inteligence (AI) v oblasti bezpečnosti a ochrany obyvatelstva představuje významný krok k zajištění efektivnější a rychlejší reakce na mimořádné události a krizové situace. AI může hrát klíčovou roli v rámci integrovaného záchranného systému, kde podporuje akceschopnost složek záchranných týmů, včetně jednotek sborů dobrovolných hasičů obcí, a to prostřednictvím analýzy dat a predikce potenciálních hrozeb. Tato technologie umožňuje rychlejší a přesnější rozhodování v situacích, kdy je na prvním místě ochrana životů a majetku obyvatelstva. Dále AI přispívá k rozvoji systému přípravy obyvatelstva na mimořádné události a krizové situace. Využitím pokročilých algoritmů a analýzy velkých dat může AI identifikovat slabiny v připravenosti a navrhnout opatření pro zlepšení. To zahrnuje i podporu dobrovolnictví a zapojení občanů do procesů ochrany obyvatelstva. (Al-suqri and Guillani, 2022)

### 4.1 Nasazení Chatbotů v bezpečnostních aplikacích

Jedním z nejrozšířenějších nástrojů využívajících umělou inteligenci je ChatBot. Klíčovou technikou, kterou chatbot využívá je porozumění přirozeného jazyka, které umožňuje chatbotům porozumět a interpretovat lidský jazyk. To zahrnuje analýzu a porozumění slov, frází, syntaxe a sémantiky. Díky tomuto je chatbot schopen odpovídat na dotazy v jakémkoliv jazyce. Chatboty často využívají strojové učení k trénování na velkých databázích a zdokonalení svých schopností odpovídání na otázky a poskytování informací. Modely strojového učení mohou být trénovány na předvídání odpovědí na základě historických dat. Některé chatboty využívají učení zpětnou vazbou pro zdokonalení svých schopností odpovídání v reálném čase. Model je posilován na základě toho, jaké odpovědi jsou považovány za efektivní nebo neefektivní. (Basnyat, Roy and Gangopadhyay, 2020)

V případě Mimořádné události lidé musí procházet nespočet internetových stránek nebo novin, aby se dozvěděli konkrétní informace o tom, jaké nebezpečí jim hrozí a jak mají postupovat. Toto je mnohdy zdlouhavý proces a ve spoustě nalezených informací se jen těžko vybírají ty důležité a pravdivé. V tomto nám může být přínosným pomocníkem právě Chatbot, navržený tak, aby byl v případě mimořádné události schopen rychlé odpovědi na naše otázky. (Li, 2018)

#### 4.1.1 Zhodnocení využití Chatbota v oblasti bezpečnosti

##### **Informační Zdroj pro Veřejnost:**

Chatboty mohou poskytovat aktuální a důležité informace veřejnosti týkající se bezpečnostních opatření, krizových situací, evakuací a dalších aspektů ochrany obyvatelstva.

##### **Rychlá Odezva na Dotazy:**

V době mimořádných událostí mohou chatboty rychle odpovídat na dotazy občanů ohledně aktuální situace, bezpečnostních opatření a postupů při evakuaci.

##### **Monitorování a Analýza Sociálních Médíí:**

Chatboty mohou být programovány k monitorování sociálních médií na klíčové informace o krizových situacích. Mohou identifikovat témata, zprávy nebo obavy veřejnosti.

##### **Odhad Kapacit a Potřeb:**

V případě mimořádných situací mohou chatboty pomáhat v odhadu kapacit útočišť, nemocnic, a dalších zařízení, a také sledovat aktuální potřeby obyvatelstva.

##### **Podpora Při Evakuaci:**

Chatboty mohou poskytovat navigační informace, upozornění na bezpečnostní hrozby a obecně podporovat občany během evakuace.

##### **Analýza Dat:**

Pomocí chatbotů lze analyzovat a vyhodnocovat velké množství dat, což může pomoci při identifikaci trendů, vzorů nebo odchylek v chování veřejnosti.

##### **Psychologická Podpora:**

Chatboty mohou poskytovat základní psychologickou podporu veřejnosti v situacích mimořádných událostí nebo krizových situacích.

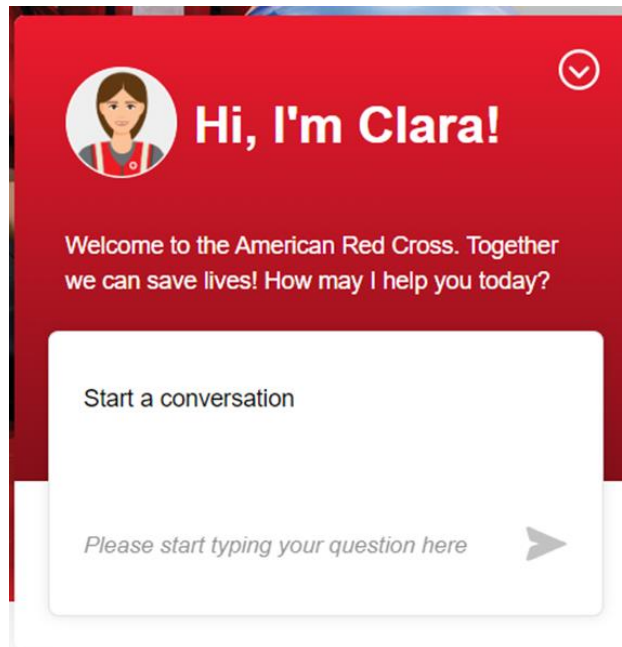
##### **Vzdělávání Obyvatelstva:**

Chatboty mohou být využity k vzdělávání obyvatelstva o připravenosti na krizové situace, první pomoci, a bezpečnostních opatřeních. (Basnyat, Roy and Gangopadhyay, 2020)

Mezi konkrétní příklady chatbotů patří Emergency respond chatbot Clara nebo FloodBot.

#### 4.1.2 Chatbot Clara

Pro navigaci přeživších katastrof vynalezl Americký červený kříž chatbota s názvem Clara, který umí komunikovat jak ve španělštině, tak v angličtině.



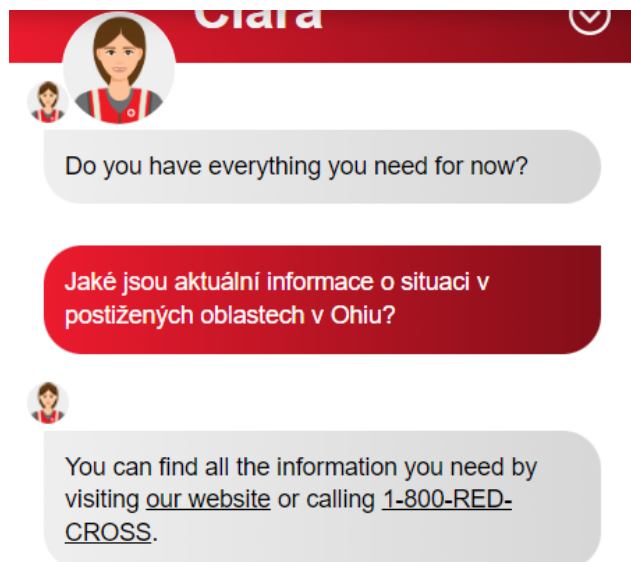
Obrázek 3– Chatbot Clara (American red cross, 2024)

Clara může odpovědět na otázky ohledně:

- Reakce na katastrofu, včetně hledání místních přístřeší nebo získání finanční pomoci,
- Finančních darů, včetně místa, kam darovat, a jak získat pomoc s darováním.
- Dobrovolnictví, včetně jak se přihlásit nebo jak se zapojit do dobrovolnické činnosti na dálku.
- Školení, jako je registrace na kurzy.
- Služby pro ozbrojené síly, včetně zdrojů pro veterány nebo členy vojenských sil.
- Mezinárodní služby, včetně informací o humanitárních akcích Amerického Červeného kříže v zahraničí.
- Darování krve, jak si domluvit schůzku na darování a další.
- Claru nalezneme na oficiálních stránkách amerického červeného kříže. (American red cross, 2024)

V průběhu března bylo okolí Ohia v Americe zasaženo několika tornády. Pro zhodnocení tohoto nástroje jsem chatbotu položila následující sadu otázek ohledně této katastrofy:

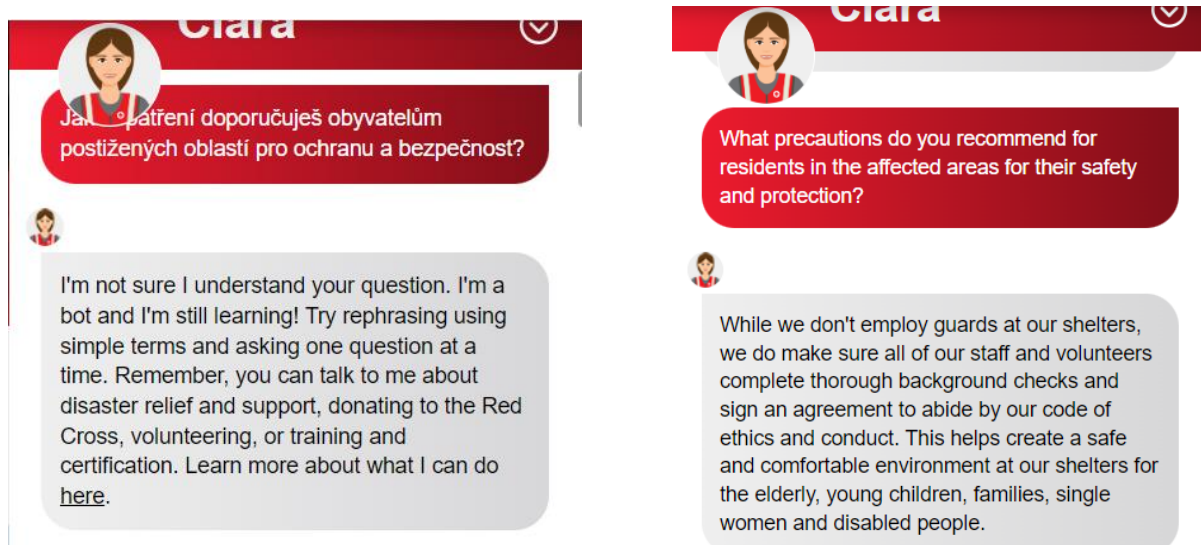
1. Jaké jsou aktuální informace o situaci v postižených oblastech v Ohiu?



Obrázek 4– Chatbot Clara, 1 odpověď (American red cross, 2024)

Odpověď chatbota na tuto otázku byl odkaz na jejich webové stránky.

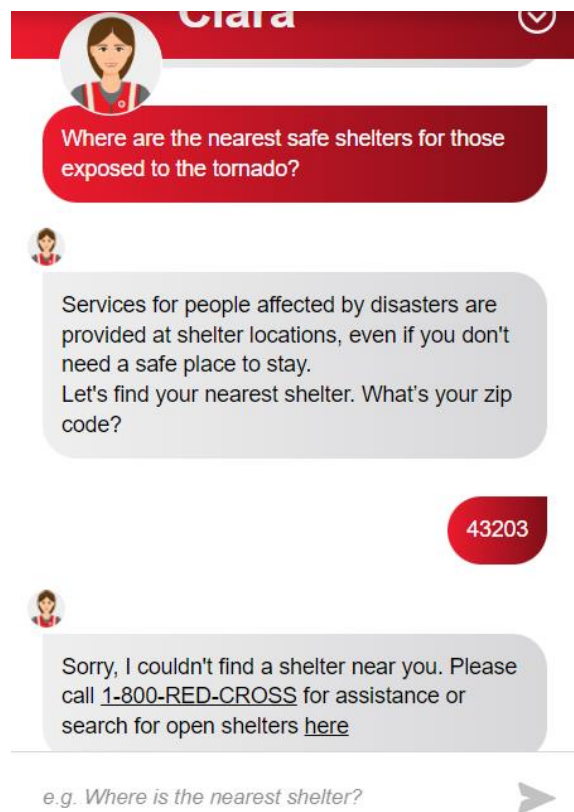
2. Jaká opatření doporučuješ obyvatelům postižených oblastí pro ochranu a bezpečnost?



Obrázek 5- Chatbot Clara, 2 odpověď (American red cross, 2024)

Této otázce chatbot neporozuměl, proto jsem pokračovala v zadávání otázek v anglickém jazyce. Na druhou otázku byla odpověď, že dbají na to, aby zaměstnanci a dobrovolníci vytvářeli bezpečné a pohodlné prostředí pro azylové domy červeného kříže.

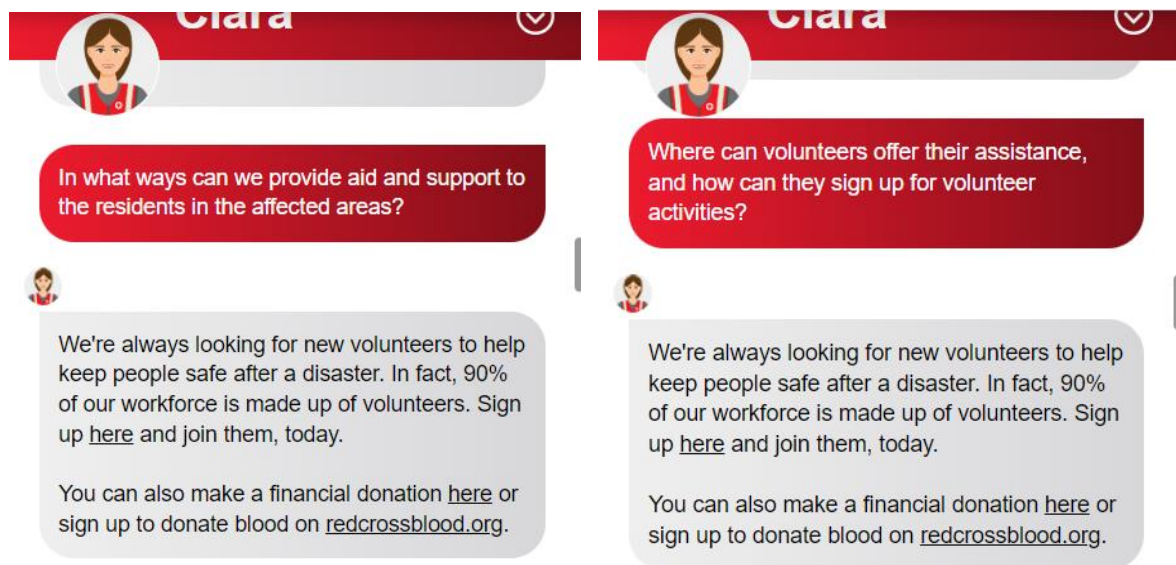
3. Kde se nacházejí nejbližší bezpečné útočiště pro ty, kteří byli vystaveni tornádu?



Obrázek 6– Chatbot Clara, 3 odpověď (American red cross, 2024)

Zde se chatbot doptal na poštovní směrovací číslo konkrétního města, aby mohl najít informace o nejbližším útočišti. Zadala jsem směrovací číslo města Columbus, který byl jedním z postižených měst tornádem v Ohiu. V odpovědi stálo, že se v blízkosti Columbusu nenachází žádné útočiště a pro více informací zde bylo uvedeno telefonní číslo Amerického červeného kříže a odkaz na webové stránky.

4. Jakými způsoby můžeme poskytnout pomoc a podporu obyvatelům postižených oblastí?
5. Kde mohou dobrovolníci nabídnout svou pomoc a jak se mohou přihlásit k dobrovolnickým aktivitám?

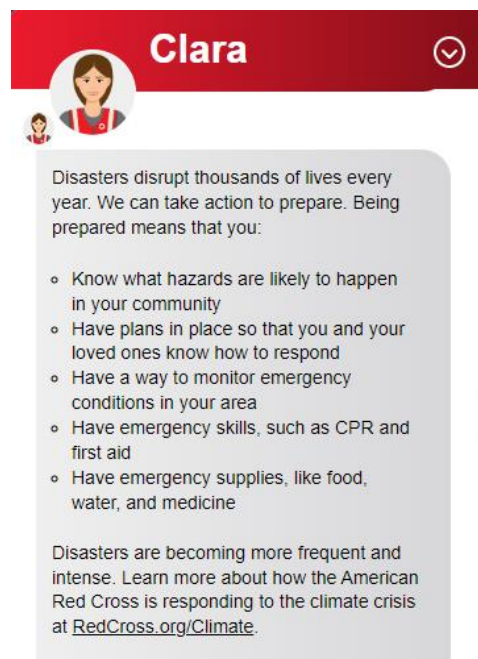


Obrázek 7- Chatbot Clara, 4 a 5 odpověď (American red cross, 2024)

Na obě následující otázky byla stejná odpověď, ve které stálo, že stále hledají možné dobrovolníky. Dále odpověď obsahovala odkaz na formulář, kde je možno přihlásit se k dobrovolníkům nebo darování krve.

6. Co má obsahovat evakuační zavazadlo

7. Jak mám postupovat při evakuaci?



Obrázek 8 Chatbot Clara, 6 odpověď (American red cross, 2024)

Na obě tyto otázky chatbot vygeneroval stejnou odpověď, ve které v pěti bodech popsal, jak být připraven na katastrofy.

### SWOT analýza:

Silné stránky	hodnocení	váha	Slabé stránky	hodnocení	váha
Dostupnost	5	0,7	Omezená interaktivita	-5	0,6
Rozmanitost informací	3	0,3	Závislost na technologii	-4	0,2
			Omezená jazyková dostupnost	-2	0,2
<b>Příležitosti</b>			<b>Hrozby</b>		
Rozšíření funkcí	5	0,5	Závislost na datových zdrojích	-3	0,3
Rozšíření na další platformy a integrace	4	0,5	Technologické a etické výzvy	-5	0,7

Tabulka 1 - SWOT analýza Clara

Interní část:  $4,4 - 4,2 = 0,2$

Externí část:  $4,5 - 4,4 = 0,1$

Celkově:  $0,2 + 0,1 = 0,3$

Nástroj Clara má převážně pozitivní charakteristiky, které mu pomáhají dosahovat určité úspěšnosti nebo konkurenční výhody, zároveň je vystaven významným hrozbám a zatím má omezené příležitosti k využití.

### Zhodnocení využitelnosti:

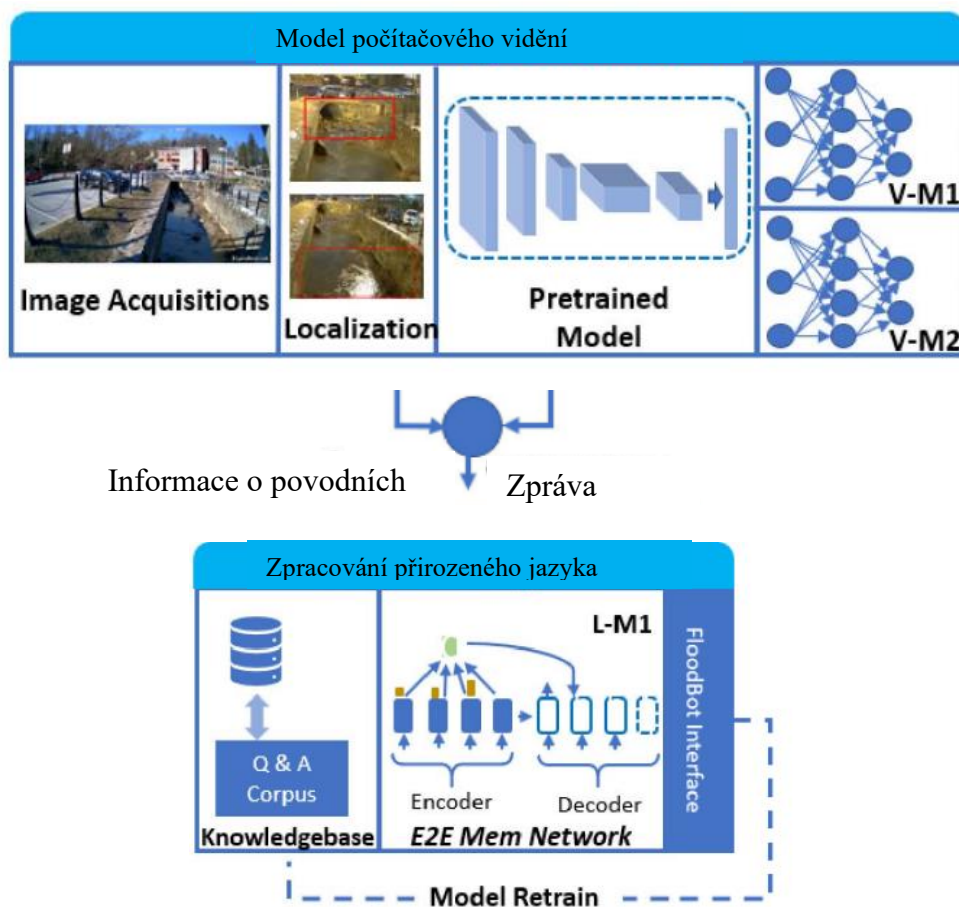
Chatbot Clara dokáže zodpovědět pomocí porozumění přirozeného jazyka i na otázky položené v českém jazyce, ne všem otázkám však porozumí. Odpovídá pouze anglicky. Není schopen vygenerovat žádné informace týkající se konkrétní katastrofy. Ve většině případů pouze odkazuje na webové stránky Amerického červeného kříže nebo na linku 911 nebo tel. číslo amerického červeného kříže. Na obecné otázky ohledně postupu při evakuaci poskytuje univerzální odpověď ohledně toho, jak být připraven na hrozící katastrofy. Tento chatbot se stále vyvíjí a zatím jsou jeho schopnosti značně omezené.

### 4.1.3 FloodBot

FloodBot je pokročilý systém založený na technologii hlubokého učení a počítačového vidění, který je navržen k monitorování a detekci záplav v reálném čase. Jeho hlavním



úkolem je analyzovat obrázky z potenciálně ohrožených oblastí a identifikovat přítomnost a rozsah záplav. FloodBot využívá kombinaci více modelů strojového učení pro detekci záplav a objektů v záplavové oblasti, což umožňuje rychlou a přesnou reakci na potenciální hrozby záplav. Tento přístup zvyšuje efektivitu a přesnost detekce tím, že využívá znalosti získané z jiných domén. Dalším důležitým aspektem je federované nasazení a výpočetní technologie na okraji sítě (Edge Computing), které umožňuje rychlejší zpracování dat a snižuje latenci v komunikaci FloodBotu. Díky tomu je možné provádět inferenci modelů přímo na zařízeních umístěných v terénu, jako jsou Raspberry Pi, Jetson Nano nebo Coral AI, což značně zlepšuje rychlost a dostupnost systému v reálném čase. FloodBot také integruje pokročilé modely pro zpracování informací a komunikaci s uživateli prostřednictvím pokročilých technik zpracování přirozeného jazyka (NLP) a konverzačního AI. Tento přístup umožňuje FloodBotu nejen identifikovat a analyzovat záplavové situace, ale také komunikovat s uživateli v přirozeném jazyce, poskytovat aktualizace, odpovídat na dotazy a nabízet relevantní informace o záplavách a jejich potenciálním dopadu na konkrétní oblasti. (Basnyat, Roy and Gangopadhyay, 2020)



Obrázek 9 – FloodBot, celková architektura (Basnyat, Roy and Gangopadhyay, 2020)

FloodBot je navržen tak, aby byl schopen autonomně shromažďovat a analyzovat data z různých zdrojů, včetně obrázků z kamer, sociálních médií a dalších digitálních platform. Díky integraci s mobilními zařízeními a sociálními sítěmi může FloodBot rychle šířit informace mezi obyvateli ohrožených oblastí a poskytovat důležité upozornění a doporučení pro evakuaci nebo jiná preventivní opatření. (Basnyat, Roy and Gangopadhyay, 2020)

### SWOT analýza:

Silné stránky	hodnocení	váha	Slabé stránky	hodnocení	váha
Využití pokročilých technologií	5	0,4	Konverzační model je stále ve vývoji	-3	0,4
AI konverzační schopnosti	4	0,3	Závislost na kvalitě a dostupnosti dat	-4	0,6
Integrace se sociálními médii	3	0,3			
<b>Příležitosti</b>			<b>Hrozby</b>		
Rostoucí poptávka po chatbotech	5	0,5	Konkurence s podobnými technologiemi	-3	0,3
Rozšíření na další platformy a integrace	4	0,5	Technologické a etické výzvy	-5	0,7

Tabulka 2 - SWOT analýza FloodBot

Interní část:  $4,1-3,6 = 0,5$

Externí část:  $4,5-4 = 0,5$

Celkově:  $0,5 - 0,5 = 1$

Nástroj FloodHub vykazuje výrazně více pozitivních než negativních charakteristik, které mu poskytují významnou konkurenční výhodu nebo umožňují dosahovat vysoké úspěchy. Slabé stránky nebo nedostatky jsou minimální, a proto nemají významný vliv na celkový úspěch.

### Zhodnocení využitelnosti:

Významným přínosem FloodBotu je především jeho schopnost poskytovat specifické informace na základě analýzy velkého množství dat, včetně obrazových dat a meteorologických informací, což umožňuje detailní hodnocení povodňových rizik. Tato schopnost nejenže zvyšuje ochranu obyvatelstva, ale také umožňuje účinnější alokaci zdrojů pro záchranné a pomocné operace. Integraci FloodBotu s mobilními zařízeními a sociálními médii by mohla zlepšit distribuci informací mezi obyvatelstvem. V době katastrof se lidé často obrací na sociální média a další online zdroje pro aktualizace.

FloodBot může tuto potřebu uspokojit tím, že poskytne rychlé a přesné informace přímo zasaženým osobám. Naopak konverzační model FloodBotu je stále ve vývoji a jeho schopnost správně identifikovat oblasti záplav je závislá na dostupnosti a kvalitě dodaných dat. Úspěšnost FloodBotu závisí na kvalitě a dostupnosti vizuálních a meteorologických dat, což může být omezeno v určitých oblastech nebo podmínkách.

## 4.2 Nasazení ostatních nástrojů umělé inteligence v bezpečnostních aplikacích

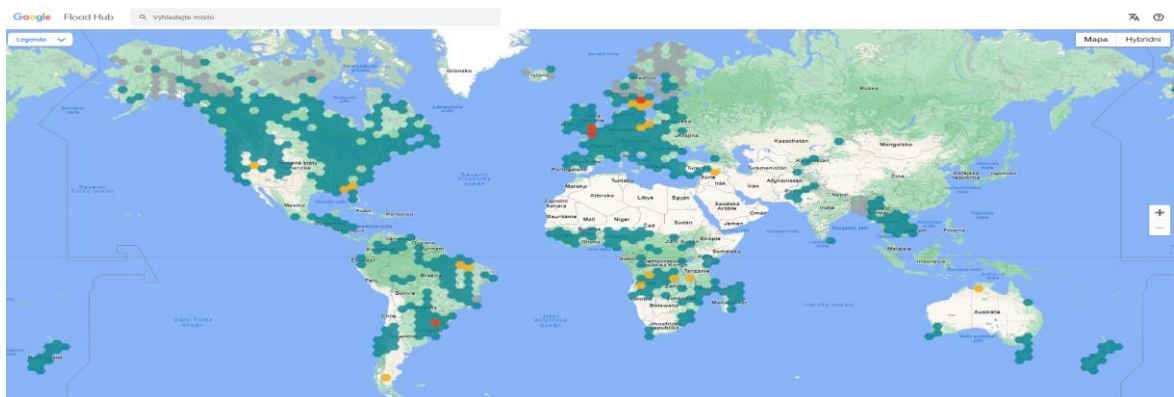
Mezi nástroje umělé inteligence, které lze využít v bezpečnostních aplikacích se zaměřením na ochranu obyvatelstva nepatří pouze chatbot, ale další spousta nástrojů, které mohou být využity například k predikci přírodních katastrof nebo k predikci výskytu a intenzity požárů. Příkladem takových aplikací je FloodHub nebo Digital Fire.

### 4.2.1 FloodHub

Umělá inteligence FloodHubu využívá různorodé, veřejně dostupné zdroje dat, jako jsou meteorologické předpovědi a satelitní snímky. Technologie pak kombinuje dva modely: Hydrologický model, který předpovídá množství vody tekoucí v řece, a model zaplavení, který předpovídá, které oblasti budou postiženy a jak hluboká voda bude.

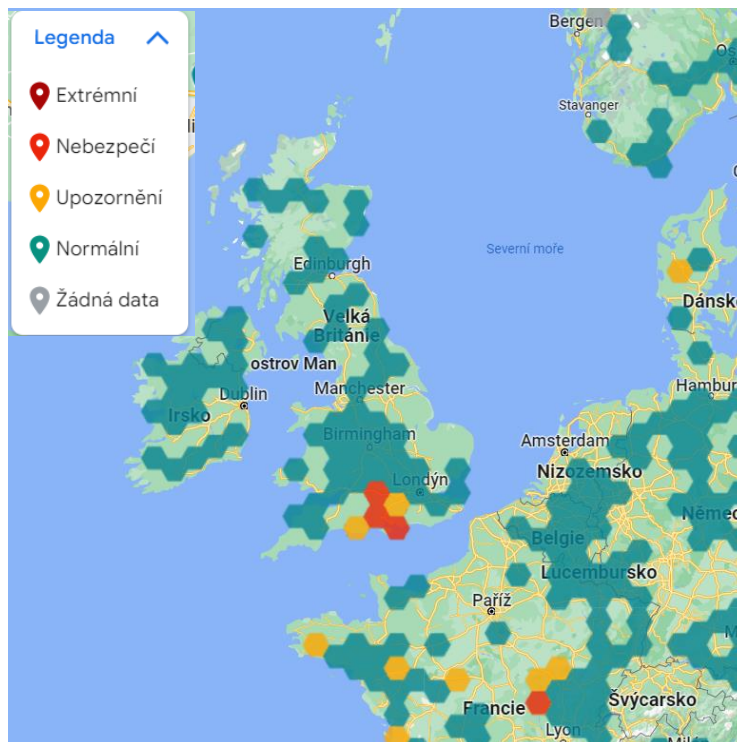
Algoritmus zpracovává veřejně dostupná data, jako jsou srážky, počasí a údaje o povodí. Na základě těchto dat předpovídá hladinu vody v řece v následujících dnech. Díky tomu lze s předstihem zjistit, zda hrozí záplavy.

AI model zaplavení pak simuluje, jak se voda bude pohybovat na základě předpovědi hydrologického modelu a satelitních snímků. Umožňuje určit, které oblasti budou zasaženy a jak vysoká bude hladina vody. (Google, 2024)



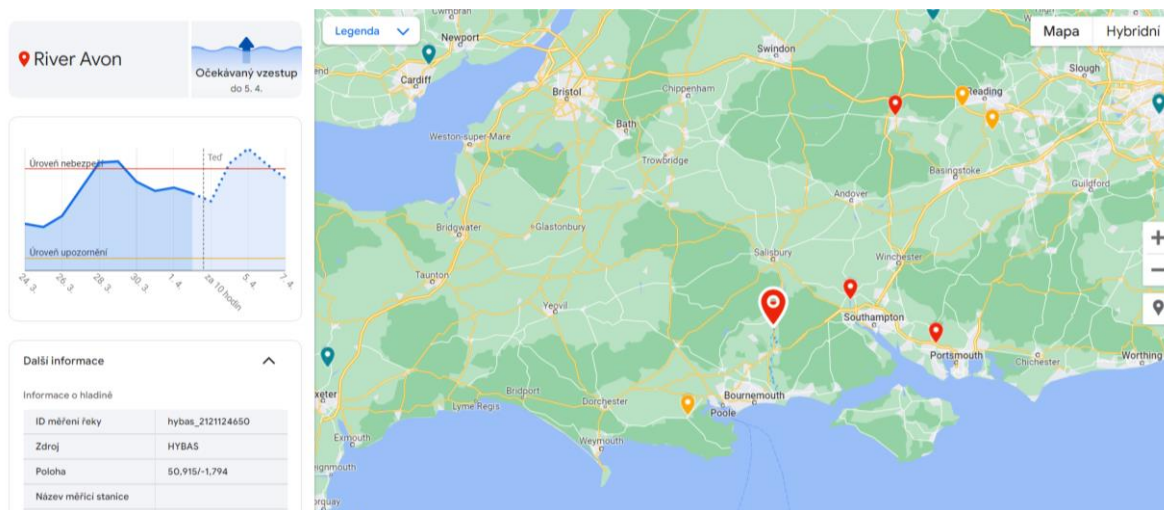
Obrázek 10– Flood Hub, mapa světa (Google, 2024)

Aplikace poskytuje aktuální informace pro 79 zemí světa.



Obrázek 11– FloodHub, mapa Velké Británie (Google, 2024)

Podle barev na mapě můžeme rozeznat, jak je na tom povodí v dané oblasti. „Úroveň upozornění“ přiřazená k jednotlivým místům ve službě Flood Hub představuje povodeň, která je v dané lokalitě očekávána v průměru jednou za dva roky. „Úroveň nebezpečí“ představuje povodeň, která je očekávána v průměru jednou za pět let.



Obrázek 12– FloodHub, River Avon (Google, 2024)

V aplikaci se můžeme podívat na aktuální stav povodí jednotlivých řek. Společně s aktuálním stavem se nám ukáže také prognóza ukazující, v jakém stavu se bude řeka nacházet v následujících dnech. Na obrázku vidíme na příkladu řeku Avon v Anglii, která se momentálně nachází na úrovni upozornění a v následujících dnech má její hladina ještě stoupat.

Další informace	
Informace o hladině	
ID měření řeky	hybas_2121124650
Zdroj	HYBAS
Poloha	50,915/-1,794
Název měřicí stanice	
Rozloha povodí	1 558,3
Ověřený model	Ano
Mapa záplav při upozornění	Ano
Limity hladiny	
Měrná jednotka	Vypouštění v metrech krychlových za sekundu
Úroveň upozornění	36,902
Úroveň nebezpečí	50,02
Extrémní úroveň	65,333

Obrázek 13– FloodHub, informace o řece Avon (Google, 2024)

Dále zde můžeme najít údaje o celkové rozloze povodí, měřicí stanici nebo limitech vodní hladiny. (Google, 2024)

### SWOT analýza:

Silné stránky	hodnocení	váha	Slabé stránky	hodnocení	váha
Pokročilá analýza dat	4	0,3	Závislost na dostupnosti dat	-5	0,5
Aktualizace v reálném čase	5	0,5	Technologická složitost	-3	0,5
Dostupnost	4	0,2			
<b>Příležitosti</b>			<b>Hrozby</b>		
Rozvoj technologie	5	0,5	Nepředvídatelnost povodní	-4	0,5
Integrace s dalšími platformami	3	0,5	Konkurence	-3	0,5

Tabulka 3 - SWOT analýza FloodHub

Interní část:  $4,5-4=0,5$   
Externí část:  $4-3,5=0,5$   
Celkově:  $0,5 + 0,5=1$

Nástroj FloodHub vykazuje výrazně více pozitivních než negativních charakteristik, které mu poskytují významnou konkurenční výhodu nebo umožňují dosahovat vysoké úspěchy. Slabé stránky nebo nedostatky jsou minimální, a proto nemají významný vliv na celkový úspěch.

#### **Zhodnocení využitelnosti:**

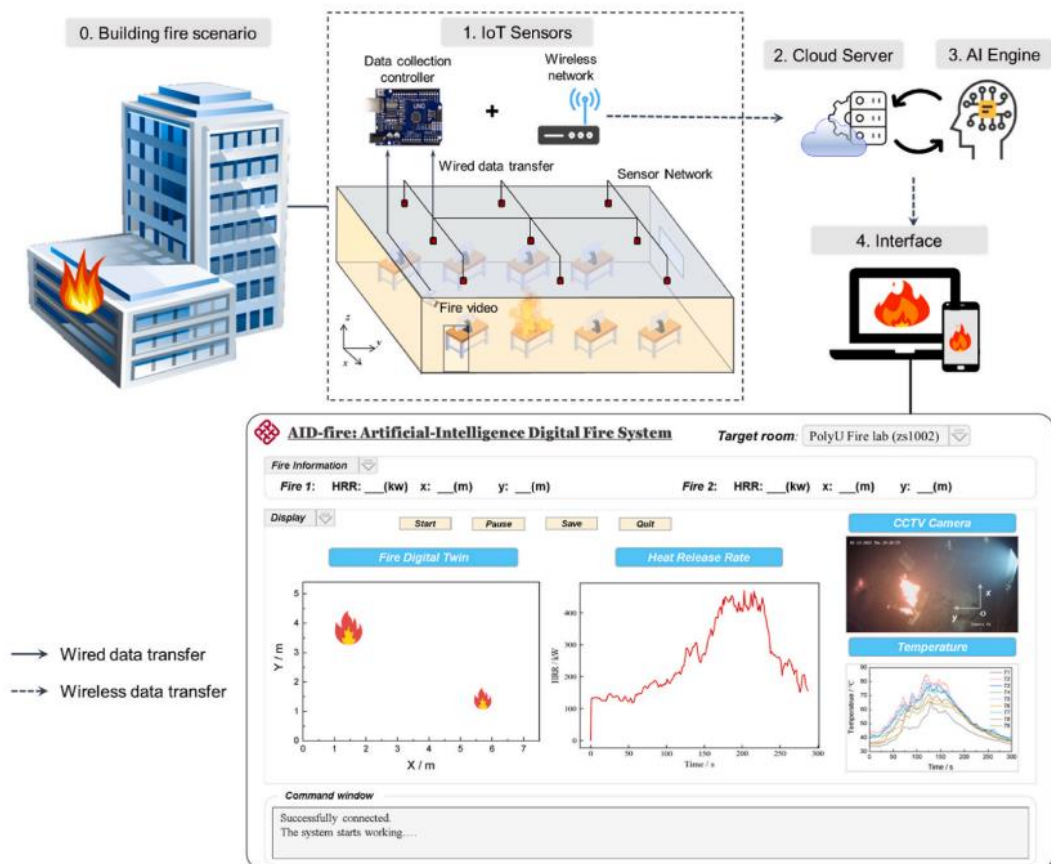
Pozitivní přínos FloodHubu je jeho schopnost poskytovat specifické informace na základě analýzy velkého množství dat, včetně obrazových dat a meteorologických informací, což umožňuje detailní hodnocení povodňových rizik. Prognózy jsou aktualizovány denně na základě nejaktuálnějších meteorologických dat. Prognózy jsou k dispozici také v denním rozlišení. Hydrologická prognóza ze vstupních dat, jako jsou srážky, teplota apod., generuje jako výstup prognózu průtoku v konkrétním povodí. Model záplavových map od Googlu je jedním z mála povodňových modelů, které na základě konkrétní hydrologické prognózy generují mapy, z nichž lze zjistit, které vesnice nebo oblasti budou zaplaveny. Toto může být přínosem pro obyvatelstvo hlavně v ohrožených územích povodněmi, které se může na takovou situaci připravit předem, a tak účinněji zabránit možným škodám způsobeným v souvislosti se vzniklou povodní. Účinnost FloodHubu je však závislá na dostupnosti a kvalitě veřejně dostupných dat. Pokud jsou data nepřesná nebo neúplná, může to ovlivnit přesnost prognóz.

#### **4.2.2 Digital Fire**

Systém Digital Fire, známý také jako AID-Fire, funguje na principu integrace čtyř hlavních komponent: senzorů IoT, cloudového serveru, AI modelu a uživatelského rozhraní. Tyto komponenty společně pracují na přenosu, správě, identifikaci a vizualizaci scénáře požáru v reálném čase. Senzory IoT sbírají teplotní data, která jsou následně přenášena na cloudový server pro ukládání a správu. AI model, založený na konvolučních dlouhodobých krátkodobých paměťových neuronových sítích (Conv-LSTM), analyzuje prostorově-časové rozložení teploty, aby identifikoval počet, velikost a polohu zdrojů požáru. Uživatelské rozhraní pak zobrazuje informace o požáru, umožňuje interakci a poskytuje důležité informace pro rozhodování v oblasti hašení požárů a evakuace. Systém AID-Fire prokázal schopnost identifikovat různé scénáře požáru s přesností vyšší než 85 %, dobu



výpočtu okolo 0,1 se zpoždění přibližně 1 s. Oproti tradičním systémům požárního hlášení, které mohou identifikovat pouze přítomnost požáru, AID-Fire poskytuje detailnější informace, jako jsou profil teploty, poloha a velikost požáru, což je důležité pro efektivní rozhodování při hašení požárů. Systém integrace dalších dat sensorů, která dokážou rozlišit mezi změnami teploty způsobenými potlačením požáru a změnami způsobenými požárem samotným. Například začlenění sensorů vlhkosti by mohlo pomoci při rozlišování mezi rychlým zvýšením vlhkosti v důsledku vodní páry z hašení požáru a změnami teploty v důsledku tepla ohně. Tento přístup by mohl zpřesnit předpovědi modelu umělé inteligence a zpřesnit jej během hasičského úsilí. Navíc vylepšení modelu umělé inteligence o rozmanitější tréninková data, která zahrnují scénáře hašení požáru, by mohlo zlepšit jeho prediktivní přesnost. Simulací nebo záznamem dat z řízených experimentů na potlačení požáru by se model AI mohl naučit rozpoznávat vzory spojené s úsilím o potlačení a podle toho upravit své předpovědi. To by pomohlo snížit počet falešných poplachů pro další zdroje požáru během fázi hašení a poskytlo by spolehlivější informace pro strategie hašení. Integrace technologií AI a IoT do systému Digital Fire (AID-Fire) demonstruje významný pokrok v detekci a správě požáru.



Obrázek 14 – Rámec procesu aplikace Digital Fire (Zang et. al, 2022)

Díky využití dat v reálném čase ze senzorů internetu věcí a použití umělé inteligence pro rychlou analýzu nabízí systém proaktivní přístup k požární bezpečnosti. Nejenže přesněji detekuje požáry, ale také poskytuje kritické informace o charakteristikách požáru, jako je velikost, umístění a intenzita, které jsou nezbytné pro efektivní hašení požáru a plánování evakuace. Systém Digital Fire představuje slibný směr ve využití technologie pro zvýšení bezpečnosti a efektivity řízení požárů. Neustálé vylepšování senzorové technologie, algoritmů AI a metod sběru dat dále rozšíří možnosti systému, což z něj činí neocenitelný nástroj při prevenci a zmírňování katastrof souvisejících s požáry. (Zang et. al, 2022)

### Využití umělé inteligence v aplikaci Digital Fire:

Systém AID-Fire využívá umělou inteligenci (AI) prostřednictvím konvolučních dlouhodobých krátkodobých paměťových neuronových sítí (Conv-LSTM), které jsou schopny učit se prostorově-časové vlastnosti teplotních dat. Tento AI model je trénován na velkou databázi obsahující 533 scénářů požárů s různými velikostmi, pozicemi a počtem zdrojů požáru. Díky tomu může AI úspěšně identifikovat informace o požáru s relativní chybou menší než 15 % a zpožděním menším než 1 sekunda. AI model také demonstruje schopnost přesně identifikovat různé scénáře požáru s přesností vyšší než 85 %, dobu výpočtu okolo 0,1 se zpožděním přibližně 1 s. To systému AID-Fire umožňuje cenovou podporu pro inteligentní hasicí praxe a napomáhá k vytvoření odolných inteligentních měst proti požárům. V porovnání s tradičními systémy požárního hlášení, které mohou identifikovat pouze přítomnost požáru, AID-Fire poskytuje podrobnější informace, jako jsou profil teploty, poloha a velikost požáru, což je důležité pro efektivní rozhodování při hašení požárů. (Zang et. al, 2022)

### SWOT analýza:

Silné stránky	hodnocení	váha	Slabé stránky	hodnocení	váha
Pokročilá technologie	4	0,3	Závislost na kvalitě a pokrytí senzorů	-4	0,6
Vysoká přesnost a rychlost	5	0,3	Výzvy s ochranou soukromí	-4	0,4
Podpora inteligentních hasicích praxí	4	0,4			
<b>Příležitosti</b>			<b>Hrozby</b>		
Rozvoj další funkcí	4	0,5	Technologické omezení	-4	0,7
Rozšíření na další oblasti	4	0,5	Konkurence	-3	0,3

Tabulka 4 - SWOT analýza Digital Fire



Interní část:  $4,3-4=0,3$   
Externí část:  $4-3,7=0,3$   
Celkově:  $0,3 + 0,3=0,6$

Výsledek SWOT analýzy u nástroje Digital Fire naznačuje poměrně pozitivní hodnocení zkoumaného prvku, avšak s mírným důrazem na pozitivní stránky. Tento nástroj má několik silných stránek, které mu poskytují určitou konkurenční výhodu nebo umožňují dosahovat úspěchů. Zároveň může mít několik slabých stránek, které by mohly omezovat jeho úspěch, ale jejich vliv je poměrně malý.

### **Zhodnocení využitelnosti:**

Využití nástroje Digital Fire v ochraně obyvatelstva představuje významný pokrok v oblasti požární bezpečnosti a ochrany obyvatelstva. Díky schopnosti systému AID-Fire detailní informace o požáru, jako jsou poloha, velikost a vývoj požáru, mohou být záchranné týmy lépe informovat a mohou efektivněji plánovat a provádět záchranné a hasicí operace. To nejen zvyšuje šance na úspěšné zvládnutí požáru, ale také minimalizuje riziko pro život obyvatelstva i hasičů. Navíc, v porovnání s tradičními systémy požárního hlášení, které mohou identifikovat pouze přítomnost požáru, AID-Fire poskytuje mnohem komplexnější a užitečnější informace. Umožňuje rychlejší a přesnější reakci na požáry, což je zásadní pro ochranu obyvatelstva a minimalizaci škod. Systém AID-Fire také ukazuje velký potenciál pro další rozvoj, včetně možnosti reálného předpovídání vývoje požáru, integrace dalších dat senzorů, která dokážou rozlišit mezi změnami teploty způsobenými potlačením požáru a změnami způsobenými požárem samotným. Například začlenění senzorů vlhkosti by mohlo pomoci rozlišit mezi rychlým zvýšením vlhkosti v důsledku vodní páry z úsilí o potlačení požáru a změnami teploty v důsledku tepla ohně. Tento přístup by mohl zpřesnit předpovědi modelu umělé inteligence a zpřesnit jej během hasičského úsilí. Navíc vylepšení modelu umělé inteligence o rozmanitější tréninková data, která zahrnují scénáře hašení požáru, by mohlo zlepšit jeho prediktivní přesnost. Simulací nebo záznamem dat z řízených experimentů na potlačení požáru by se model AI mohl naučit rozpoznávat vzory spojené s úsilím o potlačení a podle toho upravit své předpovědi. To by pomohlo snížit počet falešných poplachů pro další zdroje požáru během fází hašení a poskytlo by spolehlivější informace pro strategie hašení. Integrace technologií AI a IoT do systému Digital Fire demonstruje významný pokrok v detekci a správě požáru. Díky využití dat v reálném čase ze senzorů internetu věcí a použití umělé inteligence pro rychlou analýzu nabízí systém proaktivní přístup k požární bezpečnosti. Nejenže přesněji detekuje

požáry, ale také poskytuje kritické informace o charakteristikách požáru, jako je velikost, umístění a intenzita, které jsou nezbytné pro efektivní hašení požáru a plánování evakuace. Na druhou stranu je účinnost systému závislá na kvalitě a pokrytí senzorů IoT, což může být omezeno v některých oblastech nebo budovách. Zároveň může použití CCTV kamer a dalších senzorů může vyvolat obavy týkající se ochrany soukromí uživatelů a obyvatel. Závěrem lze říci, že systém Digital Fire představuje slibný směr ve využití technologie pro zvýšení bezpečnosti a efektivity řízení požárů. Neustálé vylepšování senzorové technologie, algoritmů AI a metod sběru dat dále rozšíří možnosti systému, což z něj činí neocenitelný nástroj při prevenci a zmírňování katastrof souvisejících s požáry.

## 5 OBLASTI VHODNÉ PRO IMPLEMENTACI NÁSTROJŮ UMĚLÉ INTELIGENCE

Oblasti vhodné pro implementaci nástrojů umělé inteligence v oblasti ochrany obyvatelstva zahrnují:

- **Zvýšené dohledové schopnosti:** AI může pomoci monitorovat veřejné prostory a analyzovat obrovské množství dat pocházejících z různých zdrojů, jako jsou satelity, drony a dohledové kamery, což pomáhá identifikovat potenciální bezpečnostní hrozby a předpovídat kriminální aktivity. Stanley Jay ve své knize *The Dawn of Robot Surveillance* z roku 2019, zmiňuje, že kamerové systémy dnešní doby bývají rozšiřovány o novou technologii, známou jako inteligentní video-analytika. S její pomocí jsou kamery schopny zaznamenat osobu na videu, vyhodnotit tuto osobu jako podezřelou a poté dokonce upozornit příslušné správní úřady nebo policii.
- **Vylepšená detekce hrozeb a kybezbezpečnost:** Algoritmy AI mohou být trénovány na detekci široké škály hrozeb, jako je neoprávněný přístup, malware a další kybernetické útoky, které mohou být pro tradiční bezpečnostní systémy těžko detekovatelné. Využití AI pro detekci a reakci na kybernetické hrozby je stále důležitější, zejména v kontextu rostoucích hrozeb ze strany státních a nestátních aktérů, jako jsou Rusko a Čína, které provádějí kyberšpionáž a usilují o kontrolu globálního datového provozu.
- **Příprava na katastrofy a reakce na ně:** V předchozích kapitolách jsme si představili nástroje jako FloodBot a Flood Hub, které hrají roli při predikci povodní. Podobně může AI identifikovat ostatní nadcházející katastrofy v reálném čase a vysílat včasné varování, což je praktické řešení pro přípravu na katastrofy. Tyto úkoly obvykle závisí na analýze a posouzení odborníky z měření senzorů v terénu, a techniky AI mohou sloužit jako alternativa k předpovídání nadcházejících událostí, jako jsou trajektorie hurikánů, bouře, zemětřesení, což je klíčové pro ochranu obyvatelstva a minimalizaci škod.
- **Ochrana kritické infrastruktury:** stejně jako v případě monitorování veřejných prostorů AI může pomoci identifikovat a monitorovat potenciální hrozby pro

kritickou infrastrukturu, včetně energetických sítí, vodních zdrojů a dopravních systémů. To je zvláště relevantní vzhledem k rizikům spojeným s čínskými investicemi do kritické infrastruktury a dominance v strategických dodavatelských řetězcích.

- Zdravotní péče a řízení pandemií: AI může hrát klíčovou roli v predikci výskytu nemocí, optimalizaci rozdělování zdravotnických zdrojů a v rychlé diagnostice, což je zásadní pro ochranu obyvatelstva před pandemiemi a jinými zdravotními hrozbami. Příkladem je využití AI při termální zobrazování na letištích v případě pandemie covid-19 nebo se využití při rozpoznávání infekce ze skenů plic pomocí počítačové tomografie viz. článek Co je umělá inteligence a jak ji využíváme? na webových stránkách Evropského parlamentu z roku 2023.
- Logistika a distribuce v krizových situacích: Článek týdeníku The Economist s názvem „How Germany’s Otto uses artificial intelligence“ přinesl informace o tom, jakým způsobem německá firma Otto využívá umělou inteligenci pro nákup, plánování a řízení zásob. Díky analýze velkého množství dat a strojovému učení vyvinuli algoritmus, který dokáže mimo jiné velmi efektivně předpovídat poptávku zákazníků v různých kategoriích zboží. Pomocí takového algoritmu může AI zlepšit efektivitu a rychlost distribuce zásob, jako jsou potraviny, léky a další nezbytné materiály, v případě přírodních katastrof nebo jiných krizových situací.
- Ochrana proti dezinformacím: Vzhledem k rostoucímu významu informačního prostoru a kybernetické bezpečnosti může AI pomoci identifikovat a bojovat proti dezinformacím, které mohou ohrozit veřejný pořádek a bezpečnost. Příkladem může být detektor „deepfake news“ od společnosti Intel s názvem FakeCatcher, který by měl dokázat detekovat falešná videa v reálném čase za pomoci analýzy proudění krve viz. článek Intel představuje Deepfake Detector v reálném čase z roku 2022 na webových stránkách společnosti Intel.
- Podpora rozhodování a krizového managementu: V článku Artificial intelligence for worker management: an overview z roku 2022 se zdůrazňuje možnost využití údajů o zaměstnancích a o způsobu, jakým vykonávají svou práci, které jsou shromažďovány v reálném čase umělou inteligencí a využívány k přijímání

automatizovaných nebo polo-automatizovaných rozhodnutí v oblasti řízení na pracovišti. Podobným způsobem může AI díky analýze velkého objemu dat z různých zdrojů poskytovat podporu při rozhodování a krizovém managementu a umožnit tak lepší predikci vývoje situací a pomáhat při plánování a koordinaci reakcí.

Implementace AI v těchto oblastech vyžaduje další výzkum a vývoj, stejně jako zajištění, že tyto technologie budou implementovány eticky a s ohledem na ochranu soukromí a bezpečnost dat.

## DÍLČÍ ZÁVĚR

Nasazení nástrojů umělé inteligence v bezpečnostních aplikacích může být klíčový pro zlepšení reakce na mimořádné události a krizové situace. V rámci praktické části práce byly představeny konkrétní příklady nástrojů AI, jako je chatbot Clara od Amerického červeného kříže, který poskytuje informace a podporu veřejnosti během katastrof, a FloodBot, který monitoruje a detekuje záplavy v reálném čase. Dále byly zmíněny aplikace FloodHub a Digital Fire, které přinášejí inovativní přístupy k řešení přírodních katastrof, jako jsou povodně a požáry, prostřednictvím analýzy dat a automatizovaných rozhodnutí. SWOT analýza odhalila některé silné a slabé stránky těchto systémů, stejně jako příležitosti a hrozby spojené s jejich implementací. Bylo zdůrazněno, že AI může hrát roli v boji proti dezinformacím, podpoře rozhodování a krizovém managementu, ale je důležité zvážit etické a soukromé otázky spojené s jejím využíváním. Závěrem, práce ukázala, že nástroje umělé inteligence, jako jsou chatbot Clara, FloodBot, FloodHub a Digital Fire, mají potenciál zlepšit připravenost na katastrofy, ochranu obyvatelstva a efektivitu reakce na krizové situace. Nicméně, pro dosažení těchto cílů je nezbytný další výzkum a vývoj, stejně jako zajištění, že tyto technologie budou implementovány eticky a s ohledem na ochranu soukromí a bezpečnost dat.

## ZÁVĚR

V této bakalářské práci jsme se zabývali využitím umělé inteligence v ochraně obyvatelstva, přičemž jsme se zaměřili na široké spektrum využití aplikací strojového učení, počítačového vidění, expertních systémů a zpracování přirozeného jazyka. Historie a vývoj umělé inteligence ukazují, že potenciál umělé inteligence v oblasti ochrany obyvatelstva je obrovský, a to jak v prevenci katastrof, tak v reakci na ně. Zjistili jsme, že umělá inteligence může hrát klíčovou roli v monitorování sociálních médií pro detekci varovných signálů, v predikci přírodních katastrof, v armádě pro vývoj autonomních systémů, v kybernetické bezpečnosti, a také v rychlé identifikaci oblastí postižených přírodními katastrofami prostřednictvím analýzy obrazů a videí. Tyto aplikace nejenže zvyšují efektivitu ochrany obyvatelstva, ale také zlepšují schopnost rychle reagovat na krizové situace a minimalizovat škody. Významnou roli hrají také chatboty, jako jsou Clara a FloodBot, které poskytují aktuální informace a podporu veřejnosti v krizových situacích. Přestože existují určitá omezení, jako je schopnost poskytovat konkrétní informace o katastrofách, je potenciál chatbotů v oblasti rychlé komunikace a poskytování podpory nezpochybnitelný. Výzkum ukázal, že chatbot Clara má potenciál být cenným nástrojem pro informování a podporu obyvatelstva v krizových situacích, ale jeho efektivita je omezena několika faktory. Jedním z hlavních omezení je jeho omezená schopnost porozumět a reagovat ve více jazycích, proto je vhodné podávat otázky pouze v anglickém nebo španělském jazyce, což může být bariérou pro neanglicky, a nešpanělsky mluvící uživatele. Navíc, Clara někdy poskytuje pouze obecné informace a odkazy na externí zdroje, místo aby poskytovala konkrétní odpovědi na specifické dotazy uživatelů. Dalším důležitým zjištěním je, že i když Clara dokáže poskytnout užitečné informace o tom, jak se připravit na katastrofy a jak reagovat v případě krize, její schopnost poskytovat specifické informace o aktuálních katastrofách nebo konkrétních bezpečných útočištích je omezená. V některých případech chatbot požaduje od uživatele zadání poštovního směrovacího čísla, aby mohl poskytnout relevantní informace, což může být pro některé uživatele nepohodlné nebo nepraktické. Přestože existují určitá omezení, výzkum také ukazuje, že chatboty jako Clara mohou hrát klíčovou roli ve zlepšování připravenosti na katastrofy a reakce na ně. Co se týče FloodBotu je vhodné vyzdvihnout schopnost jeho napojení na sociální síť a s tím spojenou schopnost získávat co nejaktuálnější informace a dále jeho schopnost napojení na mobilní zařízení a možnost okamžitého varování a upozornění obyvatelstva na hrozící nebo nastalou povodeň. V závěrečné části této práce

jsme se zaměřili na oblasti vhodné pro implementaci nástrojů umělé inteligence (AI) v kontextu ochrany obyvatelstva. V oblasti ochrany obyvatelstva a bezpečnosti jsou oblasti vhodné pro implementaci nástrojů AI rozmanité a zahrnují jak prevenci, tak reakci na krizové situace. Aplikace strojového učení mohou být využity pro analýzu velkých objemů dat z různých zdrojů, což umožňuje efektivnější predikci a prevenci katastrof.



**SEZNAM POUŽITÉ LITERATURY**

ABIODUN, Oludare Isaac; KIRU, Muhammad Ubale; JANTAN, Aman; OMOLARA, Abiodun Esther; DADA, Kemi Victoria et al., 2019. Comprehensive Review of Artificial Neural Network Applications to Pattern Recognition. Online. *IEEE Access*. Roč. 7, s. 158820-158846. ISSN 2169-3536. Dostupné z: <https://doi.org/10.1109/ACCESS.2019.2945545>. [cit. 2024-04-08].

ABDULHUSSEIN, Ansam A.; KUBA, Hassain K. a ALANSSARI, Alaa N. A., 2020. *Computer Vision to Improve Security Surveillance through the Identification of Digital Patterns*. Online. Sochi, Russia: Applications and Manufacturing (ICIEAM). Dostupné z: <https://doi.org/10.1109/ICIEAM48468.2020.9112022>. [cit. 2024-02-15].

AL-SUQRI, Mohammed Nasser a Maryam GILLANI, 2022. A Comparative Analysis of Information and Artificial Intelligence Toward National Security. Online. *IEEE Access*. 10, 64420-64434. ISSN 2169-3536. Dostupné z: [doi:10.1109/ACCESS.2022.3183642](https://doi.org/10.1109/ACCESS.2022.3183642). [cit. 2023-12-07].

BORISOVA, Angela R. a NIKOLOV, Linko G., 2023. SYSTEMS WITH ARTIFICIAL INTELLIGENCE FOR DEFENSE AND SECURITY. Online. *SCIENTIFIC RESEARCH AND EDUCATION IN THE AIR FORCE*. 2023-07-28, roč. 24, s. 53-58. ISSN 22473173. Dostupné z: <https://doi.org/10.19062/2247-3173.2023.24.7>. [cit. 2024-04-08].

ČESKO. MINISTERSTVO OBRANY. Bezpečnostní strategie ČR. Online. Praha: Ministerstvo obrany České republiky, ©2023. Dostupné z: [https://mocr.army.cz/images/id\\_40001\\_50000/46088/Bezpecnostni\\_strategie\\_Ceske\\_republiky\\_2023.pdf](https://mocr.army.cz/images/id_40001_50000/46088/Bezpecnostni_strategie_Ceske_republiky_2023.pdf). [cit. 2024-02-03].

ČESKO. MINISTERSTVO VNITRA. Koncepce ochrany obyvatelstva do roku 2025 s výhledem do roku 2030. Online. Praha: Ministerstvo vnitra České republiky, ©2021. Dostupné z: [file:///C:/Users/janam/Downloads/Koncepce\\_OOb\\_2025-2030%20\(1\).pdf](file:///C:/Users/janam/Downloads/Koncepce_OOb_2025-2030%20(1).pdf) [cit. 2024-02-03].

D. SAFFAH, Dr. Mariam a HAMEED AL-HINDAWI, Dr. Fareed, 2021. Deixis: A Pragmatic Perspective. Online. *The International Journal of Social Sciences and Humanities Invention*. 2021-06-10, roč. 8, č. 06, s. 6488-6496. ISSN 2349-2031. Dostupné z: <https://doi.org/10.18535/ijsshi/v8i06.03>. [cit. 2024-04-08].

ERTEL, Wolfgang, 2017. *Introduction to Artificial Intelligence*. 2nd ed. 2017. Imprint: Springer. Undergraduate Topics in Computer Science. ISBN 978-3-319-58486-7

GIARRATANO, Joseph C., 1998. *Experiment Systems: Principles and Programming*. 3rd ed. Boston: PWS Publishing Company. ISBN 0-534-95053-1

GOOGLE, 2024. FloodHub. GOOGLE. FloodHub, 2024. Online. Dostupné z: <https://sites.research.google/floods/1/0/0/3>. [cit. 2024-04-08].

JAIN, Harsh et al., 2020. Weapon Detection using Artificial Intelligence and Deep Learning for Security Applications. Online. In: *2020 International Conference on Electronics and Sustainable Communication Systems (ICESC)*. IEEE, s. 193-198. ISBN 978-1-7281-4108-4. Dostupné z: doi:10.1109/ICESC48915.2020.9155832. [cit. 2024-02-15].

KAUL, Vivek; ENSLIN, Sarah a GROSS, Seth A., 2020. History of artificial intelligence in medicine. Online. *Gastrointestinal Endoscopy*. Roč. 92, č. 4, s. 807-812. ISSN 00165107. Dostupné z: <https://doi.org/10.1016/j.gie.2020.06.040>. [cit. 2024-04-08].

KRISHNAMOORTHY, C.S. a RAJEEV, S., 2018. *Artificial Intelligence and Expert Systems for Engineers*. Online. 11. CRC Press. ISBN 9781315137773. Dostupné z: <https://doi.org/10.1201/9781315137773>. [cit. 2024-04-08].

KUMAR, Ela, 2011. *Natural Language Processing*. 4. I K International Publishing House. ISBN 9380578776.

LARKIN, Howard D., 2022. FDA Approves Artificial Intelligence Device for Guiding Regional Anesthesia. Online. *JAMA*. 2022-12-06, roč. 328, č. 21. ISSN 0098-7484. Dostupné z: <https://doi.org/10.1001/jama.2022.20029>. [cit. 2024-04-08].

LI, Xin a SHI, Yiliang, 2018. Computer Vision Imaging Based on Artificial Intelligence. Online. In: *2018 International Conference on Virtual Reality and Intelligent Systems (ICVRIS)*. IEEE, s. 22-25. ISBN 978-1-5386-8031-5. Dostupné z: <https://doi.org/10.1109/ICVRIS.2018.00014>. [cit. 2024-04-08].

LIPTON, A.J.; REARTWELL, C.H.; HAERING, N. a MADDEN, D., 2003. Automated video protection, monitoring & detection. Online. *IEEE Aerospace and Electronic Systems Magazine*. Roč. 18, č. 5, s. 3-18. ISSN 0885-8985. Dostupné z: <https://doi.org/10.1109/MAES.2003.1201453>. [cit. 2024-04-08].

MAHESH, Batta, 2018. Machine Learning Algorithms. Online. *International Journal of Science and Research*, 9(1), ISSN 2319-7064. Dostupné z: <https://ijsr.net/archive/v9i1/ART20203995.pdf>. [cit. 2024-04-08].

PANNU, Avneet, 2015. Artificial intelligence and its scope in different areas with special reference to the field of education. Online. *International Journal of Engineering and Innovative Technology*, 4(10), ISSN 2277-3754. Dostupné z: [https://www.ijeit.com/Vol%204/Issue%2010/IJEIT1412201504\\_15.pdf](https://www.ijeit.com/Vol%204/Issue%2010/IJEIT1412201504_15.pdf). [cit. 2024-04-08].

PYAYT, A. L.; MOKHOV, I. I.; KOZIONOV, A.; KUSHERBAEVA, V.; MELNIKOVA, N. B. et al., 2011. Artificial intelligence and finite element modelling for monitoring flood defence structures. Online. In: *2011 IEEE Workshop on Environmental Energy and Structural Monitoring Systems*. IEEE, s. 1-7. ISBN 978-1-4577-0610-3. Dostupné z: <https://doi.org/10.1109/EESMS.2011.6067047>. [cit. 2024-04-08].

ROUDNÝ, Radim a LINHART, Petr, 2004. *Krizový management*. Pardubice: Univerzita Pardubice. ISBN80-7194-674-5.

RUSSELL, Stuart J. a Peter NORVIG, 2010. *Artificial intelligence: a modern approach*. 3rd ed. Upper Saddle River: Prentice Hall. Prentice Hall series in artificial intelligence. ISBN 978-0136042594.

SZELISKI, Richard, 2022. Computer Vision. Online. *Texts in Computer Science*. Cham: Springer International Publishing. ISBN 978-3-030-34371-2. Dostupné z: <https://doi.org/10.1007/978-3-030-34372-9>. [cit. 2024-04-08]

TECUCI, Gheorghe, 2012. Artificial intelligence. Online. *WIREs Computational Statistics*. Roč. 4, č. 2, s. 168-180. ISSN 1939-5108. Dostupné z: <https://doi.org/10.1002/wics.200>. [cit. 2023-12-06].

THE AMERICAN NATIONAL RED CROSS. Meet Clara, the Disaster Response Chatbot, 2024. THE AMERICAN NATIONAL RED CROSS. *American red cross*. Online. 2024. Dostupné z: <https://www.redcross.org/get-help/disaster-relief-and-recovery-services/meet-clara.html>. [cit. 2024-04-08].

WANG, Pei, 2019. On Defining Artificial Intelligence. Online. *Journal of Artificial General Intelligence*. 2019-01-01, roč. 10, č. 2, s. 1-37. ISSN 1946-0163. Dostupné z: <https://doi.org/10.2478/jagi-2019-0002>. [cit. 2024-04-08].

WORLD ECONOMIC FORUM, 2023. The Global Risks Report 2023. 18th edition. ISBN 978-2-940631-36-0. [cit. 2024-02-16]

ZANG Tianhang, WANG Zilong, ZENG Yanfu, WU Xiqiang, HUANG Xinyan, XIAO Fu, 2022. Building Artificial-Intelligence Digital Fire (AID-Fire) system: A real-scale demonstration. Online. *Journal of Building Engineering. Journal of building engineering*. Amsterdam: Elsevier, 62(105363). ISSN 2352-7102. Dostupné z: <https://doi.org/10.1016/j.jobe.2022.105363>. [cit. 2024-03-08].

ZELINKA, Ivan, 2003. *Umělá inteligence: hrozba nebo naděje?* Praha: BEN – technická literatura. ISBN 80-7300-068-7

## SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AI Umělá inteligence

ML počítačové učení

NPL zpracování přirozeného jazyka

**SEZNAM OBRÁZKŮ**

Obrázek 1- Agent a prostředí (Russel and Norvig, 2012) .....	13
Obrázek 2-Stádia porozumění přirozeného jazyka (Tecuci, 2011) .....	18
Obrázek 3– Chatbot Clara (American red cross, 2024).....	36
Obrázek 4– Chatbot Clara, 1 odpověď (American red cross, 2024) .....	37
Obrázek 5- Chatbot Clara, 2 odpověď (American red cross, 2024) .....	37
Obrázek 6– Chatbot Clara, 3 odpověď (American red cross, 2024) .....	38
Obrázek 7- Chatbot Clara, 4 a 5 odpověď (American red cross, 2024) .....	39
Obrázek 8 Chatbot Clara, 6 odpověď (American red cross, 2024) .....	39
Obrázek 9 – FloodBot, celková architektura (Basnyat, Roy and Gangopadhyay, 2020) ....	41
Obrázek 10– Flood Hub, mapa světa (Google, 2024) .....	43
Obrázek 11– FloodHub, mapa Velké Británie (Google, 2024) .....	44
Obrázek 12– FloodHub, River Avon (Google, 2024) .....	44
Obrázek 13– FloodHub, informace o řece Avon (Google, 2024) .....	45
Obrázek 14 – Rámec procesu aplikace Digital Fire (Zang et. al, 2022) <b>Chyba!</b>	<b>Záložka</b>
<b>není definována.</b>	

## **SEZNAM TABULEK**

Tabulka 1 - SWOT analýza Clara.....	40
Tabulka 2 - SWOT analýza FloomBot .....	42
Tabulka 3 - SWOT analýza HloodHub.....	45
Tabulka 4 - SWOT analýza Digital Fire.....	48