

POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostního managementu

Katedra managementu a informatiky

Bezpečnostní aspekty umělé inteligence

Diplomová práce

Security Aspects of Artificial Intelligence

Master thesis

VEDOUCÍ PRÁCE
RNDr. Václav HNÍK, CSc.

AUTOR PRÁCE
Bc. Tomáš MATÝS

PRAHA

2023

ČESTNÉ PROHLÁŠENÍ

Prohlašuji, že předložená práce je mým autorským dílem, které jsem vypracoval samostatně. Veškerou použitou literaturu a další zdroje, z nichž jsem čerpal v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Praze, dne

.....

Tomáš Matýs

ANOTACE

Diplomová práce se zabývá umělou inteligencí a aktuálními trendy v bezpečnosti týkající se umělé inteligence včetně připravované právní legislativy. Umělá inteligence zasahuje nás všechny čím dál tím víc a stává se stále více diskutovatelným tématem. Vzhledem k tomu, že se stále více soukromých a veřejných institucí digitalizuje a automatizuje kvůli průmyslu 4.0, tak nevyhnutelně některé služby stále více používají AI algoritmy nebo samotnou specializovanou umělou inteligenci například v překladech, v automobilovém průmyslu nebo digitálním umění.

KLÍČOVÁ SLOVA

kyberprostor * umělá inteligence * digitální umění * automobilový průmysl * překladatelství * malware * osobní data * bezpečnost * školství * internet věcí

ANNOTATION

This thesis deals with Artificial Intelligence and current trends in AI security, including upcoming legal legislation. Artificial Intelligence is affecting all of us more and is becoming an increasingly debated topic. As increasingly private and public institutions are being digitized and automated due to Industry 4.0, some services are increasingly using AI algorithms or specialized AI itself, for example in translations, the automotive industry or digital art.

KEYWORDS

cyberspace * artificial intelligence * digital art * automotive Industry * translation services * malware * personal data * security * educational system * internet of things

PODĚKOVÁNÍ

Tímto bych rád poděkoval vedoucímu práce panu RNDr. Václavu Hníkovi, CSc. za věnovaný čas, připomínky i rady a za odborné vedení, které mi usnadnily psaní mé odborné diplomové práce, rodičům a zaměstnancům knihovny Policejní akademie České republiky v Praze za ochotu.

Obsah

ÚVOD.....	7
1. CÍLE A METODIKA PRÁCE	8
2. TEORETICKÁ ČÁST	9
2.1 UMĚLÁ INTELIGENCE	9
2.2 PRÁVNÍ ÚPRAVY UMĚLÉ INTELIGENCE U NÁS A V ZAHRANIČÍ	10
2.3 KYBERNETICKÁ BEZPEČNOST A KYBERNETICKÝ PROSTOR	17
2.4 KYBERNETICKÉ HROZBY UMĚLÉ INTELIGENCE	19
2.5 KYBERTERORISMUS A UMĚLÁ INTELIGENCE	21
2.5.1POTENCIONÁLNÍ CÍLE KYBERTERORISMU 21	
2.5.2INSTITUCE, KTERÉ BY SE MĚLY ZABÝVAT BEZPEČNOSTÍ A UMĚLOU INTELIGENCÍ.....	22
3. PRAKTICKÁ ČÁST.....	30
3.1 UMĚLÁ INTELIGENCE V RŮZNÝCH ODVĚTVÍCH A KRITÉRIA HODNOCENÍ KAUZ S NÍ SPOJENÁ V ROCE 2022/2023	30
3.2 VYBRANÉ PŘÍPADY A BEZPEČNOSTNÍ SITUACE SPOJENÉ S UMĚLOU INTELIGENCÍ.....	31
3.2.1UMĚLÁ INTELIGENCE V ČÍNĚ A JEJÍ BEZPEČNOSTNÍ HROZBA 32	
3.2.2 KAUZY S VYUŽITÍM UMĚLÉ INTELIGENCE V AUTOMOBILOVÉM PRŮMYSLU	40
3.2.3 KAUZY S POUŽITÍM UMĚLÉ INTELIGENCE V DIGITÁLNÍM UMĚNÍ 48	
3.3 RIZIKA UMĚLÉ INTELIGENCE PRO PRACOVNÍ LOKÁLNÍ A GLOBÁLNÍ TRH.....	55
4. DOPORUČENÍ	62

ZÁVĚR	64
SEZNAM OBRÁZKŮ	66
SEZNAM LITERATURY	67

ÚVOD

Umělá inteligence je v současné době jedním z nejvíce diskutovaných témat v oblasti technologického výzkumu a vývoje. Nejde již o výplod lidské fantazie, jak tomu bylo dříve, ale očekává se, že umělá inteligence přinese velké výhody pro společnost. Avšak s jejím rozšiřujícím využíváním také roste potřeba zabezpečit tyto systémy před útoky a nežádoucím poškozením, ale také zneužitím. Bezpečnost umělé inteligence je proto nezbytná pro udržení bezpečnosti všech systémů a pro zajištění toho, že samotná umělá inteligence bude využívána pro pozitivní změny ve společnosti. Tato diplomová práce se zaměří na základní bezpečnostní aspekty umělé inteligence a na způsoby, jak zajistit, aby byly systémy umělé inteligence bezpečné. Bezpečnost umělé inteligence je pro všechna odvětví lidské činnosti stejně důležitá, protože může chránit nejen osobní údaje a informace o lidech, usnadňovat práci, třídění informací apod. Vzhledem k tomu, že použití umělé inteligence se stává stále důležitějším nástrojem také pro školy, je důležité, aby se vyvinula a implementovala odpovídající strategie bezpečnosti umělé inteligence také v této oblasti. Rovněž se budeme zabývat odvětvími, která jsou nejvíce ohrožena.

1. CÍLE A METODIKA PRÁCE

Cílem této diplomové práce je seznámit a přinést konkrétní vhledy, predikce a řešení včetně dlouhodobého pohledu na problematiku umělé inteligence a bezpečnostních aspektů okolo ní, jak z pohledu nedaleké minulosti v roce 2022, tak i z pohledu současného dění v roce 2023. Budu prozkoumávat a analyzovat současný stav v této oblasti, identifikovat a popisovat klíčové aplikace umělé inteligence v současnosti, zároveň popisovat trendy a výzvy, které umělá inteligence představuje v oblastech jako jsou například lékařství, finanční služby, průmyslové aplikace, digitální umění, automobilový průmysl apod. Budu představovat nové přístupy a metody v této oblasti či navrhopvat a vyhodnocovat možnosti budoucího využití umělé inteligence a jejích technologických aplikací.

Teoretická část práce se zaměří na vysvětlení pojmů, představení jednotlivých typů právních úprav, kyberterorismus a představení institucí, které se tím zabývají. Zmíněny budou obecné hrozby v této oblasti.

Vlastní praktickou částí této seminární práce bude určení dílčích problémů umělé inteligence s využitím případových studií. Vybral jsem si několik kauz, které probírám detailněji, a kde poté navrhuji jejich možné řešení či zlepšení. Rozebírám tam dále šířeji tendence vývoje umělé inteligence a jejích bezpečnostních aspektů s možnostmi jejich řešení.

V závěru práce zhodnotím získané výsledky jak ze strany analýz, tak z internetových aplikací či vědeckých publikací. Na základě těchto dílčích analýz kauz, trendů a výsledků se pokusím navrhnout zlepšení stávající situace a celkové doporučení či řešení i s poukázáním na možný střednědobý až dlouhodobý vývoj.

Během vytváření diplomové práce jsem využil mnoho zdrojového sběru informací z odborných knih, publikací, a to především z veřejně přístupných informací získaných na webových stránkách. Součástí jsou také vědecké práce univerzit a jiných soukromých společností, které se zabývají problematikou kybernetické bezpečnosti a informačních technologií.

2. TEORETICKÁ ČÁST

V této části budu pojednávat o umělé inteligenci. Zaměřím se především na právní úpravy v různých zahraničních státech, kyberterorismu a institucí, které se tímto zabývají.

2.1 UMĚLÁ INTELIGENCE

Umělá inteligence (Artificial Intelligence dále jen AI) se v dnešní době definuje poněkud těžko, a z tohoto důvodu máme mnoho definic. Jednu z nich definoval Michal Pěchouček následovně:

„AI je zaprvé vědecká disciplína a zároveň soubor softwarových nebo hardwarových technologií, které pomáhají automatizovat, zrychlovat, zpřesňovat nebo škálovat lidské kognitivní schopnosti – vnímat, poslouchat, uvažovat a rozhodovat.“¹

Intelligence umělého typu se stala nedílnou součástí života člověka, aniž by si toho byl plně vědom. Prvním stupněm je specifická umělá inteligence (Artificial Narrow Intelligence), která je určena pro konkrétní účely – například práce s informacemi, komunikace, finančnictví, doprava a zábava. Zde se využívá základní vlastnosti umělé inteligence po nastrádání obrovského množství dat za přesně stanovených podmínek vyhledávat nebo analyzovat daný problém. Tento typ AI je vhodný na provádění jednoho úkolu nebo omezeného okruhu úkolů. Jejich slabinou ale je, že jakmile se změní podmínky v nepředvídatelné, systém selže. Jde ale v současnosti o velmi využívané systémy – např. vyhledávání dotazů v aplikacích Google, doporučení videí na YouTube, také hraní počítačových her apod.

Potom je tu všestranná umělá inteligence (Artificial General Intelligence), která je srovnatelná s lidskou inteligencí – ve své komplexnosti, schopnosti abstrakce, plánování a učení se na základě získaných poznatků. Tady je zatím lidstvo na počátku vývoje, anebo se to tak nyní jeví. Vznik této inteligence je možný

1 Neurazitely.cz: informační portál o kybernetice. PĚCHOUČEK, Michal. *Umělá Inteligence a život zitrka* [online]. 13.5.2019. [cit. 3.2.2023]. Dostupné z: <https://neurazitely.cz/umela-inteligence-zivot-zitrka-michal-pechoucek/>

vytvořením alternativy lidského mozku, nebo jeho dalším vývojem. Když se povolí umělé inteligenci volné zásahy na zdokonalování systému a jeho funkcí, otevírá se potenciálně nebezpečná cesta. Ta umožňuje AI komunikovat s lidmi, pracovat s velkými objemy dat, vybírat si informace podle zadaných parametrů a hodnotit jejich obsah a přesnost, a to nejen ve vztahu k jejímu cíli, ale také v otázce důvěryhodnosti dat. Velkým problémem využití umělé inteligence je například ovládání automatizovaných zbraňových systémů, které jsou v rozporu se třemi známými zákony robotiky Isaaca Asimova.² Někteří jsou toho názoru, že umělá inteligence je spíše pokročilá statistika nebo strojové učení. Navenek to tak může sice vypadat, neboť tuto „zručnost“ umělá inteligence jistě má, ale jde o velké zjednodušení a podcenění jejích možností do budoucna.

2.2 PRÁVNÍ ÚPRAVY UMĚLÉ INTELIGENCE U NÁS A V ZAHRANIČÍ

Právní aspekty v oblasti využívání umělé inteligence jsou v současnosti teprve na počátku, neboť jde o novější obor. Shromáždil jsem tedy v této části informace o právních nařízeních řešící alespoň z části tuto problematiku v zemích či uskupeních, které jsou v této oblasti nejvyspělejší, a také nejprve situaci v naší zemi.

V **České republice** neexistuje žádná konkrétní právní úprava týkající se umělé inteligence. Existuje však celá řada právních předpisů, které se týkají obecně oblastí, jako je například ochrana osobních údajů, ochrana spotřebitele, ochrana duševního vlastnictví, ochrana soukromí atd., které se týkají i umělé inteligence. Nicméně, česká vláda schválila Strategii AI, která má za cíl přijmout moderní opatření pro podporu a rozvoj AI. Strategie AI, která platí od roku 2020, se zaměřuje na posílení právního rámce pro AI v České republice. Tím má být zajištěno, že budou zohledněna práva spotřebitelů, přírody a veřejného zdraví.

2 Czdefence.cz: *informační portál o armádních věcech*. ŠIŠKA. Martin. *Výroční zpráva Vojenského zpravodajství hovoří mimo jiné o fake news* [online]. 11. 10. 2021. [cit. 1.2.2023] Dostupné z: <https://www.czdefence.cz/clanek/vyrocní-zprava-vojenskeho-zpravodajstvi-hovori-mimo-jine-o-fake-news>

Strategie AI také stanoví, že AI musí být v souladu s právními předpisy a mezinárodními zásadami.³

V současné době Vláda České republiky také poskytuje dotační program pro podniky a organizace, které se chtějí účastnit využití AI. Tyto pokyny jsou k dispozici na webových stránkách Ministerstva průmyslu a obchodu. Pokyny jsou zaměřeny na širší hlediska, jako je výzkum a vývoj, testování a implementace AI.⁴ Rovněž je Česká republika v procesu podávání návrhů, a schvalování evropské směrnice NIS2 – nového zákona o kybernetické bezpečnosti, který má začít platit od poloviny roku 2024.⁵ Současně má ministerstvo průmyslu a obchodu připraveny krátkodobé, střednědobé a dlouhodobé plány až do roku 2035.⁶ Na to navazuje i strategie AV21, jež je iniciativa Akademie věd České republiky, která má za cíl podporovat špičkový výzkum ve veřejném zájmu. Jedním z výzkumných programů strategie je technologie pro informační společnost, který se zaměřuje na vývoj a aplikaci umělé inteligence, strojového učení, datové analýzy a dalších oblastí. Cílem tohoto programu je přispět k řešení společenských a ekonomických výzev pomocí moderních informačních technologií.⁷

V EU existuje několik právních dokumentů, které se dotýkají umělé inteligence. Nejvýznamnější je Směrnice o bezpečnosti umělé inteligence, která stanoví minimální požadavky na bezpečnost a účinnost umělé inteligence. Dalšími právními dokumenty, které se týkají AI, jsou Směrnice o duševním vlastnictví a Směrnice o ochraně osobních údajů.

3 *Databaze-strategie.cz: informační portál databází ČR. Strategie AI České republiky. (2020)* [online]. Ministerstvo průmyslu a obchodu. [cit. 1.2.2023] Dostupné z: <https://www.databaze-strategie.cz/cz/mpo/strategie/narodni-strategie-umele-inteligence-v-cr>

4 *Ris3.cz: informační portál dotačního programu ČR. Dotační program RIS3 pro podniky a organizace účastnící se AI* [online]. (2023). Ministerstvo průmyslu a obchodu. [cit. 1.2.2023]. Dostupné z: <https://www.ris3.cz/o-ris3/narodni-dimenze/priority/tematicke-vertikalni-prioritydomeny-specializace/tri-dimenze-domeny-vyzkumne-a-inovacni-specializace/klicove>

5 *Osvěta.nukib.cz: edukační portál Nukibu* [online]. [cit. 1.2.2023]. Dostupné z: <https://osveta.nukib.cz/course/view.php?id=145#section-3>

6 *Dataplan.info: webový portál úložiště dokumentů* [online]. [cit. 29.5.2023]. Dostupné z: https://www.dataplan.info/img_upload/7bdb1584e3b8a53d337518d988763f8d/nsAI.pdf

7 *Strategie.avcr.cz: webový portál Akademie věd ČR* [online]. [cit. 16.7.2023]. Dostupné z: <https://strategie.avcr.cz/programy/technologie-1>

V roce 2018 Evropská komise vydala strategii AI pro Evropu, která obsahuje několik návrhů pro přijetí právního rámce EU pro AI. Strategie zahrnuje následující pokyny a regulace:

1. Zajištění přijatelnosti: Komise žádá, aby AI byla používána v souladu s principy etiky a lidskými hodnotami.
2. Zajištění bezpečnosti: Komise požaduje, aby AI byla bezpečná a spolehlivá.
3. Podpora právní jistoty: Komise požaduje, aby byl vyvinut právní rámec pro AI, který poskytne právní jistotu pro podniky a spotřebitele.
4. Zajištění otevřenosti a průhlednosti: Komise chce, aby byla AI transparentní a měla otevřený přístup k datům, které byly využity při jejím vývoji.
5. Zajištění odpovědnosti: Komise požaduje, aby byla AI odpovědná a byla stanovena odpovědnost za její chování.
6. Zajištění odpovědnosti za šetření spotřebitelů: Komise požaduje, aby byly zajištěna ochrana spotřebitelů před zneužíváním AI.
7. Podpora výzkumu a inovací: Komise požaduje, aby byly podporovány výzkum a inovace v oblasti AI.⁸

Z hlediska etiky je nesmírně důležité se při práci s umělou inteligencí rozhodovat podle etických pokynů pro zajištění důvěryhodnosti AI.⁹

Evropská komise právě nyní schvaluje a implementuje Návrh Nařízení Evropského parlamentu a Rady, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (Akt o umělé inteligenci)¹⁰ a návrh nařízení o strojních

8 *Eur-lex.europa.eu: informační portál Evropské komise. Evropská komise. Sdělení komise evropskému parlamentu Radě. Evropskému hospodářskému a sociálnímu výboru a výboru regionů* [online]. Brusel. 25.4.2018. [cit. 1.2.2023]. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52018DC0237&from=CS>

9 *Etické pokyny pro zajištění důvěryhodnosti AI* [online]. Lucemburk: Publications Office, Evropská komise, Generální ředitelství pro komunikační sítě, obsah a technologie, 2019. <https://data.europa.eu/doi/10.2759/0856>. [cit. 1.2.2023]. Dostupné z: <https://op.europa.eu/cs/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1>

10 *Nařízení evropského parlamentu a rady, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (Akt o umělé inteligenci) a mění určité legislativní akty unie* [online]. Brusel: Evropská komise, 21.4.2021. [cit. 1.2.2023] Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A52021PC0206>

výrobcích.¹¹ Předchozí návrhy vznikly na základě koordinovaného plánu pro umělou inteligenci 2021.¹² Důležité je rovněž, že s informací o AI a zacházení s nimi je součástí i Evropského prohlášení o digitálních právech a zásadách.¹³ Důsledkem toho je „*Administrative Arrangement on Artificial Intelligence for the Public Good*“ i v rámci výzkumu a spolupráci s USA.¹⁴ V blízké budoucnosti nejspíše můžeme očekávat do roku 2030 ještě další právní změny, protože si EU toto dala za prioritu.¹⁵

V **USA** existuje několik federálních zákonů, které se dotýkají umělé inteligence. Nejvýznamnější je Zákon o ochraně osobních údajů, který definuje standardy, jakým způsobem se mohou organizace zabývat osobními údaji. Dalšími zákony, které se týkají umělé inteligence, jsou Zákon o duševním vlastnictví, Zákon o spotřebitelském ochranném právu a Zákon o ochraně soukromí.¹⁶

V roce 2021 **NATO** přijala strategii umělé inteligence, kterou podporuje a stanovuje pokyny a regulace pro její využití. Právní úpravy budou založeny na principu zodpovědnosti a bezpečnosti a zahrnovat strategii, pokyny a regulace pro využití AI v rámci NATO. Cílem bude poskytnout jasnou a konzistentní představu o postupu při uplatňování AI a poskytnout jasné pokyny pro národní státy

11 *Eur-lex.europa.eu: informační portál Evropské komise. Evropská komise. Nařízení Evropského parlamentu a rady o strojních výrobcích* [online]. Brusel. 21.4.2021. [cit. 1.2.2023]. Dostupné z: https://eur-lex.europa.eu/resource.html?uri=cellar:1f0f10ee-a364-11eb-9585-01aa75ed71a1.0023.02/DOC_1&format=PDF

12 *Digital-strategy.ec.europa.eu: oficiální informační portál Evropské unie. Evropská komise. Koordinovaný plán pro umělou inteligenci 2021 – přezkum* [online]. Brusel. 30.01.2023. [cit. 1.2.2023]. Dostupné z: <https://digital-strategy.ec.europa.eu/cs/library/coordinated-plan-artificial-intelligence-2021-review>

13 *Digital-strategy.ec.europa.eu: oficiální informační portál Evropské unie. Evropská komise. European Declaration on Digital Rights and Principles* [online]. Brusel. 07.02.2023. [cit. 8.2.2023]. Dostupné z: <https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles>

14 *Digital-strategy.ec.europa.eu: oficiální informační portál Evropské unie. Evropská komise. The European Union and the United States of America strengthen cooperation on research in Artificial Intelligence and computing for the Public Good* [online]. Brusel. 27.01.2023. [cit. 8.2.2023]. Dostupné z: <https://digital-strategy.ec.europa.eu/en/news/european-union-and-united-states-america-strengthen-cooperation-research-artificial-intelligence>

15 *Eur-lex.europa.eu: informační portál Evropské komise. Rada EU. Rozhodnutí Evropského Parlamentu a Rady (EU) 2022/2481* [online]. Brusel. 19.12.2022. [cit. 1.2.2023]. Dostupné z: <https://eur-lex.europa.eu/eli/dec/2022/2481/oj>

16 *Ai.gov: oficiální informační portál vlády USA* [online]. [cit. 8.2.2023]. Dostupné z: <https://www.ai.gov/>

a organizace.¹⁷ Na základě zkušeností z let 2021–2023 dojde ke změně a aktualizování regulací a právních předpisů, protože bezpečnostní situace se hodně změnila.¹⁸

Kanada má stále více zákonů a právních předpisů, které se týkají umělé inteligence. Kanadské úřady a orgány vykonávající právo vidí AI jako důležitý nástroj pro inovaci a vytváření příležitostí. Nejdůležitější právní úpravy AI v Kanadě jsou: Zákon o spravedlivém zacházení se zaměstnanci: Tento zákon zabraňuje zaměstnavatelům vyhazovat zaměstnance kvůli přechodu na AI. Zákon o ochraně osobních údajů a soukromí: Tento zákon zaručuje, že informace osob budou zpracovávány v souladu s příslušnými zákonnými předpisy. Zákon o kanadském občanství: Tento zákon zaručuje, že občané Kanady mají právo být informováni o tom, jaké informace o nich byly shromážděny, a jak byly použity prostřednictvím AI.

Austrálie věnovala pozornost právní úpravě AI a vydala několik právních předpisů, aby regulovala a zabezpečila její používání. Mezi tyto předpisy patří: Zákon o ochraně osobních údajů: Tento zákon zaručuje, že informace osob budou zpracovávány v souladu s příslušnými zákonnými předpisy. Zákon o etickém výzkumu: Tento zákon stanoví pravidla pro spravedlivé a etické využívání AI ve výzkumu. Zákon o ochraně spotřebitele: Tento zákon zaručuje, že spotřebitelé budou chráněni před neoprávněným využíváním AI.

Japonsko má několik právních předpisů, které regulují používání AI. Mezi tyto předpisy patří: Zákon o ochraně osobních údajů: Tento zákon zaručuje, že informace osob budou zpracovávány v souladu s příslušnými zákonnými předpisy. Zákon o etickém výzkumu: Tento zákon stanoví pravidla pro spravedlivé a etické využívání AI ve výzkumu. Zákon o informačních technologiích: Tento zákon stanoví pravidla pro spolehlivé a bezpečné nakládání s AI.

17 *Nato.int: oficiální informační portál NATO. Summary of the NATO Artificial Intelligence Strategy* [online]. Brusel. 22.10.2021. [cit. 8.2.2023]. Dostupné z: https://www.nato.int/cps/en/natohq/official_texts_187617.htm

18 *Nato.int: oficiální informační portál NATO. SNETSELAAR, David, Georg FRERKS, Lauren GOULD, Sebastiaan RIETIENS, Tim SWEIJS. Knowledge security. Insights for NATO* [online]. Brusel, 30.09.2022. [cit. 8.2.2023]. Dostupné z: <https://www.nato.int/docu/review/articles/2022/09/30/knowledge-security-insights-for-nato/index.html>

Indie je v oblasti právní úpravy AI poměrně novým hráčem. V roce 2018 vydala vláda národní strategii pro AI, ve které se zabývá právními otázkami souvisejícími s AI. Mezi tyto právní předpisy patří: Zákon o ochraně osobních údajů: Tento zákon zaručuje, že informace osob budou zpracovávány v souladu s příslušnými zákonnými předpisy. Zákon o etickém výzkumu: Tento zákon stanoví pravidla pro spravedlivé a etické využívání AI ve výzkumu. Zákon o informačních technologiích: Tento zákon stanoví pravidla pro spolehlivé a bezpečné nakládání s AI.

V roce 2020 vydala Duma (**ruský parlament**) zákon, který umožňuje vládě stanovit právní rámec pro umělou inteligenci. Zákon upravuje rozsah a použití umělé inteligence v rámci veřejného a soukromého sektoru prostřednictvím přísných regulačních standardů a opatření.

V **Číně** vypracovala Komise pro vědu a technologii Čínské lidové republiky (CSTC) první návrh Právního předpisu o AI, který je nyní v procesu schvalování. Tento předpis by měl zahrnovat všechny AI technologie, které využívají čínské zdroje dat a zajišťovat, aby AI byly v souladu s čínskými právními a etickými standardy. V květnu 2019 byly schváleny Pekingské AI principy.¹⁹

V červnu 2020 vydalo **iránské ministerstvo informačních a komunikačních technologií** (MTICT) první právní úpravu o umělé inteligenci, která stanoví etické, bezpečnostní a právní normy pro AI. Tento předpis upravuje AI podnikání, výzkum a vývoj a provádění AI pro veřejné instituce a poskytovatele služeb.

V červenci 2020 **Německo** schválilo zákon zvaný Zákon o digitálních službách, který vyžaduje, aby společnosti v oblasti AI poskytovaly veřejnosti informace o tom, jak AI systémy fungují. Zákon také vyžaduje, aby AI systémy byly transparentní a poskytovaly informace o tom, jak a proč systém činí určitá rozhodnutí.

V **Izraeli** je připravována legislativa týkající se umělé inteligence (AI). Ministerstvo práce a sociálních věcí vypracovalo návrh zákona o AI, který byl

19 KOLAŘÍKOVÁ, Linda a Filip HORÁK. *Umělá inteligence a právo*. Praha: Wolters Kluwer, 2020. [cit. 27.11.2022]. s. 48. ISBN 978-80-7598-783-9.

schválen v Knesetu v červnu 2020. Návrh zákona obsahuje specifický rámec pro AI, který stanoví zásady pro posuzování technologií, které by se měly používat a jakým způsobem mají být regulovány. Cílem zákona je také udržovat etický standard v AI a zajistit, aby byly dodržovány zásady ochrany soukromí a ochrany osobních údajů. Návrh zákona také stanoví, že všechna AI musí být schválena a certifikována před použitím. Tato certifikace by měla být provedena v souladu s příslušnými regulačními předpisy. Návrh zákona také stanoví, že v případě porušení předpisů mohou být uděleny sankce až do výše 500 000 šekelů. Tento návrh zákona byl navržen s cílem poskytnout jasný právní rámec pro implementaci AI v Izraeli. A současně se připravují pravidla pro vývoj umělé inteligence, návrh je k dispozici z listopadu 2022.²⁰

V **Britském království** je připravena a schválena strategie „*Umělá inteligence pro národní prosperitu*“, kterou vypracovalo ministerstvo dopravy v září 2020. Strategie je založena na třech pilířích: podpoře rozvoje AI, zajištění jejího správného nasazení a posílení důvěry veřejnosti v AI.

Jedním z hlavních cílů je přijetí jasného regulačního rámce pro AI, který poskytne jasný právní rámec pro AI a stanoví etické standardy. Strategie také stanoví pravidla pro posuzování AI a stanoví zásady pro zajištění ochrany soukromí a osobních údajů. Kromě toho se v strategii vyzývá, aby se vyvinuly nástroje pro monitoring, kontrolu a správu AI.²¹

V **Severní Koreji** nejsou žádné veřejně dostupné právní úpravy umělé inteligence. Nicméně, v září 2019 se objevily zprávy, že severokorejská vláda zřídila první AI laboratoř v Pyongyangu.

20 Gov.il: oficiální informační portál izraelské vlády. *For the first time in Israel. The principles of the policy for the responsible development of the field of artificial intelligence were published for public comment* [online]. 17.11.2022. [cit. 8.2.2023]. Dostupné z: <https://www.gov.il/en/departments/news/most-news20221117>

21 *Assets.publishing.service.gov.uk: oficiální informační úložiště britské vlády. National AI Strategy* [online]. 09.2021. [cit. 08.02.2023]. Dostupné z: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwj46eyif38AhXplYsKHTNFaO0QFnoECAwQAQ&url=https%3A%2F%2Fassets.publishing.service.gov.uk%2Fgovernment%2Fuploads%2Fsystem%2Fuploads%2Fattachment_data%2Ffile%2F1020403%2FNational_AI_Strategy__mobile_version_.pdf&usq=AOvVaw0oHJzJcYsiGgkWE5jE5_66

2.3 KYBERNETICKÁ BEZPEČNOST A KYBERNETICKÝ PROSTOR

Kybernetická bezpečnost může být definována několika různými způsoby. Například Microsoft definuje kybernetickou bezpečnost jako sadu procesů, osvědčených postupů a technologických řešení, které zvyšují ochranu vašich kritických systémů a dat před neoprávněným přístupem.²²

Vláda ČR definuje kybernetickou bezpečnost jako celkovou ochranu sítí před kybernetickými útoky a hrozbami, aby byla zachována bezpečnost informací.²³ Další definice kybernetické bezpečnosti zahrnují například postup obrany počítačů, serverů, mobilních zařízení, elektronických systémů, programů, sítí a dat před škodlivými útoky, poškozením nebo neoprávněným přístupem. Kybernetická bezpečnost je také známá jako informační bezpečnost a je uplatňována jak u počítačů, tak i sítí. Cílem informační bezpečnosti je ochrana informací a majetku před krádeží, korupcí nebo přírodní katastrofou, anebo ochranu digitálních informací, zařízení a aktiv. To zahrnuje osobní údaje, účty, soubory, fotky i peníze. Zkratka „CIA” se často používá k reprezentaci tří pilířů kybernetické bezpečnosti: důvěrnost, integrita a dostupnost.²⁴

S umělou inteligencí úzce souvisí také prostor, v němž se využívá a nachází. Podle využití umělé inteligence můžeme prostor rozdělit na tzv. virtuální (internetový, digitální, kybernetický) a fyzický (využití robotických součástí v průmyslu i jinde, dronů a jiných mechanických přístrojů s umělou inteligencí).

Jde nejčastěji o internetové prostředí, které je velmi variabilní, jeho smysl a přístup se mění denně a všichni dotčení účastníci jsou nuceni na tyto změny odpovídat včas a adekvátně. Informační a komunikační technologie jsou rozšířeny ve společnosti, od úrovně jednotlivců až po mezinárodní rovinu. Jeden

22 Microsoft.com: oficiální informační portál. *What-is-cybersecurity* [online]. [cit. 19.04.2023]. Dostupné z: <https://www.microsoft.com/cs-cz/security/business/security-101/what-is-cybersecurity>

23 Vlada.cz: oficiální informační portál české vlády. *Kybernetická bezpečnost* [online]. 06.12.2021. [cit. 19.04.2023]. Dostupné z: <https://www.vlada.cz/cz/evropske-zalezitosti/umela-intelligence/kyberneticka-bezpecnost/kyberneticka-bezpecnost-192766/>

24 HNÍK, Václav. *Manažerská informatika*. [online]. Praha: Policejní akademie České republiky v Praze. 2022. ISBN: 974-80-7251-530-1. [cit. 31.5.2023] Dostupné z <https://katalog.polac.cz/Record/POLAC.119852>

z významných trendů je vývoj v oblasti operačních technologií, který je těsně spojen s průmyslovou částí. Dle Výkladového slovníku kybernetické bezpečnosti je kybernetický prostor:

*„Digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, službami a sítěmi elektronických komunikací“.*²⁵

Tato základní definice není dostatečná pro úplné pochopení tématu. Poprvé byl pojem „cyberspace“ použit v povídce „*Jak vypálit Chrom*“ od Williamem Gibsonem v roce 1982. Gibson ve svém románu *Neuromancer* charakterizoval kyberprostor jako virtuální prostor, ve kterém interagují komunity, kde jsou shromažďovány a vyhledávány data a informace.²⁶

Do obecného povědomí se ale pojem kyberprostor začíná dostávat až po vydání deklarace Johna Barlowa (zakladatele Electronic Frontier Foundation) „*A Declaration of the Independence of Cyberspace*“. Čeští autoři Kolouch a kolektiv rozvádějí definici a deklarují, že „*Kyberprostor je tvořen prvky informačních a komunikačních technologií, které vytvářejí pomocí protokolu TCP/IP celosvětovou, globální počítačovou síť, a jednotlivými počítačovými systémy, které jsou do této sítě připojeny a které v ní interagují. Vlastní interakce uvedených systémů samozřejmě není možná bez zásahu jednotlivých uživatelů (administrátorů či koncových uživatelů)*“.²⁷

Autoři tu popisují základní vlastnosti kyberprostoru – jako je decentralizace, globálnost, otevřenost, hojnost informací a interaktivita. Zároveň dělí kyberprostor na tři úrovně (fyzickou, logickou a sociální). Fyzická úroveň zahrnuje komponenty sítě, jako jsou kabely, řídicí prvky a další zařízení. Logická úroveň se skládá ze síťových propojení mezi uzly, které jsou realizovány pomocí síťových komunikačních protokolů. Sociální úroveň je zastoupena kyberosobnostmi, které

25 JIRÁSEK, Petr., Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. Policejní akademie ČR v Praze a Česká pobočka AFCEA, Praha, 2014, s.59. ISBN 978–80–7251–397–0

26 KOLOUCH, Jan., Pavel BAŠTA a kol. *CYBERSECURITY* [online]. Praha: CZ.NIC, 2019. [cit. 26.2.2023]. s.35 ISBN: 978–80–88168–34–8. Dostupné z: <https://knihy.nic.cz/files/edice/cybersecurity.pdf>

27 KOLOUCH, Jan., Pavel BAŠTA a kol. *CYBERSECURITY* [online]. Praha: CZ.NIC, 2019. [cit. 26.2.2023]. s.36 ISBN: 978–80–88168–34–8. Dostupné z: <https://knihy.nic.cz/files/edice/cybersecurity.pdf>

jsou v podstatě identifikaci osob v síti (e–mailová adresa, IP adresa apod.). Kyberosobnost může být v reálném světě odlišná od skutečné osoby.²⁸

2.4 KYBERNETICKÉ HROZBY UMĚLÉ INTELIGENCE

Bezpečností hrozby umělé inteligence souvisí v současnosti právě hlavně s prostředím internetu a tzv. kyberprostorem. Malware (neboli škodlivý software) je jednou z mnoha bezpečnostních kybernetických hrozeb v tomto prostoru, se kterou se setkáváme denně.

V minulosti byly hrozby pouze na regionální/individuální úrovni, protože od počátku k inteligentním technologiím měli přístup jen vědci a pravděpodobnost zneužití byla nízká, neboť většinu vývoje tehdy financovala armáda. Od té doby si informační technologie, a s tím spojené hrozby, prošly celou řadou obměn a dnes má kybernetická bezpečnost nezastupitelnou roli při udržení vnitřní bezpečnosti a veřejného pořádku na území státu i v globálním měřítku. Změny se týkají jak samotných typů hrozeb, tak i změn v rozsahu závažnosti, práva, tak i změn, týkající se zabezpečení. Kybernetická bezpečnost je rovněž důležitou složkou Auditů národní bezpečnosti z roku 2016. Bohužel ne na všechny hrozby je možné se zavčasu přichystat, obzvláště pokud je útočníkem osoba či sdružení mající velkou pravomoc, a proto je velký nátlak na posílení členů na úřadech veřejné správy či v komerčním prostředí v rámci IT oborů. V roce 2023 se jedná především o posílení členů administrátorů, správců sítě, či bezpečnostních expertů v rámci informačních technologií. Naštěstí se ukázalo, že malware efektivně tento model nemůže moc dobře vytvořit, protože chápe jazyk, ale ne programování a zatím nemá dostatek zkušeností jako například ChatGPT podle modelu GPT 3.5.²⁹

28 KOLOUCH, Jan., Pavel BAŠTA a kol. *CYBERSECURITY* [online]. Praha: CZ.NIC, 2019. [cit. 26.2.2023]. ISBN: 978–80–88168–34–8. Dostupné z:

<https://knihy.nic.cz/files/edice/cybersecurity.pdf>

29 *Youtube.com: oficiální informační portál společnosti Youtube* © 2023 Google LLC.

HUTCHINS. Marcus. *Can ChatGPT Write Malware Better Than Me* [online] 22.01.2023. [cit. 8.2.2023]. Dostupné z: https://www.youtube.com/watch?v=L9w_k2ypRr0

Mnohem horším způsobem jsou pak kombinace několika těchto kybernetických útoků zároveň. K takovýmto útokům také čas od času dochází a jejich dosah bývá mnohonásobně horší.

DoS (Denial of Service) je napadení určitých služeb například mail, webové stránky apod. tak, že jejich servery se zahltní a služby přestanou fungovat.

DDoS: „(Distributed Denial of Service) Útoky na webové stránky, e-mail a další počítačové služby jsou stále běžné. Toto jméno je identifikátorem útoku, kdy nejde o odstranění webové stránky nebo internetové služby, ale hlavním cílem je odstranit je. V tomto případě by se například mohlo jednat o pokus zahltnit určité servery zbytečnými požadavky a informacemi, přetížit daný systém a učinit jej nedostupným uživatelům pro normální použití. Tomuto útoku lze zabránit například nastavením firewallu, který může blokovat činnost hackerů, problém je, že to lze provést pouze hromadně, což znamená, že i legitimní uživatelé budou mít možnost publikovat. DoS zahrnuje účast tisíců počítačů na internetu, na nichž je potřeba nainstalovat DoS software. Tento software lze nainstalovat i bez povolení uživatelů.“³⁰ ³¹ To se může stát, když je například server předimenzovaný, takže nemá čas správně zpracovávat požadavky od více uživatelů, kteří využívají služeb webu či procesu a v důsledku toho přestane správně fungovat systém. Příkladem může být podcenění počtu studentů zapsaných do kurzu na univerzitách.

Umělá inteligence se často spoléhá na softwarové ovladače k tomu, aby ovládala hardware a obešla operační systém. Pokud je však útok proveden prostřednictvím těchto programů, je nesmírně obtížné, aby ho antivirový software odhalil, zvláště pokud je program dobře zašifrován a vypadá jako oficiální aktualizace.

30 It-slovník.cz: slovník IT pojmů [online]. [cit. 3.2.2023]. Dostupné z: <https://it-slovník.cz/pojem/ddos-utok>

31 Wikipedia.org: informační portál o všech věcech [online]. [cit. 3.2.2023]. Dostupné z: https://cs.wikipedia.org/wiki/Denial_of_service

2.5 KYBERTERORISMUS A UMĚLÁ INTELIGENCE

Kyberterorismus je označení pro zločiny, které jsou spáchány za pomoci počítačů a sítí. Tyto zločiny mohou zahrnovat šíření virů, útoky DoS, krádeže osobních údajů, finanční podvody a podobně.

Umělá inteligence se může použít k rozšíření rozsahu a dopadu kyberterorismu. Také může být použita například k vytváření složitých útoků, které dokážou překonat tradiční bezpečnostní opatření nebo k rozpoznávání zranitelností a zneužívání dat, což opětovně může vést k rychlejšímu a účinnějšímu kyberterorismu.

Pokračování ve vývoji umělé inteligence může znamenat, že kyberteroristé budou schopni vytvářet stále sofistikovanější útoky, které budou mnohem obtížnější zastavit, což prakticky znamená nutnost vytvořit obrannou umělou inteligenci.

Již nyní se umělá inteligence může využívat a také jistě využívá k rozpoznávání hrozeb napadení v antivirových systémech, k rozpoznávání podvodných transakcí apod.

2.5.1 POTENCIÁLNÍ CÍLE KYBERTERORISMU

Potenciální cíle kyberterorismu jsou cíle, jež se týkají různých oblastí, jako je finanční sektor, infrastruktura, komunikace, doprava, průmysl, vláda a občanská společnost (měkké cíle). Tyto cíle se úzce vážou k umělé inteligenci (AI), protože AI je schopna vytvářet systémy, které jsou schopny vyhodnocovat velké objemy dat a provádět přesné rozhodnutí rychleji než člověk. To umožňuje kyberteroristům získat přístup k informacím, které by normálně nebyly dostupné, a mohou tak poškodit systémy vybavené AI.

Některé z potenciálních cílů kyberterorismu s umělou inteligencí jsou následující.

Použití umělé inteligence k útokům na **kritickou infrastrukturu**. Kyberteroristé mohou použít umělou inteligenci k útokům na kritickou infrastrukturu jako jsou energetické, dopravní, finanční, vládní a průmyslové systémy. Tato kritická infrastruktura je zranitelná vůči útokům umělé inteligence, protože tyto systémy jsou otevřené, a pokud jsou přístupné internetu, jsou snadno

napadnutelné. Kyberteroristické útoky umělé inteligence na kritickou infrastrukturu mohou mít devastující důsledky, jako je úplná ztráta dat a systémů, narušení fungování kritických infrastrukturních systémů (např přerušení dodávek elektrické energie, dopravy apod.) a vyvolání finančních ztrát.

Použití umělé inteligence k **ovládnutí a ovládání počítačových sítí**. Toto je také závažné bezpečnostní riziko. Může zde dojít k převzetí kontroly nad počítačovými sítěmi, například k ovládnutí bezdrátových sítí nebo k ovládání počítačových sítí. Tato technologie může být použita k získání nebo k odcizení citlivých informací, jako jsou například finanční údaje nebo státní tajemství.

Použití umělé inteligence k útokům na **kritické informační systémy**. Kyberteroristé mohou použít umělou inteligenci k útokům na kritické informační systémy. Tyto systémy mohou být použity k získávání citlivých informací nebo k odcizení informací, které jsou nezbytné pro fungování organizace.

Použití umělé inteligence k **šíření propagandy a dezinformací**. Kyberteroristé mohou použít umělou inteligenci k šíření propagandy a dezinformací. Tato technologie může být použita k ovlivňování veřejného mínění a získávání politických nebo ekonomických výhod.

Použití umělé inteligence k **útokům na sociální sítě**. Kyberteroristé mohou použít umělou inteligenci k útokům na sociální sítě. Tato technologie může být použita k získávání citlivých informací o uživateli a k šíření dezinformací.

2.5.2 INSTITUTE, KTERÉ BY SE MĚLY ZABÝVAT BEZPEČNOSTÍ A UMĚLOU INTELIGENCÍ

V této kapitole budu popisovat instituce zabývající se kybernetickou bezpečností a umělou inteligencí. Popíšu zde podle mého názoru jenom ty největší a nejdůležitější například NÚKIB aj.

CENTRUM PROTI HYBRIDNÍM HROZBÁM VNITŘNÍ BEZPEČNOSTI MINISTERSTVA VNITRA

Dříve Středisko pro boj s terorismem a hybridními hrozbami Ministerstva vnitra (dále jen CTHH Ministerstva vnitra) je jednou ze tří agentur kybernetické bezpečnosti v ČR, pokud vyloučíme bezpečnostní služby a instituce Nato. Jde

o útvar Ministerstva vnitra s vnitřní působností (na území celé ČR). CTHH MV se ve své práci řídí celou řadou bývalých českých státních informačních a bezpečnostních úřadů a služeb i bezpečnostních společností ve stejném oboru činnosti. Sestavením dvacetičlenného týmu byla pověřena právnička ministerstva vnitra Eva Romancová.³²

Ministr vnitra Milan Chovanec na jaře 2016 na základě auditu národní bezpečnosti doporučujícího implementaci na všech obdobných pracovištích a v souladu s českou bezpečnostní strategií z roku 2015 rozhodl o zřízení ústředního orgánu, který zahájil činnost dne 1. ledna 2017.

S účinností od 1. července 2022 byl z Centra vyčleněn Program boje proti terorismu a Centrum se zaměřuje výhradně na smíšené hrozby pro vnitřní bezpečnost.³³

Centrum proti hybridním hrozbám vnitřní bezpečnosti sice na svých webovkách a dokumentech neuvádí, že pracuje s bezpečnostními aspekty umělé inteligence, avšak umělá inteligence je součástí hrozeb v kyberprostoru, což je podmnžinou hybridních hrozeb u nás.

Mezi hlavní bezpečnostní hrozby analyzované MV patří: útoky proti měkkým cílům a bezpečnostní aspekty migrace, extremismus, masové akce, narušování veřejného pořádku, různé trestné činnosti, dezinformační kampaně související s vnitřní bezpečností státu a organizovaná trestná činnost.

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST

Podle etického kodexu, poslání, hodnot, vize a jiných dokumentů Národního úřadu pro kybernetickou bezpečnost a informační bezpečnost (dále jen NÚKIB) se tam přímo nezmiňuje umělá inteligence a její bezpečnostní aspekty,

32 *Wikiwand.com: doplněk pro wikipedii. informační portál o všech věcech* [online]. [cit. 5.2.2023]. Dostupné z:

https://www.wikiwand.com/cs/Centrum_proti_terorismu_a_hybridn%C3%ADm_hrozb%C3%A1m
33 *Mvcr.cz: informační portál Ministerstva vnitra* [online]. [cit. 5.2.2023]. Dostupné z:
<https://www.mvcr.cz/chh/clanek/specialni-dokumenty-faq.aspx>

avšak v jeho zprávách se občas objeví a řeší ji v rámci bezpečnosti a potencionálních útoků případně ve spolupráci s jinými subjekty.³⁴

NÚKIB je jednou ze tří kybernetických regulačních agentur v České republice, s výjimkou bezpečnostních složek. Je národním orgánem s působností na celém území českého státu. Stejně jako jiné úřady i NÚKIB spolupracuje s dalšími bezpečnostními složkami, službami a agenturami se stejnou oblastí působnosti. NÚKIB se 120 zaměstnanci zahájil své funkční období 1. srpna 2017 a převzal část agendy dříve pod správou správy Národního centra kybernetické bezpečnosti působícího od roku 2011. V rámci této instituce funguje výkonná divize NÚKIB se specializací na kybernetickou bezpečnost do roku 2020.³⁵

*„NÚKIB je ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany. Dále má na starosti problematiku neveřejné služby v rámci družicového systému Galileo.“*³⁶

Ředitelem NÚKIB je od 1. července 2022 Lukáš Kintr. Ředitelé tohoto úřadu se pravidelně účastní Bezpečnostní rady státu, kde jsou členy Výboru pro kybernetickou bezpečnost.

Na konci roku 2022 a v roce 2023 se NÚKIB spolupodílí na tvorbě nového zákona o kybernetické bezpečnosti a prováděcích vyhláškách, které mají začít platit od poloviny roku 2024.³⁷

Návrh nové právní úpravy je k dispozici široké veřejnosti na webových stránkách nis2.nukib.cz do 26. února 2023. Jde o zapojení odborné veřejnosti ještě před definitivní tvorbou nového zákona.

34 *Nukib.cz: informační portál Národního řádu kybernetické bezpečnosti* [online]. [cit. 31.5.2023]. Dostupné z: <https://www.nukib.cz/cs/o-nukib/o-uradu/>

35 *Wikiwand.com: doplněk pro wikipedii. informační portál o všech věcech* [online]. [cit. 5.2.2023]. Dostupné z: <https://www.wikiwand.com/cs/N%C3%A1rodn%C3%AD%20%C3%BA%C5%99ad%20pro%20kybernetickou%20a%20informa%C4%8Dn%C3%AD%20bezpe%C4%8Dnost>

36 *Nukib.cz: informační portál Národního řádu kybernetické bezpečnosti* [online]. [cit. 5.2.2023]. Dostupné z: <https://www.nukib.cz/>

37 *Osveta.nukib.cz: edukační portál Nukibu* [online]. [cit. 1.2.2023]. Dostupné z: <https://osveta.nukib.cz/course/view.php?id=145#section-3>

SDRUŽENÍ CZ.NIC

„Zájmové sdružení právnických osob CZ.NIC bylo založeno předními poskytovateli internetových služeb v roce 1998 a nyní má již 116 členů. Hlavními činnostmi sdružení jsou provozování registru jmen domén registrovaných pod doménou CZ, zabezpečování provozu domény nejvyšší úrovně .CZ a osvěta v oblasti jmen domén. V současné době se sdružení intenzivně věnuje rozšiřování technologie DNSSEC a služby mojID, rozvoji systému správy domén a podpoře nových technologií a projektů prospěšných pro internetovou infrastrukturu v České republice. Sdružení provozuje také interní bezpečnostní tým CZ.NIC–CSIRT a od roku 2011 Národní CSIRT tým České republiky – CSIRT.CZ. V roce 2013 stál CZ.NIC u vzniku bezpečnostního projektu FENIX. CZ.NIC je členem sdružení EURid. spravujícího evropskou doménu EU a dalších obdobně zaměřených mezinárodních společností (CENTR, ccNSO a jiné).“³⁸

V oficiálních dokumentech se sdružení nezmiňuje o umělé inteligenci, nicméně se stará o bezpečnost aplikací eGovernmentu a ochraně infrastruktury a také pomáhá policii. V rámci těchto aktivit nepřímo řeší umělou inteligenci a možné zneužití.

Sdružení pomáhá s osvětou, má širokou spolupráci se školami, pracuje na aplikacích eGovernmentu a stará se o národní CSIRT tým. Rovněž se stará o nové technologie DNSSEC a IPv6 a jiné podle jeho programového období 2020–2024.³⁹

POLICIE ČR A ZPRAVODAJSKÉ SLUŽBY

Řešení kyberkriminality u jednotlivých občanů České republiky má na starosti Policie ČR. Do 23.5.2018 existovala na webových stránkách policie hotline linka pro hlášení kyberkriminality. Policie úzce spolupracuje s cz.nic na řešení těchto problémů.⁴⁰ Aktuálně je zapojena do kampaně Nepindej v Karlovarském kraji, která začala v druhé půlce roku 2022 na osvětu veřejnosti proti

38 Nic.cz: informační portál sdružení CZ.NIC [online]. [cit. 5.2.2023]. Dostupné z: <https://www.nic.cz/page/351/>

39 Nic.cz: informační portál sdružení CZ.NIC [online]. [cit. 31.5.2023]. Dostupné z: https://www.nic.cz/files/nic/doc/Koncepce_CZNIC_2020-2024.pdf

40 Policie.cz: informační portál policie ČR [online]. [cit. 5.2.2023]. Dostupné z: <https://www.policie.cz/clanek/ukonceni-provozu-hotline.aspx>

kyberútokům.⁴¹ A dohledává a řeší i válečné zločiny na Ukrajině v rámci univerzální jurisdikce.

Podle různých zpráv včetně těch výročních se policie, vojenské a nevojenské instituce jenom okrajově zabývají umělou inteligencí, i když stále častěji řeší situace způsobené jejím zneužitím například dezinformační kampaně a jiné útoky v kyberprostoru.⁴²

V případě hackingu se neoprávněný přístup k počítačovým systémům a nosičům informací obvykle řeší podle § 230 trestního zákoníku, což je trestný čin, který lze použít pro většinu úkonů, tzv. hacking, narušení dat, narušení systému a v neposlední řadě přinejmenším zneužití zařízení. Nejvýraznějším zkoumaným příkladem je chování pachatele, který obchází zabezpečení počítačového systému a přistupuje k datům oběti, v čemž může libovolně pokračovat. Součástí těchto jednání bylo mimo jiné šíření škodlivého kódu, zřízení tzv. zadní vrátka pro volně dostupný software atd. Stále častější praxí je nabourávání se do e-mailových účtů, účtů sociálních sítí, účtů online bankovníctví, což vede k narušení soukromí, získávání citlivých informací s potenciálem je poškodit nebo zničit nebo získat finanční prospěch. To zahrnuje i další následné trestné činnosti (vydírání, zlomyslné obtěžování, krádeže účtů, podvody). K tomuto druhu trestné činnosti patří také kybernetické útoky (např. DDoS) nebo vydírání prostřednictvím ransomware.

Další možná forma porušení důvěrnosti zpráv přenášených podle § 182 trestního zákoníku, jejímž nejčastějším projevem je tzv. sniffing, při kterém autor zachycuje probíhající komunikaci mimo síť a získává tak citlivá data. nejen z hlediska návštěvnosti, ale i obsahu. To se často stává u nezabezpečených Wi-Fi připojení, na straně poštovního serveru, s nimiž je manipulováno, a v poslední době kvůli útokům na domácí router. Zločinci pak získají přístup k citlivým údajům, jako jsou hesla, platební údaje nebo citlivý osobní či soukromý obsah, které pak používají k nátlaku na oběti za účelem jejich finančního zisku nebo alespoň

41 *Policie.cz: informační portál policie ČR* [online]. [cit. 5.2.2023]. Dostupné z: <https://www.policie.cz/clanek/kyber-kampan-nepindej.aspx>

42 *Bis.cz: informační portál bezpečnostní informační služby* [online]. [cit. 31.5.2023]. Dostupné z: <https://www.bis.cz/public/site/bis.cz/content/vyrocní-zpravy/2021-vz-cz-2.pdf>

k poškození pověsti oběti. Policie řeší také podvodné blogy, e-shopy, klamavé jednání, porušování etiky a pirátství.⁴³

Policie ČR využívá umělou inteligenci k řešení různých úkolů, jako je identifikace pachatelů, vyšetřování zločinů a poskytování informací o zločincích. Umělá inteligence jim poskytuje možnost vyhodnocovat obrovské množství dat, které by jinak bylo nemožné analyzovat. Například ta využívá algoritmy strojového učení k vyhodnocování obrazových dat a hlasových nahrávek, aby identifikovala podezřelé osoby.

Umělá inteligence také umožňuje policii vybírat z velkého množství dat potenciální pachatele. Vyhodnocování dat může být provedeno rychleji a efektivněji než rutinní postupy vyšetřování. To umožňuje policii lépe cílit svá vyšetřování.

Policie ČR dále využívá umělou inteligenci k ochraně občanů před útoky. Využívá například policie algoritmy strojového učení k vyhodnocování dat o útocích, aby identifikovala útočníky a zjistila, jaká míra ochrany je potřebná.

Z předchozího textu vyplývá, že je možné se chránit je možné se chránit proti útokům pomocí několika jednoduchých opatření. Patří mezi ně používání silných hesel, aktualizování softwaru a dodržování bezpečnostních pravidel. Navíc by měli občané vždy dbát na to, aby informace, které sdílejí na internetu, byly důvěryhodné.

Nevojenská zpravodajská služba na území České republiky, která má za cíl chránit občany České republiky od nejrůznějších forem terorismu a zároveň chránit stát před působením cizích špiónážních služeb je Bezpečnostní informační služba (BIS). Tato služba je kontrolována vládou České republiky. Úkoly zadává prezident a vláda. Informace a metody práce jsou v utajeném režimu neveřejné. BIS vznikla v 30.7.1994.

Vojenské zpravodajské služby se zabývají vojenskými informacemi, obranyschopností, zbrojním průmyslem, podporou bojových operací. V rámci své

⁴³ *Policie.cz: informační portál policie ČR* [online]. [cit. 5.2.2023]. Dostupné z: <https://www.policie.cz/clanek/kyberkriminalita.aspx>

činnosti řeší také kybernetickou bezpečnost. Vojenské zpravodajství vzniklo 1.1.2005 a spadá pod Ministerstvo obrany ČR.

NATO CCD COE

NATO vytvořilo „*Středisko pro spolupráci v kybernetické obraně*“,⁴⁴ kde se snaží v rámci kyberbezpečnosti vyvinout a zavést mezinárodní standardy pro obranu proti útokům na kybernetickou infrastrukturu. Centrum pro výzkum excellence také zajišťuje vzdělávání, výzkum a poradenství v oblasti kybernetické bezpečnosti a jeho členové se účastní mezinárodních aktivit zaměřených na zvyšování úrovně kybernetické bezpečnosti. Centrum také provádí mezinárodní analýzy rizik a poskytuje podporu v boji proti útokům na kybernetickou infrastrukturu. Na obrázku 1⁴⁵ pod tímto textem bude vidět přehled aktuálních všech center excellence NATO.



Obrázek 1 Centra NATO Excellence

44 JIRÁSEK, Petr., Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. Policejní akademie ČR v Praze a Česká pobočka AFCEA, Praha, 2014, s.63. ISBN 978–80–7251–397–0.

45 Obrázek 1 převzat z: *Nato centra Excellence* [online]. [cit. 5.2.2023]. Dostupné z: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/12/pdf/221202-coe-map.pdf

Toto centrum sídlí v Estonsku ve městě Tallinn. Aktuálně (2023) má 28 členských států a z mnoha významných věcí, kterou publikovalo, je například Tallinnský Manuál 2.0, který popisuje, jak aplikovat mezinárodní právo v rámci kyberprostoru.⁴⁶

Další úřad, který je součástí této soustavy institucí a pomáhá je spojovat je „Úřad NATO pro správu kybernetické obrany, jehož smyslem je zastřešovat a propojovat existující schopnosti kybernetické obrany v rámci Aliance.“⁴⁷

Rovněž nemůžeme zapomenout na NATO CIRC – Technické centrum „Centrum technické podpory NATO CIRC – druhá úroveň. Zajišťuje schopnost reakce na incidenty, sledování incidentů, obnovení systémů a poskytuje přímou technickou podporu a pomoc provoznímu a bezpečnostnímu managementu provozovaných informačních systémů NATO.“⁴⁸ Česká republika se aktivně zúčastňuje cvičení NATO na obranu kyberprostoru a v roce 2022 jsme se umístili pátí a v roce 2021 třetí, máme trochu zhoršující se tendenci.⁴⁹

Tato síť institucí NATO se ve svých zprávách okrajově zmiňuje o umělé inteligenci, řeší ji spíše nepřímo v rámci jiných bezpečnostních incidentů, přestože zmínky o umělé inteligenci a jejích bezpečnostních aspektech se neustále zvyšují.

46 Ccdcoe.org: informační portál CCD COE [online]. [cit. 5.2.2023]. Dostupné z: <https://ccdcoe.org/about-us/>

47 JIRÁSEK, Petr., Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. Policejní akademie ČR v Praze a Česká pobočka AFCEA, Praha, 2014, s.63. ISBN 978–80–7251–397–0.

48 JIRÁSEK, Petr., Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. Policejní akademie ČR v Praze a Česká pobočka AFCEA, Praha, 2014, s.63. ISBN 978–80–7251–397–0.

49 Lupa.cz: informační portál o informačních novinkách a softwaru, SEDLÁK, Jan. *Locked Shields 2022: Česko opět uspělo na kybercvičení NATO, ale pohoršilo si* [online]. 25. 4. 2022. [online]. [cit. 5.2.2023]. Dostupné z: <https://www.lupa.cz/aktuality/locked-shields-2022-cesko-opet-uspelo-na-kybercviceni-nato-ale-pohorsilo-si/>

3. PRAKTICKÁ ČÁST

V této velké kapitole popíšu a budu analyzovat vybrané bezpečnostní situace jako jsou umělá inteligence v Číně, umělá inteligence v automobilovém průmyslu a umělá inteligence v digitálním umění. Z mého pohledu jsou tyto oblasti aktuálně nejvíce v popředí řešení z pohledu bezpečnostních aspektů umělé inteligence.

3.1 UMĚLÁ INTELIGENCE V RŮZNÝCH ODVĚTVÍCH A KRITÉRIA HODNOCENÍ KAUZ S NÍ SPOJENÁ V ROCE 2022/2023

Pro svou diplomovou práci jsem si vybral s bližším popisem mnoho závažných případů či kauz, které se liší svým bezpečnostním potenciálem a schopností ohrožit nás všechny, jež do značné míry přímo či nepřímo ovlivňují náš život. Prvně jmenovaná témata spojená s umělou inteligencí jsou více mediálně známá, co se týče jejich využití. Další jsou méně známá, avšak vzájemně jsou provázána s celosvětovým dosahem. Dále uvedu strukturu, jak budu hodnotit jednotlivé kauzy bezpečnostních aspektů umělé inteligence

OBECE O KAUZE

V této části popisuji, jak se daný případ projevuje, ve které zemi se nachází a propojení s ostatními. Jsou zde také popsána konkrétní data a to, co je o tomto případě známo z médií nebo jiných zdrojů či dokumentů. Zároveň tu stručně uvádím míru rizika daného případu.

VYSVĚTLENÍ TERMÍNŮ DANÉ KAUZY

Každý případ má své charakteristiky a je nutné je pro tyto případy vysvětlit. K tomu slouží tato sekce. Tyto termíny jsou převzaty buď ze slovníku odborných termínů příslušného oddělení nebo z oficiální zprávy příslušné asociace, nadace, organizace, komunity nebo mezinárodní společnosti.

ROZBOR BEZPEČNOSTNÍ SITUACE A RIZIKA

Jak jsem již zmínil v teoretické části, existuje mnoho typů bezpečnostních útoků, rizik či situací. Následně v této části budu v tomto dokumentu podrobně popisovat, o jaká konkrétní bezpečnostní rizika se bude jednat.

VÝSLEDKY A POTENCIONÁLNÍ DOPADY RIZIKA POUŽITÍ UMĚLÉ INTELIGENCE

Každý případ má svůj výsledek. Zde se zabývám zjištěnými dopady každého případu. Dopady mohou být různé povahy, např. sociální, psychologické, finanční, ekonomické nebo mohou způsobit omezené fyzické škody. Nejčastějším dopadem ve zmíněných případech je zhoršení ekonomické situace nebo ztráta dat. Jednotlivé případy trvají dodnes a rozsah je většinou mezinárodní.

MOŽNOSTI ŘEŠENÍ DANÉ BEZPEČNOSTNÍ SITUACE

V této části popíšu možné způsoby daných situací z mého pohledu. Zde uvedu možná řešení v podobných situacích, pokud jsem je našel z jiných zdrojů.

Obecná řešení jsou většinou snažit se předejít situacím ohrožujícím bezpečnost, například prostřednictvím vzdělávacích programů, implementací bezpečnostních pravidel a postupů nebo poskytováním odborných poradenských služeb. Dále potom je to použití technického vybavení a technologií, jako jsou kamerové systémy, zabezpečení proti krádežím a ochrana osobních údajů, aby se zabránilo nebo omezilo riziko útoku nebo zneužití.

3.2 VYBRANÉ PŘÍPADY A BEZPEČNOSTNÍ SITUACE SPOJENÉ S UMĚLOU INTELIGENCÍ

V této kapitole budu popisovat a analyzovat vybrané bezpečnostní situace spojené s umělou inteligencí.

3.2.1 UMĚLÁ INTELIGENCE V ČÍNĚ A JEJÍ BEZPEČNOSTNÍ HROZBA

V této části chci popisovat a analyzovat podle mého dlouhodobou bezpečnostní hrozbu pro náš stát.

OBEČNĚ O KAUZE

Historie umělé inteligence v Číně je dlouhá a pestrá. Již v roce 1956 byl založen první výzkumný ústav umělé inteligence v Číně na Pekingské univerzitě. V roce 1983 byl spuštěn první národní projekt umělé inteligence v Číně s názvem „*Výzkum a aplikace expertních systémů*“, dále potom v roce 1999 byla založena Čínská asociace pro umělou inteligenci (CAAI), která je největší profesní organizací v oboru umělé inteligence v Číně a samozřejmě v roce 2017 byla přijata „*Nová generace plánu rozvoje umělé inteligence*“, která stanovila cíle a strategie pro posílení postavení Číny jako světového lídra v oblasti umělé inteligence do roku 2030.⁵⁰

Umělá inteligence v Číně se aplikuje v mnoha oblastech, jako je např. medicína, kde umělá inteligence pomáhá s diagnostikou, léčbou, prevencí a výzkumem nemocí. Dále v oblasti bezpečnosti umělá inteligence umožňuje rozpoznávání obličejů, hlasů a gest pro monitorování a kontrolu obyvatel. Ve vzdělání umělá inteligence podporuje personalizované učení, hodnocení a zpětnou vazbu pro studenty. V průmyslu umělá inteligence optimalizuje výrobu, logistiku, řízení kvality a údržbu zařízení.

Čína hraje zásadní roli v oblasti umělé inteligence (AI). Je zde vyvinuta řada aplikací AI v oblastech jako jsou finance, zdravotnictví, doprava a technologie. Čína je díky svému silnému průmyslu a rozvinutým městským oblastem výhodnou pozicí pro výzkum a vývoj AI.

V oblasti financí je Čína ve vrcholných pozicích AI. Například jedna z předních čínských bank, China Construction Bank (CCB), využívá AI pro

⁵⁰Wikipedia.org: informační portál o všech věcech. *Artificial intelligence* [online]. [cit. 26.2.2023]. Dostupné z: https://en.wikipedia.org/wiki/Artificial_intelligence

automatizaci procesů a pro předvídání potřeb klientů. CCB také vyvinula AI–řízeného robota, který pomáhá klientům se zpracováním úvěrů.

V oblasti zdravotnictví je Čína známá svými pokročilými AI–řízenými systémy. Například AI–řízený systém vyvinutý společností Tencent pro lidskou diagnostiku je schopen přesně diagnostikovat nemoci, jako je rakovina, pomocí AI. Systém byl úspěšně používán pro diagnostiku pacientů v Číně.

V oblasti dopravy je Čína velmi aktivní. AI jsou využívány k řízení řídicích systémů, optimalizaci dopravního plánování a řízení dopravy. Například čínská automobilka Geely využívá AI k řízení dopravy ve svých městských oblastech.

Čína je také v čele světového vývoje AI technologií. Společnosti jako Baidu, Tencent a Alibaba vyvíjejí AI–řízené technologie pro několik účelů. Například společnost Baidu vyvíjí AI–řízenou platformu, která pomáhá spotřebitelům a podnikům s využíváním AI technologií.

AI je v Číně aktivně využívána v oblastech jako financování, zdravotnictví, doprava a technologie. AI se stává stále důležitějším nástrojem pro čínské spotřebitele a podniky, a Čína je jednou z největších výrobců AI technologií na světě.

Například čínská společnost Baidu plánuje v březnu 2023 představit alternativu chatbota ChatGPT s názvem Ernie Bot. Popularita ChatGPT podporovaného Microsoftem raketově stoupá díky jeho schopnosti chatovat s lidskými hlasy, generovat text od poezie a esejů až po obchodní smlouvy nebo pomáhat s jednoduchým řízeným programováním. ChatGPT ale není oficiálně dostupný v Číně, přestože je tam o něho velký zájem.

Nebo startup databázového softwaru PingCap již má na trhu produkt založený na ChatGPT. Umožňuje zákazníkům analyzovat provozní data jejich společnosti, jako jsou nejprodávanější modely automobilů, během několika sekund, aniž by museli znát počítačový programovací jazyk.⁵¹

51 Novinky.cz: *informační portál mediální společnosti. Baidu ukáže příští měsíc vlastního chatovacího robota* [online]. 23.2.2023. [cit. 23.2.2023]. Dostupné z: <https://www.novinky.cz/clanek/internet-a-pc-baidu-ukaze-pristi-mesic-vlastniho-chatovaciho-robota-40423800>

VYSVĚTLENÍ TERMÍNŮ DANÉ KAUZY

Superintelligence je entita, která předčí lidi celkovou inteligencí nebo nějakou konkrétní mírou inteligence.⁵² Umělá inteligence (AI) se vztahuje k počítačovým systémům, které jsou schopny řešit problémy, dokončovat úkoly a napodobovat lidské kognitivní schopnosti. Existují různé typy AI, včetně umělé úzké inteligence (ANI), která má úzký rozsah schopností; umělé obecné inteligence (AGI), která je na úrovni lidských schopností; nebo umělé superintelligence (ASI), která je schopnější než člověk.

Umělá superintelligence (ASI) překračuje lidskou úroveň inteligence a překonává kognitivní schopnosti lidí. To znamená, že ASI by mohla být schopna vyřešit problémy a dokončit úkoly, které jsou pro člověka nemožné nebo velmi obtížné.

Poslání čínské společnosti Baidu je zjednodušit komplikovaný svět pomocí technologií. Společnost byla založena v roce 2000 jako platforma pro vyhledávače a v roce 2010 byli prvním uživatelem umělé inteligence, aby usnadnili vyhledávání obsahu na internetu. K vývoji nových obchodů s umělou inteligencí také použili „*Baidu Brain*“, jejich hlavní technologický motor AI.

Dnes je Baidu již přední společností v oblasti umělé inteligence se silným internetovým portfoliem. Je jednou ze společností na světě, která nabízí kompletní sadu AI zahrnující infrastrukturu sestávající z čipů AI. Tyto součásti zabezpečují rámce hlubokého učení, základních funkcí AI, jako je zpracování přirozeného jazyka, graf znalostí, rozpoznávání řeči, počítačové vidění a rozšířená realita. Svými produkty tato společnost otevírá platformu umělé inteligence pro usnadnění široké aplikace a použití.

Během posledních dvou desetiletí si vybudovali diverzifikované portfolio produktů a služeb s velkými celkovými tržními příležitostmi. K jejich portfoliu produktů a služeb má měsíčně přístup více než jedna miliarda zařízení a jejich podnikání zahrnuje ekosystém stovek milionů uživatelů, milionů vývojářů a stovek tisíc podniků. Jejich vlajkový produkt je Baidu App, což je aplikace na prvním místě

⁵²Merriam-webster.com: *informační vyhledávací portál* [online]. 2023. [cit. 13.7.2023]. Dostupné z: <https://www.merriam-webster.com/dictionary/superintelligence>

pro vyhledávání v Číně. V prosinci 2020 dosáhli 544 milionů MAU (měsíční aktivní uživatelé). Jejich využití silné technologické základny k podpoře obchodního modelu s otevřenou platformou nejen přitahuje více účastníků do jejich ekosystému, ale také jim zpětně dodává bohatství a životaschopnost do jejich ekosystému a celkově posiluje dlouhodobé vyhlídky jejich podnikání.

Baidu se skládá ze dvou segmentů:

- 1) Baidu Core, který tvořil více než 70 % jejich příjmů za poslední tři roky,
- 2) iQIYI, který tvořil jejich zbývající tržby.

Baidu Core, poháněná umělou inteligencí, poskytuje hlavně online marketingové a nemarketingové služby s přidanou hodnotou, stejně jako produkty a služby z nových iniciativ AI, které je společně pohánějí prostřednictvím tří motorů růstu.

Mobile Ecosystem je portfolio více než jednoho tuctu aplikací, včetně Baidu App, Haokan a Baidu Post, které poskytuje otevřenou platformu, která prostřednictvím jejich stavebních bloků umělé inteligence sdružuje širokou škálu obsahu a služeb třetích stran.

AI Cloud je kompletní sada cloudových služeb a řešení, včetně PaaS, SaaS a IaaS, a jedinečně odlišená jejich různými řešeními pomocí systémů AI.

Intelligent Driving & Other Growth Initiatives (OGI) jsou jejich růstové iniciativy, které zahrnují inteligentní řízení (služby pro autonomní řízení, včetně HD map, automatizovaného parkování s obsluhou a autonomního navigačního pilota, inteligentních elektrických vozidel a flotil robotaxi), stejně jako chytrá zařízení Xiaodu poháněná inteligentním asistentem DuerOS a vývojem čipu AI.

Baidu byla kotována na národním trhu NASDAQ (později přejmenovaném na Nasdaq Global Market) v srpnu 2005 a od března 2021 byla duálně kotována na burze cenných papírů Hong Kong Limited (SEHK). Tato společnost se snaží být Googlem Číny.⁵³

Alibaba Group byla založena v roce 1999 18 lidmi pod vedením Jacka Ma, bývalého učitele angličtiny z Hangzhou v Číně. Od počátku sdíleli zakladatelé

⁵³ *Baidu.com: informační vyhledávací portál* [online]. 2023. [cit. 26.2.2023]. Dostupné z: <https://ir.baidu.com/company-overview>

společnosti víru, že internet vyrovná podmínky tím, že umožní malým podnikům využívat inovace a technologie k efektivnějšímu růstu a konkurenceschopnosti v domácích i globálních ekonomikách. Od spuštění své první webové stránky, která pomáhá malým a středním podnikům v Číně prodávat na mezinárodní úrovni, se Alibaba Group rozrostla do digitálního ekosystému s podniky zahrnujícími čínský obchod, mezinárodní obchod, místní spotřebitelské služby, Cainiao, cloud, digitální média, zábavu, inovační iniciativy., a další. Posláním Alibaba Group je, aby bylo snadné podnikat kdekoli. Alibaba se podobá obchodní společnosti Amazon.

Vize Alibaba Group je být dobrou společností, která vydrží 102 let. Představují si, že se jejich zákazníci budou setkávat, pracovat a žít v Alibabě. Jejich vizí pro fiskální rok 2036 je sloužit 2 miliardám globálních spotřebitelů, umožnit 10 milionům podniků být ziskovými a vytvořit 100 milionů pracovních míst.⁵⁴

Společnost Tencent byla založena v roce 1998 a sídlí v Shenzhen v Číně a hlavní zásadou společnosti Tencent je používat technologii pro dobro. Jejich sociální a komunikační služby spojují více než miliardu lidí po celém světě a pomáhají jim zůstat v kontaktu s přáteli a rodinou, mají přístup k dopravě, platí za každodenní potřeby a baví se. Společnost Tencent má mnoho částí, jak je vidět na obrázku 2⁵⁵.



Obrázek 2 Struktura společnosti Tencent

54 *Alibabagroup.com: informační portál obchodní společnosti Alibaba* [online]. 2023. [cit. 26.2.2023]. Dostupné z: <https://www.alibabagroup.com/en-US/about-alibaba>

55 Obrázek 2 převzat z: *Tencent.com: informační portál mediální a investiční společnosti Tencent* [online]. 2023. [cit. 26.2.2023]. Dostupné z: <https://www.tencent.com/en-us/about.html#about-con-1>

Tencent také vydává některé ze světově nejoblíbenějších videoher a další vysoce kvalitní digitální obsah, který obohacuje interaktivní zábavu pro lidi na celém světě. Tencent také poskytuje širokou škálu služeb, jako je cloud computing, reklama, FinTech a další obchodní služby na podporu digitální transformace a obchodního růstu svých zákazníků. Tencent je kotována na hongkongské burze od roku 2004.⁵⁶

ROZBOR BEZPEČNOSTNÍ SITUACE A RIZIKA

Z právního pohledu je třeba nejprve zmínit informace upřesňující celé bezpečnostní riziko, a tou je především uzákonění Zákona Čínské lidové republiky o státní zpravodajské činnosti, přijatý parlamentem Číny v roce 2017. Ten nařizuje jednotlivcům i firmám z důvodu státní potřeby špionáž ve prospěch Číny, jak je uvedeno podle Odstavce 1: Základní ustanovení, „7. článek: *Každá organizace i občan musí v souladu se zákonem podporovat, napomáhat a podílet se na státní zpravodajské činnosti a zachovávat v tajnosti vše, co je jim známo o státní zpravodajské činnosti. Stát poskytuje ochranu jednotlivcům a organizacím, které podpoří státní zpravodajskou činnost, napomohou jí a podílejí se na ní.*“⁵⁷ Díky tomuto zákonu jsou znevýhodňovány a ztrácejí důvěryhodnost všechny čínské firmy ve světě mimo stát Čínské lidové republiky.

Musíme rovněž brát v úvahu, že je Čína autoritativní stát, jehož hlavním zájmem je vlastní prospěch i v oblasti bezpečnosti a nemůžeme tedy čekat, že z tohoto hlediska bude brát ohled na bezpečnostní zájmy ostatních zemí, tedy i naší země.

Umělá inteligence v Číně má mnoho výzev a rizik. Těmi jsou například etické a právní otázky týkající se ochrany soukromí, lidských práv a odpovědnosti za rozhodování založené na umělé inteligenci. Bezpečnostní a geopolitické riziko zneužití umělé inteligence pro vojenské nebo špionážní účely nebo pro podkopání

⁵⁶ Tencent.com: informační portál mediální a investiční společnosti Tencent [online]. 2023. [cit. 26.2.2023]. Dostupné z: <https://www.tencent.com/en-us/about.html#about-con-1>

⁵⁷ Sinopsis.cz: informační portál projektu neziskové organizace AcaMedia z.ú. realizovaný za odborné spolupráce s Katedrou sinologie FF UK v Praze. Čínský zákon o celonárodní špionáži [online]. 27.2.2019. [cit. 26.2.2023]. Dostupné z: <https://sinopsis.cz/cinsky-zakon-o-celonarodni-spionazi/>

demokratických hodnot. Sociální a ekonomické dopady umělé inteligence na zaměstnanost, nerovnost a sociální soudržnost. Technologické a vědecké výzvy spojené s dosažením superinteligence nebo generální umělé inteligence, která by mohla překonat lidskou inteligenci ve všech ohledech.

Čína může zneužít umělou inteligenci pro vojenské nebo špiónážní účely, například pro vývoj autonomních zbraní nebo kybernetických útoků. Čína může ohrožit lidská práva a demokratické hodnoty pomocí umělé inteligence, například pro sledování a potlačování disidentů nebo menšin. Dále může usilovat o globální dominanci v umělé inteligenci a tvořit technologický ekosystém budoucnosti, který by ovlivnil ekonomiku, kulturu a politiku celého světa.

Bezpečnostní rizika a výzvy, které jsem před tím zmínil, se již postupně některá začínají objevovat, a proto nejde o pouhou fikci. Například čínské zpravodajské služby se na Českou republiku stále zaměřují pomocí své vědecko – technické špiónáže a zneužívají k tomu i mezinárodní vědecké projekty. Čeští akademici by tak měli zbystřit při spolupráci s čínskými kolegy.⁵⁸

Rovněž podle analýzy Joint Research Centre má Čína více publikovaných patentů než USA nebo Evropská unie, ale současně má méně startupů či firem než USA.⁵⁹

VÝSLEDKY A POTENCIONÁLNÍ DOPADY RIZIKA POUŽITÍ UMĚLÉ INTELIGENCE

Podle mého názoru pravděpodobnost tohoto rizika je hodně velká a reálná, hlavně proto, že už se tak děje. Jako příklad slouží zvyšující se počty kybernetických útoků. Ty dopady jsou například:

58 KARÁSKOVÁ, Ivana, Filip ŠEBOK a Veronika BLABLOVÁ. *Čína jako riziko pro bezpečnost výzkumu: doporučení pro akademické a výzkumné instituce* [online]. Praha: Asociace pro mezinárodní otázky (AMO), 2022. Analýza (Asociace pro mezinárodní otázky). ISBN: 978–80–88470–17–5. [cit. 26.2.2023]. Dostupné z: https://www.amo.cz/wp-content/uploads/2022/11/HTDTR_cina-jako-riziko-pro-bezpecnost-vyzkumu.pdf

59 RIGHI, Riccardo, Camila PINEDA LEON, Melisande CARDONA, Josep SOLER GARRIDO, Michail PAPAZOGLU, Sofia SAMOILI a Miguel VAZQUEZ–PRADA BAILLET. *AI Watch Index 2021* [online]. Lucemburk: Publications Office of the European Union, 2022. EUR 31039 EN. ISBN 978–92–76–53602–4. doi:10.2760/921564. JRC128744. [cit. 26.2.2023]. Dostupné z: <https://publications.jrc.ec.europa.eu/repository/handle/JRC128744>

Možnost zneužití AI pro špionáž, sabotáž nebo kybernetické útoky proti českým institucím, podnikům nebo infrastruktuře. Možnost ztráty konkurenční výhody nebo technologického náskoku v oblastech, kde má Česká republika silné postavení, jako je strojírenství, zemědělství nebo zdravotnictví. Možnost porušení etických principů nebo lidských práv při používání AI pro sociální kreditování, masové sledování nebo cenzuru. Možnost ohrožení existenciální bezpečnosti lidstva v případě vzniku superinteligence s cíli neslučitelnými s lidskými hodnotami.

Česká republika se snaží čelit těmto rizikům tím, že podporuje rozvoj umělé inteligence v souladu s evropskými normami a hodnotami. Vláda schválila Národní strategii umělé inteligence v ČR, která je založena na třech pilířích: excelentní výzkum a inovace, odpovědné používání AI a rozvoj digitálních dovedností a gramotnosti. Česká republika také spolupracuje s ostatními členskými státy EU a mezinárodními organizacemi na stanovení společných pravidel a standardů pro AI.

Nepříznivé dopady to může mít na náš průmysl a obchod s Čínou, zvláště tam, kde by naše firmy nevědomky podporovaly čínské firmy, které obchodují s Ruskou federací. Ta je aktuálně ve válce a pod sankcemi a pomocí umělé inteligence by se ještě více skryly, a jak bylo již řečeno dříve, došlo by ke špionáži.⁶⁰ Měli bychom si uvědomit, že umělá inteligence se používá už k rozpoznávání obličejů a hlasu pro sociální kreditování, sledování a cenzuru či digitální avataři pro moderování televizních show a on-line platform.

MOŽNOSTI ŘEŠENÍ DANÉ BEZPEČNOSTNÍ SITUACE

Jedna z možností řešení tohoto bezpečnostního rizika je zvyšovat povědomí a gramotnost o rizicích a přínosech AI mezi veřejností i odborníky. Další možnost je zlepšovat ochranu osobních dat a soukromí před zneužitím AI pro špionáž nebo manipulaci. Významným činitelem je i podporovat spolupráci a dialog mezi EU a Čínou na stanovení společných etických principů a pravidel

60 GARCIA, Naomi. *Trade Secrets. Exposing China–Russia Defense Trade in Global Supply Chains* [online]. C4ADS. July 15. 2022. 2022. s. 23 [cit. 26.2.2023]. Dostupné z: <https://c4ads.org/wp-content/uploads/2022/07/TradeSecrets-Report.pdf>

pro AI a investovat do výzkumu a inovace AI v souladu s evropskými hodnotami a normami. Důležitým bodem je také rozvíjet digitální dovednosti a kompetence potřebné pro práci s AI nebo vedle ní.

Další scénář možného řešení bezpečnostních rizik je ve zvýšení bezpečnostních opatření a zabránění nelegálnímu přístupu k citlivým informacím a datům. Prostřednictvím lepšího šifrování a využití bezpečnostních technologií se dá minimalizovat riziko úniku dat. Dále je vhodné nařídit a kontrolovat bezpečnostní standardy a pravidla, které vyžadují, aby všechny připojené systémy a sítě byly chráněny proti útokům zvenčí a zajišťují, že žádné nelegální aktivity neprobíhají.

Potom je vhodné zvýšit bezpečnostní výzkum a vývoj, aby se zajistilo, že budou k dispozici technologie pro detekci a odhalení útoků v souvislosti s umělou inteligencí. Tyto technologie by měly být schopny reagovat na útoky a aktivně je odrazovat.

Kromě toho je důležité spolupracovat s mezinárodními partnery a vyvinout strategii, která by se zaměřovala na zajištění bezpečnosti v oblasti umělé inteligence. Tato strategie by měla zahrnovat vzájemnou spolupráci v oblasti výzkumu a vývoje, spolupráci při stanovení bezpečnostních standardů a technologií a vytvoření platformy pro sdílení dat o bezpečnosti a útocích. Zde je potřeba zmínit i nezastupitelnou roli NATO a EU.

Konečně je vhodné zavést a vymáhat přísné sankce pro nelegální aktivity a porušení bezpečnostních opatření. Tyto sankce by měly být dostatečně silné na to, aby poskytovaly odrazovací efekt a zabránily budoucím podobným činům.

3.2.2 KAUZY S VYUŽITÍM UMĚLÉ INTELIGENCE V AUTOMOBILOVÉM PRŮMYSLU

V automobilovém průmyslu je mnoho kauz a bezpečnostních situací, proto jsem v této kapitole si vybral pouze jen některé.

OBECNĚ O KAUZE

Podle nových poznatků Národního úřadu pro bezpečnost silničního provozu (NHTSA) v USA, které se zaměřovaly na bezpečnostní výkon technologicky podporovaných, samořídících nebo autonomních vozidel na silnici.

Agentura shromažďovala data od 1. července 2021 do 15. května 2022 poté, co nařídila výrobcům automobilů hlásit kolize vozidel s pokročilými technologiemi řízení. Z těchto údajů NHTSA vygenerovala dvě zprávy, jednu zaměřenou na vozidla s pokročilými asistenčními systémy pro řidiče (ADAS) a další na systémy automatizovaného řízení (ADS).

Vozy s pokročilými asistenčními systémy pro řidiče jsou vozy, které mají automatické funkce pro rychlost a řízení, ale přesto vyžadují lidského řidiče. Příklady těchto funkcí jsou varování před kolizí, automatické brzdy, adaptivní tempomat a inteligentní parkovací asistent. Nejpopulárnější je, že tyto funkce jsou začleněny do režimu „*Autopilot*“ vozidel Tesla a do sady „*Sensing*“ novějších vozidel Honda.

Následují zjištění NHTSA o haváriích ADAS:

- Za 10 měsíců se vozy s pokročilými asistenčními systémy staly účastníky 392 kolizí.
- 273 z těchto nehod (téměř 70 %) se týkalo vozidel Tesla. Následovaly vozy Honda (90 bouraček) a Subaru (10 bouraček).
- Z celkových 392 nehod mělo šest obětí na životech. Z těchto šesti smrtelných nehod se pět týkalo vozidel Tesla.
- 27 dalších nehod mělo za následek středně těžká až těžká zranění.

Mezi státy měla Kalifornie nejvíce nehod ADAS: 125 nehod za 10 měsíců.

Mezitím se další zpráva NHTSA zabývala vozidly s automatizovanými systémy řízení, pokročilejšími automobilovými technologiemi, které nevyžadují lidské řidiče. Dobře propagovaným příkladem je režim „*Plné autonomní jízdy*“ společnosti Tesla. Ačkoli jsou technologie ADS stále ve vývoji a nejsou dosud dostupné veřejnosti, řada vozidel vybavených ADS již jezdí na veřejně přístupných silnicích.

Toto jsou zjištění NHTSA o haváriích souvisejících s ADS:

- Za 10 měsíců došlo u vozů s automatizovaným řízením ke 130 kolizím
- 62 z těchto nehod (48 %) se týkalo vozidel Waymo. Následovaly vozy Transdev (34 nehod) a CrAlse cars (23 nehod).

Waymo, jednotka autonomních vozidel společnosti Alphabet Inc., uvedla, že má ve svém vozovém parku více než 700 autonomních vozidel. Společnost provozuje plně autonomní službu pro volání v Arizoně a testuje ji v Kalifornii. Společnost uvedla, že všechny nehody se staly při nízkých rychlostech, přičemž airbagy se nafoukly pouze u dvou z nich.⁶¹

Z celkového počtu 130 nehod měly 4 za následek středně těžká až těžká zranění. Mezi státy měla Kalifornie nejvíce nehod ADS: 90 nehod za 10 měsíců. (Stojí za zmínku, že velká část testování vozů bez řidiče – včetně vozů Waymo, Tesla a CrAlse – probíhá v Kalifornii.)⁶²

Společnost Tesla má však svoje vlastní bezpečnostní zprávy týkající se těchto různých incidentů, kde se snaží mírnit dopady na její ekonomické aktivity a jméno společnosti.⁶³

61 *Npr.org: informační portál mediální společnosti. Nearly 400 car crashes in 11 months involved automated tech, companies tell regulators* [online]. 15.06.2022. [cit. 23.2.2023]. Dostupné z: <https://www.npr.org/2022/06/15/1105252793/nearly-400-car-crashes-in-11-months-involved-automated-tech-companies-tell-regul>

62 *Hamparyan.com: informační portál právníků zaměřených na nehody. Tesla Autopilot Accident Statistics and Other Driver-Assist/Autonomous Driving Technology Crash Data Released* [online]. [cit. 23.2.2023]. Dostupné z: <https://www.hamparyan.com/tesla-autopilot-accident-statistics/>

63 *Tesla.com: oficiální informační portál společnosti Tesla. Tesla Vehicle Safety Report* [online]. [cit. 23.2.2023]. Dostupné z: <https://www.tesla.com/VehicleSafetyReport>

VYSVĚTLENÍ TERMÍNŮ DANÉ KAUZY

Národní úřad pro bezpečnost silničního provozu (NHTSA) v USA je vládní agenturou a je zodpovědný za udržování bezpečnosti lidí na amerických silnicích.

Prostřednictvím prosazování standardů výkonu vozidel a partnerství se státními a místními vládami snižuje NHTSA úmrtnost, zranění a ekonomické ztráty při nehodách motorových vozidel.⁶⁴

NHTSA poskytuje granty vládám států, aby státy mohly provádět efektivní programy bezpečnosti silničního provozu.

Tesla, Inc. je americká nadnárodní společnost pro automobilový průmysl, umělou inteligenci a čistou energii se sídlem v Austinu v Texasu.

Tesla navrhuje a vyrábí elektrická vozidla (elektrická auta a nákladní auta), bateriová úložiště energie z domova až po síť, solární panely a solární střešní tašky a související produkty a služby.

Z hlediska kapitalizace je Tesla jednou z nejhodnotnějších společností na světě a od roku 2023 je nejhodnotnější automobilkou na světě. V roce 2021 měla společnost celosvětově nejvíce prodejů bateriových elektrických vozidel a plug-in elektrických vozidel, přičemž získala 21 % bateriového elektrického (čistě elektrického) trhu a 14 % trhu plug-in (včetně plug-in hybridy).

Se sídlem v Texasu provozuje šest obrovských, vertikálně integrovaných továren na třech kontinentech. S více než 100 000 zaměstnanci, Tesla týmy navrhuje, vyrábějí, prodávají své produkty interně včetně servisu i externě.

Prostřednictvím své dceřiné společnosti Tesla Energy společnost vyvíjí a je významným dodavatelem fotovoltaických systémů ve Spojených státech.⁶⁵

Alphabet, Inc. je v souhrnu sbírka společností. Největší z nich je samozřejmě Google. V Alphabetu jsou obsaženy společnosti, které jsou dost daleko od hlavních internetových produktů. Dalšími společnostmi jsou: Life Sciences (které fungují na kontaktních čočkách snímajících glukózu) a Calico (zaměřené na dlouhověkost).

64 *Nhtsa.gov: oficiální informační portál vládní agentury USA* [online]. [cit. 23.2.2023]. Dostupné z: <https://www.nhtsa.gov/about-nhtsa>

65 *Tesla.com: oficiální informační portál společnosti Tesla* [online]. [cit. 23.2.2023]. Dostupné z: <https://www.tesla.com/about>

Wikipedia.org: informační portál o všech věcech [online]. [cit. 23.2.2023]. Dostupné z: https://en.wikipedia.org/wiki/Tesla,_Inc

Ovšem od společností Alphabet pochází zprávy a analýzy o umělé inteligenci napříč všemi produkty.⁶⁶

ROZBOR BEZPEČNOSTNÍ SITUACE A RIZIKA

Automatické systémy pro dopravu s AI asistenty jsou součástí nové vlny technologického vývoje, které mají potenciál poskytovat výhody ve formě lepšího využívání silnic, větší bezpečnosti a nižších nákladů na pohonné hmoty. Nicméně, aby byly tyto systémy účinné a bezpečné, je třeba posoudit jejich bezpečnostní rizika.

Hlavní bezpečnostní rizika spojená s AI asistenty nebo autopiloty v automobilových systémech jsou: selhání systému AI, neúmyslné nebo úmyslné zneužití systému, neúmyslné poškození systému a únik informací včetně napadení systémů autopilotů a AI.

K tomuto zneužití již v minulosti došlo, např. o to se už několikrát úspěšně pokusil Tencent⁶⁷. Jde o mezinárodní investiční korporaci s vazbou na Čínskou lidovou republiku.

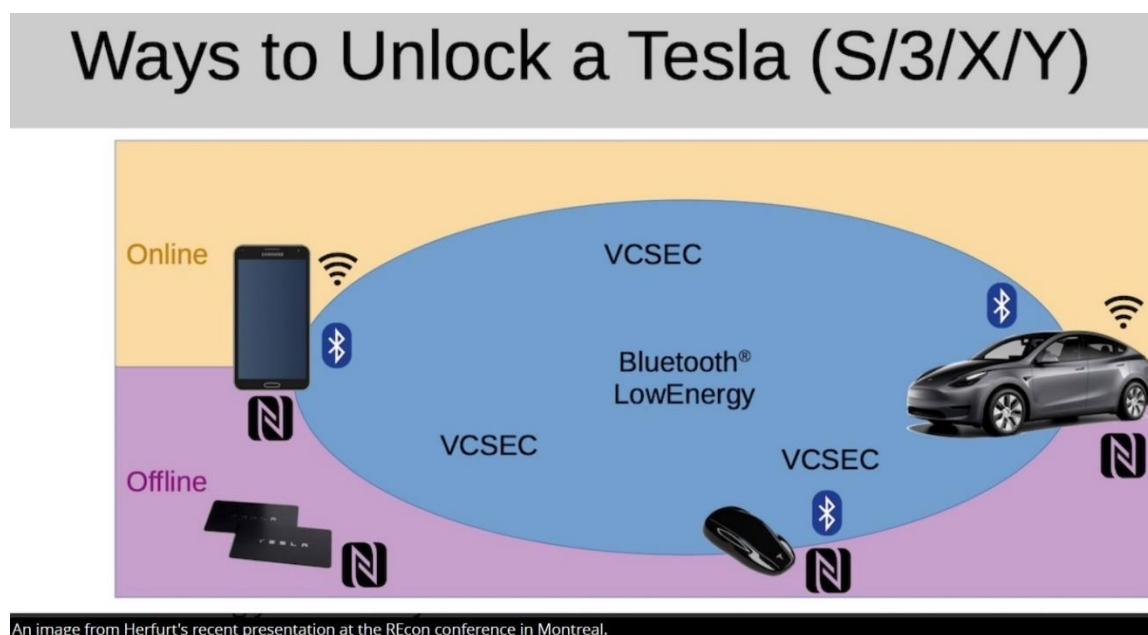
Selhání systému AI může vést k tomu, že AI nedokáže správně interpretovat a reagovat na situaci na silnici, což může vést ke ztrátě životů a majetku. Neúmyslné nebo úmyslné zneužití systému může vést k tomu, že řidič nedostane správnou informaci o situaci na silnici a může se rozhodnout pro nevhodnou jízdní trasu nebo rychlost. Neúmyslné poškození systému AI může být způsobeno technickými chybami nebo špatným nastavením systému AI, což může vést k nedostatečnému řízení dopravy a k náhlým změnám v chování automobilu.

Únik informací může být způsoben neúmyslným porušením bezpečnostních opatření nebo úmyslným hackováním systému. Například

66 *Abc.xyz: oficiální informační portál společnosti Alphabet, Inc.* [online]. [cit. 23.2.2023]. Dostupné z: <https://abc.xyz/>

67 *Keenlab.tencent.com: informační blog společnosti skupiny Keenlab patřící pod Tencent. Car Hacking Research: Remote Attack Tesla Motors* [online]. 19.09.2016. [cit. 23.2.2023]. Dostupné z: <https://keenlab.tencent.com/en/2016/09/19/Keen-Security-Lab-of-Tencent-Car-Hacking-Research-Remote-Attack-to-Tesla-Cars/>

u Tesly to vedlo ke zpřístupnění jiných vozidel Tesly⁶⁸, jak ukázáno na obrázku 3⁶⁹. Z toho vyplývá nutnost být v dosahu vozu během klíčového 130sekundového okna odemknutí pomocí NFC karty.



Obrázek 3 Možnosti, jak odemknout Teslu

Pokud majitel vozidla běžně používá k odemykání auta aplikaci pro telefon, což je zdaleka nejběžnější způsob odemykání vozů Tesla, pak si útočník může vynutit použití karty NFC pomocí rušičky signálu. Tím zablokuje frekvenci BLE používanou telefonem Tesla-as-a-key aplikaci, což může vést ke zneužití nebo zveřejnění informací o řidiči.

K zajištění bezpečnosti AI v automobilových systémech je nutné provádět důkladnou analýzu rizik a implementovat odpovídající bezpečnostní opatření. Některá z těchto opatření zahrnují pravidelné provádění testů AI systému, kontrolu bezpečnostních systémů a nastavení, pravidelnou kontrolu aktualizací systému AI a vytváření bezpečnostních manuálů pro řidiče a technický personál.

68 Arstechnica.com: *informační portál o technických věcech, Gone in 130 seconds. New Tesla hack gives thieves their own personal key* [online]. 06.08.2022. [cit. 23.2.2023]. Dostupné z: <https://arstechnica.com/information-technology/2022/06/hackers-out-to-steal-a-tesla-can-create-their-very-own-personal-key/>

69 Obrázek 3 převzat z: Arstechnica.com: *informační portál o technických věcech, Gone in 130 seconds. New Tesla hack gives thieves their own personal key* [online]. 06.08.2022. [cit. 23.2.2023]. Dostupné z: <https://arstechnica.com/information-technology/2022/06/hackers-out-to-steal-a-tesla-can-create-their-very-own-personal-key/>

VÝSLEDKY A POTENCIONÁLNÍ DOPADY RIZIKA POUŽITÍ UMĚLÉ INTELIGENCE

Umělá inteligence v dopravě má mnoho potenciálních dopadů na společnost, ekonomiku a životní prostředí. Pozitivní dopady mohou být tyto:

Zvýšení bezpečnosti a snížení nehod díky autonomním vozidlům a dronům. Zlepšení efektivity a optimalizace dopravních systémů díky plánování, řízení a predikci. Snížení emisí skleníkových plynů a spotřeby energie díky inteligentním řešením pro sdílenou mobilitu a alternativní paliva. Vytvoření nových pracovních příležitostí a trhů v oblasti vývoje, provozu a údržby umělé inteligence v dopravě.

Na druhou stranu umělá inteligence v dopravě také přináší některá rizika a výzvy, jako jsou:

Ztráta pracovních míst a sociální nerovnost důsledkem automatizace a digitalizace. Kybernetická bezpečnost a ochrana dat před možnými útoky nebo zneužitím. Etické a právní otázky ohledně odpovědnosti, transparentnosti a regulace umělé inteligence v dopravě. Spolehlivost a kvalita umělé inteligence v různých podmínkách a situacích.⁷⁰

Technologie umělé inteligence jsou klíčové pro vývoj nové generace bezpečnostních systémů vozidel, které mohou lépe chránit řidiče a chodce při řešení situací, kdy schopnosti lidského řidiče selžou (např. kvůli nesoustředěnosti nebo během rychlých událostí). Vozidla s vysokou úrovní automatizace také prokázala svůj potenciál vyhnout se nehodám ve složitých situacích, které mohou být pro řidiče náročné. Selhání umělé inteligence, ať už náhodné nebo v důsledku kybernetického útoku, se však vyskytlo také v situacích, kdy by lidští řidiči nebyli zmateni.⁷¹

70 RECHTIK, Marek. *Kybernetická bezpečnost v automobilovém sektoru. Bezpečnostní Teorie a Praxe* [online]. 2021, roč. 2021, č. 2. Praha. Policejní akademie ČR v Praze. [cit. 25.2.2023]. s.121–132. ISSN 2571–4589. Dostupné z: <https://veda.polac.cz/wp-content/uploads/2021/07/Kyberneticka-bezpecnost-v-automobilovem-sektoru.pdf>

71 HAMON, Ronan, Henrik JUNKLEWITZ, Jose Ignacio SANCHEZ MARTIN, David FERNANDEZ LLORCA, Emilia GOMEZ GUTIERREZ, Antonio HERRERA ALCANTARA a Akos KRISTON. *Artificial Intelligence in Automated Driving: an analysis of safety and cybersecurity challenges*. Brusel: European Commission [online]. 2022. JRC127189. [cit. 25.2.2023]. Dostupné z: <https://publications.jrc.ec.europa.eu/repository/handle/JRC127189>

Z psychologického pohledu dopady na řidiče jsou změna postoje a důvěry k technologii a jejímu vlivu na bezpečnost a kontrolu. Změna motivace a zájmu o řízení a jeho sociální a kulturní hodnoty. Změna emocí a nálad při řízení nebo cestování s umělou inteligencí. Změna chování a adaptace k novým situacím a pravidlům v dopravě.

Technická náročnost napadení je střední. Protože typy útoků mohou být phishingové útoky s využitím umělé inteligence, které se snaží získat citlivé informace od uživatelů nebo je přesvědčit k nebezpečným akcím. Další typy útoků jsou manipulace s umělou inteligencí, která se snaží ovlivnit její rozhodování nebo chování pomocí podvržených dat nebo signálů. Pak je ještě třeba zmínit možnosti sabotáže nebo poškození hardwaru či softwaru umělé inteligence v dopravě, jež mohou mít za následek nehody nebo poruchy.

MOŽNOSTI ŘEŠENÍ DANÉ BEZPEČNOSTNÍ SITUACE

Právní řešení těchto incidentů v ČR je dáno současnými právními předpisy, která se neustále vyvíjí a sleduje i linii EU norem. Co se týká automobilového průmyslu a rizik spojených s umělou inteligencí v něm, je zatím pouze dáno v České republice mít povinné ručení pro všechna motorová vozidla včetně těch s AI.

EU má zaveden princip objektivní odpovědnosti pro výrobce nebo provozovatele umělé inteligence v případě škody na majetku nebo osobách, v EU je také navrhován etický a právní rámec pro umělou inteligenci, který by stanovil pravidla pro transparentnost, bezpečnost a důvěru.

Prakticky většinou oběť žaluje a požaduje náhradu škod po vlastníku daného dopravního prostředku, a pokud se uzná vinným, tak platí on. Ovšem pokud z vyšetřování může vyjít najevo, že za nehodu mohla technická chyba daného dopravního prostředku, která mohla vzniknout nikoliv ze zavinění daného vlastníka, ale například aktualizací softwaru, tak se žaluje výrobce daného dopravního prostředku a musí znova proběhnout šetření a dokazování.⁷²

⁷² OSULA, Anna–Maria, Bríd NÍ GHRÁINNE, Dan Jerker B. SVANTESSON, et al. *Cybersecurity law casebook*. Brno: Masaryk University, 2021. s.243–244 ISBN 978–80–210–9773–5.

Samozřejmě existují i obecná pravidla pro naše bezpečí, která všude doporučuji. Jde tedy o to zajistit včasnou aktualizaci bezpečnostních systémů, nenechávat cenné věci v dopravním prostředku, při odemykání a zamykání se ujistit, že nás nikdo nesleduje a nevyvíjí podezřelou aktivitu či sledovat upozornění od policie a výrobce daného prostředku.

3.2.3 KAUZY S POUŽITÍM UMĚLÉ INTELIGENCE V DIGITÁLNÍM UMĚNÍ

V digitálním umění je v poslední době příliš mnoho kauz zahrnující umělou inteligenci, a proto jsem si vybral pouze některé.

OBEČNĚ O KAUZE

13. ledna 2023 podal hromadnou žalobu designér, programátor a právník Matthew Butterick, který kromě toho se stejným týmem advokátů řeší žalobu GitHub Copilot kvůli pirátství a zdrojovým kódům. V tomto případě se k Butterickovi připojili tři umělci, jimiž jsou ilustrátorka a autorka stripů Sarah's Scribbles Sarah Andersen, dále malířka, lektorka a ilustrátorka Kelly McKernan a koncepční umělkyně Karla Ortiz, která se podílela na řadě filmů a her, například i pro Marvel. Žaloba byla vznesena proti společnosti Stability AI, která stojí za vývojem Stable Diffusion, dále společnosti DeviantArt, jež provozuje stejnojmennou komunitu pro umělce, která se však svezla na vlně umělé inteligence a porušuje vlastní podmínky používání, a také společnosti Midjourney, jejíž služba je v tuto chvíli na poli AI umění nejznámější. K celé záležitosti vznikl i web, kde jsou detailně popsány principy generovaného umění, ale i smysl žaloby, jelikož zatím neexistuje žádný právní precedens, jak poznamenala sama Karla Ortiz. K dispozici je také seznam umělců, na jejichž dílech se měla umělá inteligence cvičit.⁷³

⁷³ Vortex.cz: *informační portál o technických věcech, hrách a umění*. SULKOVÁ, Kristýna. *Umělci žalují autory AI generátorů kvůli krádežím děl, cílem jsou Stable Diffusion, Midjourney, ale i DeviantArt. Žalobu podalo i Getty Images* [online]. 18. 1. 2023. [cit. 23.2.2023]. Dostupné z: <https://www.vortex.cz/umelci-zaluji-autory-ai-generatoru-kvuli-kradezim-del/>

Umělci žádají soud o zastavení používání Stable Diffusion a odškodnění za porušení autorských práv. Tvrdí, že Stable Diffusion obsahuje neoprávněné kopie milionů jejich děl bez jejich souhlasu nebo kompenzace. Také argumentují, že Stable Diffusion poškozuje jejich reputaci a snižuje hodnotu jejich děl.

Soudní spor by mohl mít dopad na budoucnost umění generovaného umělou inteligencí.

Obviněné společnosti reagovaly různě na soudní spor. Jejich různá vyjádření uvádím níže.

Stability AI prohlásila, že Stable Diffusion je otevřený AI nástroj, který je určen pro vzdělávací a výzkumné účely. Tvrdí, že nejsou zodpovědní za to, jak jejich uživatelé používají jejich software. Také tvrdí, že Stable Diffusion nekopíruje existující obrázky, ale vytváří nová originální díla.

Deviant Art uvedla, že respektuje autorská práva umělců a nabídla možnost umělcům požádat o odstranění jejich děl ze Stable Diffusion. Také uvedla, že Stable Diffusion je experimentální funkce na jejich webu a není určena k porušování autorských práv.

Midjourney nevydala žádné oficiální prohlášení o soudním sporu. Nicméně podle některých zdrojů se pokusila vyjednávat s umělci o možném smírném řešení.⁷⁴

VYSVĚTLENÍ TERMÍNŮ DANÉ KAUZY

Stability AI je společnost, která staví otevřené AI nástroje, které nám pomohou dosáhnout našeho potenciálu. Jejich nejznámějším produktem je Stable Diffusion V2, který je založen na modelu latentní difúze. Tento model dokáže generovat vysoko rozlišené obrázky z textových popisů nebo klíčových slov.

Další oblastí je generování textu z obrázků. Stability AI pracuje na novém produktu nazvaném Stable Caption V1, který by měl být schopen popsat obsah

74 Stablediffusionlitigation.com: informační portál o soudních sporech a umění. BUTTERICK, Matthew. *We've filed a law-sAlt chal-leng-ing Sta-ble Dif-fu-sion, a 21st-cen-tury col-lage tool that vio-lates the rights of artists. Because AI needs to be fair & eth-i-cal for every-one* [online]. 13. 1. 2023. [cit. 27.2.2023]. Dostupné z: <https://stablediffusionlitigation.com/>

obrázku pomocí přirozeného jazyka. Tento produkt by mohl být konkurentem Google Cloud Vision API, který nabízí podobnou službu.

Stabilita plánuje další produkty na konec tohoto roku. Startup plánuje vydat soupeře ChatGPT, řekl technologický ředitel Tom Mason. Jeho cílem je také debutovat systémy pro video generované umělou inteligencí a silně se zaměřuje na poskytování služeb společností ve filmovém průmyslu. „*Tento rok pracujeme na videomodelech, což je moje vášeň,*“ řekl Mason.⁷⁵

Stability AI byla založena v roce 2020 v Londýně. Jejím zakladatelem a CEO je James Smith, bývalý vědec z DeepMind. Mezi další klíčové členy týmu patří Alice Jones, hlavní vědecká pracovnice a vedoucí týmu latentní difúze, a Bob Lee, hlavní technický ředitel a vedoucí týmu pro rozvoj Stable Diffusion.

Stability AI má více než 80 zaměstnanců, kteří pracují na různých projektech souvisejících s umělou inteligencí. Společnost má tři hlavní oddělení: výzkum a vývoj (R&D), marketing a obchod (M&S) a právní a etické (L&E). R&D oddělení se zabývá návrhem a implementací nových AI modelů a algoritmů. M&S oddělení se stará o propagaci a distribuci produktů společnosti. L&E oddělení se zabývá otázkami souvisejícími s autorskými právy, ochranou osobních údajů a etikou umělé inteligence.

Stability AI je financována zejména ze soukromých zdrojů. V roce 2021 získala 89 milionů liber ve druhém kole financování od společností Sequoia Capital, Andreessen Horowitz a Y Combinator. Společnost také spolupracuje s některými akademickými institucemi, jako jsou University of Oxford, Imperial College London a ETH Zurich.⁷⁶

Deviant Art je online komunita pro umělce a milovníky umění. Nabízí platformu pro sdílení a prohlížení uměleckých děl různých žánrů a stylů. DeviantArt, založená v srpnu 2000, je největší online sociální síť pro umělce a umělecké nadšence a platforma pro začínající i zavedené umělce, kteří mohou

⁷⁵ Bloomberg.com: mediální informační portál o všech věcech. BASS. Dina a ANAND. Priya. *OpenAI Is Drawing Competition From Fleet of Startups* [online]. 06. 02. 2023. [cit. 27.2.2023]. Dostupné z: <https://www.bloomberg.com/news/articles/2023-02-06/openai-s-growing-list-of-competitors-anthropic-google-stability-ai-and-more>

⁷⁶ Stability.ai: oficiální informační portál společnosti STABILITY AI LTD [online]. 2023. [cit. 27.2.2023]. Dostupné z: <https://stability.ai/>

vystavovat, propagovat a sdílet svá díla s nadšenou komunitou zaměřenou na umění. Mají přes 61 milionů registrovaných členů a měsíčně přilákají přes 45 milionů unikátních návštěvníků. Deviant Art spolupracuje se Stability AI na integraci Stable Diffusion do svého webu.⁷⁷

Midjourney je nezávislá výzkumná laboratoř, která produkuje umělou inteligenci pod stejným názvem, která vytváří obrázky z textových popisů. Midjourney byla založena Davidem Holzem, spoluzakladatelem společnosti Leap Motion. Poprvé vstoupila do otevřené testovací fáze beta (stupeň vývoje softwaru) 12. července 2021. Nicméně již 14. března 2022 byl spuštěn discord server s žádostí o přístup k AI.

Midjourney má za cíl zkoumat nové formy myšlení a rozšiřovat imaginativní schopnosti lidského druhu. Jejich AI je založena na modelu nazvaném Midas, který je inspirován modelem latentní difúze od Stability AI. Midas dokáže generovat různé styly a žánry obrázků z jednoduchých nebo složitých textových popisů.

Midjourney má malý tým složený z vědců, umělců a programátorů. Jejich zakladatel a CEO David Holz je také hlavním výzkumníkem a vedoucím týmu Midas. Mezi další členy týmu patří Anna Lee, hlavní umělecká ředitelka a vedoucí týmu pro vizuální stylizaci, a Tom Chen, hlavní technický ředitel a vedoucí týmu pro optimalizaci a škálování AI.

Midjourney je mobilní aplikace pro Android zařízení, která umožňuje uživatelům vytvářet obrázky pomocí Stable Diffusion. Aplikace využívá technologii Qualcomm Snapdragon Neural Processing Engine (NPE) pro urychlení generování obrázků na mobilních zařízeních.⁷⁸

ROZBOR BEZPEČNOSTNÍ SITUACE A RIZIKA

Umělá inteligence v digitálním umění je schopnost strojů vytvářet nebo podporovat tvorbu uměleckých děl, jako jsou hudba, malba, literatura nebo film.

⁷⁷ Deviantart.com: oficiální informační portál společnosti [online]. 2023. [cit. 27.2.2023]. Dostupné z: <https://www.deviantart.com/>

⁷⁸ Midjourney.com: oficiální informační portál nezávislé laboratoře společnosti [online]. 2023. [cit. 27.2.2023]. Dostupné z: <https://www.midjourney.com/home/?callbackUrl=%2Fapp%2F>

Umělá inteligence může být použita k napodobení lidské kreativity, generování nových nápadů či stylů, nebo ke spolupráci s lidmi na společných projektech.

Přínosy umělé inteligence v tomto odvětví jsou rozmanitá, například mohou rozšířit možnosti a dostupnost umění pro širokou veřejnost, podpořit kulturní rozmanitost a inkluzi, zlepšit kvalitu a originalitu uměleckých děl, poskytnout nové způsoby učení a inspirace pro lidi i stroje, přispívat k sociálnímu a ekonomickému rozvoji.

Rizika umělá inteligence mohou být v ohrožení autorských práv a duševního vlastnictví umělců i uživatelů, narušení tradiční estetické normy a hodnoty, zpochybnit lidskou roli a identitu v umění, vyvolat etické a morální dilematy ohledně odpovědnosti za umělecká díla vytvořená stroji nebo jejich zneužití pro manipulaci nebo propagandu.⁷⁹

Závažným problémem je ten fakt, že tato rizika už jsou všude přítomná, a jak bylo napsáno v úvodu této kauzy, tak již probíhají. Existuje mnoho příkladů digitálního umění vytvořeného pomocí AI, některé z nich jsou:

Classical AI je projekt společnosti Microsoft a České filharmonie, který využívá AI k vytváření nových hudebních skladeb ve stylu klasických skladatelů jako Beethoven nebo Dvořák. Projekt byl představen v roce 2021 a od té doby se stal populárním mezi milovníky klasické hudby.

AI používá technologii nazvanou Ricercar, která dokáže analyzovat existující hudební díla a generovat nové motivy a harmonie na základě nich. Ricercar také umožňuje lidským hudebníkům interagovat s AI a improvizovat společně.

Classical AI je příkladem symbolické AI, která pracuje s logikou a jazykovým zpracováním. Symbolická AI byla dominantním paradigmatem

79 *BOZP a budoucnost práce: přínosy a rizika nástrojů umělé inteligence na pracovištích* [online]. Lucemburk: Úřad pro publikace Evropské unie, EU-OSHA (Evropská agentura pro bezpečnost a ochranu zdraví při práci), 05.07.2019. [cit. 27.2.2023]. Dostupné z: <https://osha.europa.eu/cs/publications/osh-and-future-work-benefits-and-risks-artificial-intelligence-tools-workplaces>

v počátcích výzkumu AI, ale postupně ustoupila ve prospěch sub-symbolické AI, která se zaměřuje na neuronové sítě a strojové učení.⁸⁰

DALL-E je generativní model AI od společnosti OpenAI, který dokáže vytvářet realistické obrázky na základě textových popisů. Například můžete zadat „kočka se zmrzlinou“ a DALL-E vygeneruje různé verze takového obrázku.

NightCafe je online platforma, která umožňuje uživatelům vytvářet a sdílet digitální umění pomocí AI. Můžete si vybrat ze stovek stylů a efektů a aplikovat je na své fotografie nebo obrázky.

Artbreeder je další online platforma, která používá AI ke generování nových obrázků na základě kombinace existujících. Můžete si hrát s různými parametry a vidět, jak se mění vzhled vašeho uměleckého díla.⁸¹

VÝSLEDKY A POTENCIÁLNÍ DOPADY RIZIKA POUŽITÍ UMĚLÉ INTELIGENCE

Umělá inteligence (AI) má velký potenciál pro rozvoj digitálního umění a pro podporu tvůrčích schopností lidí. AI může pomoci s generováním nových nápadů, stylů a forem uměleckého vyjádření. AI také může zlepšit kvalitu a dostupnost uměleckých děl pro širokou veřejnost. Nicméně, AI také přináší některá rizika a výzvy pro zaměstnance v oblasti digitálního umění.

Otázky pro potenciální dopady zjistíme pomocí otázek jako například: Jak zajistit transparentnost, spravedlnost a odpovědnost za AI? Jak chránit autorská práva a duševní vlastnictví tvůrců? Jak respektovat lidskou důstojnost a kulturní rozmanitost? Jak ovlivní AI společenskou úlohu umění a jeho hodnoty? Jak se vyrovnat s možným ztrátou pracovních míst nebo změnou povahy práce v důsledku automatizace? Jak podpořit spolupráci mezi lidmi a AI? Jak připravit zaměstnance na nové dovednosti a kompetence potřebné pro práci s AI? Jak

80 Microsoft.com: oficiální informační portál společnosti Microsoft. KARLIN, Primož. *Classical AI. Umělá inteligence otvírá nové obzory nejen v umění* [online]. 2023. [cit. 27.2.2023]. Dostupné z: <https://news.microsoft.com/cs-cz/features/classical-ai-umela-inteligence-otvira-nove-obzory-nejen-v-umeni/>

81 Mpost.io: informační portál o všech věcech. YALALOV, Damir. *7 nejlepších generátorů umění AI roku 2023: Midjourney, DALL-E, NightCafe, Artbreeder* [online]. 25. února 2023. [cit. 27.2.2023]. Dostupné z: <https://mpost.io/cs/7-nejlep%C5%A1%C3%ADch-gener%C3%A1tor%C5%AF-ai-artu-2022-midjourney-dall-e-nightcafe-artbreeder/>

podporovat celoživotní učení a adaptabilitu? Jak začlenit etické vzdělání do kurikul uměleckých škol?

Rizika umělé inteligence v digitálním umění určitě mohou být například tohoto typu AI může ohrozit autorská práva a duševní vlastnictví umělců tím, že napodobuje nebo kopíruje jejich díla bez jejich souhlasu nebo uznání. AI může také snižovat hodnotu a originalitu uměleckých děl tím, že je masově produkuje nebo standardizuje. AI může ovlivnit trh práce v digitálním umění tím, že nahradí některé dovednosti nebo povolání automatizací nebo optimalizací.

Trh práce v digitálním umění je ovlivněn různými faktory, jako jsou technologické změny, ekonomické podmínky nebo kulturní trendy. Možnosti, jak AI může ovlivnit trh práce uvádím níže.

AI může zvýšit poptávku po nových dovednostech a kompetencích v digitálním podnikání, jako jsou online obchod, digitální marketing, sociální média nebo analýza dat. AI může také snížit poptávku po některých tradičních dovednostech a povoláních v digitálním umění, jako jsou grafický design, fotografie nebo ilustrace. AI může změnit způsob práce a spolupráce v digitálním umění tím, že podporuje více flexibilní a projektové formy zaměstnání nebo týmovou práci napříč různými disciplínami.

Aktuálně můžeme pozorovat obrovský psychologický nátlak na umělce v digitálním průmyslu u různých studií, které se zabývají filmem, VFX apod. Současně v Japonsku už se pokusili vytvořit kreslený seriál jenom s pár lidmi bez studia, je to především kvůli tomu, že v Japonsku je dlouhodobý nedostatek animátorů, což je způsobeno tím, že jsou špatně placeni.

Technická náročnost závisí především na trhu práce a firmách či studiích, což je problém, protože už teď začínají s tím být problémy.

MOŽNOSTI ŘEŠENÍ DANÉ BEZPEČNOSTNÍ SITUACE

Umělci se mohou bránit tím, že se mohou informovat o možnostech a rizicích AI a sledovat její vývoj a dopady na jejich obor. Dále se umělci mohou zapojit do diskusí a iniciativ o etických a právních aspektech AI a požadovat transparentnost a odpovědnost od tvůrců a uživatelů. Další možností je, že se AI či umělci mohou vzdělávat a rozvíjet své dovednosti a kompetence v oblastech, kde AI nemůže napodobit lidskou inteligenci, jako je kreativita, empatie nebo

kritické myšlení. A v neposlední řadě umělci mohou spolupracovat s ostatními umělci nebo odborníky z jiných disciplín, aby využili synergii mezi lidskou a umělou inteligencí a vytvářeli nové formy umění.

Ty právní případy, o kterých jsem se zmínil v úvodu této kauzy se týkají bohužel i naší země České republiky, protože máme dobré vztahy s USA a bude záležet na naší vládě, jak se k tomu postaví. Očekává se, že dojde k různým změnám a přesunu velkého množství lidí v daném průmyslu, protože firmy na základě poptávky budou požadovat, aby umělci pracovali s umělou inteligencí nebo si budou muset změnit zaměstnání. O výsledku této kauzy se můžeme jenom dohadovat, protože k rozhodnutí ještě nedošlo. Ovšem mohu podotknout, že ve Spojených státech amerických došlo k určitému rozhodnutí ze strany kanceláře autorství knihovny kongresu, a to že je vyžadováno prokázání použití velké části lidského faktoru při tvorbě díla.⁸²

Rovněž bych chtěl zmínit, že umělci se mohou částečně chránit nástrojem Glaze. Glaze je nástroj vyvinutý týmem vědců z University of Chicago, který umožňuje umělcům chránit svůj styl před napodobováním pomocí AI modelů. Software maskuje obrázky tak, že modely nesprávně naučí jedinečné rysy, které definují styl umělce, čímž brání následným snahám o generování umělých plagiátů. Glaze analyzuje vaše umění a vytváří upravenou verzi (sotva viditelnou pro lidské oko), která může být použita k ochraně vašeho stylu před napodobováním AI.⁸³

3.3 RIZIKA UMĚLÉ INTELIGENCE PRO PRACOVNÍ LOKÁLNÍ A GLOBÁLNÍ TRH

Rozvoj umělé inteligence (AI) přináší na pracovní trhy České republiky i globálně různá rizika a trendy. Zde je přehled některých z nich:

⁸²*Federalregister.gov: informační portál databáze právních spisů Spojených států amerických.* [online]. 2023. [cit. 20.6.2023]. Dostupné z:

<https://www.federalregister.gov/documents/2023/03/16/2023-05321/copyright-registration-gAldance-works-containing-material-generated-by-artificial-intelligence>

⁸³*Glaze.cs.uchicago.edu: informační portál nástroje Glaze univerzity Chicago.* [online]. 2023. [cit. 16.7.2023]. Dostupné z: <https://glaze.cs.uchicago.edu/what-is-glaze.html>

Automatizace a ztráta pracovních míst: AI a automatizace mají potenciál nahradit některé pracovní pozice, což může způsobit nezaměstnanost v určitých odvětvích. Například výrobní linky mohou být nahrazeny roboty a algoritmy mohou provádět rutinní administrativní úkoly. To může ovlivnit především nízko kvalifikované pracovníky.

Potřeba přeškolení a rekvalifikace: Se změnou technologií a nástupem AI budou pracovníci potřebovat nové dovednosti, aby se mohli přizpůsobit novým pracovním požadavkům. Je důležité investovat do rekvalifikace a dalšího vzdělávání pracovníků, aby byli schopni zastávat nové role, které vyžadují vyšší míru kreativity, analytického myšlení a lidských dovedností.

Poptávka po nových dovednostech: S nástupem AI se mění poptávka po dovednostech. Některá pracovní místa mohou být nahrazena automatizací, ale zároveň vznikají nová pracovní místa vyžadující dovednosti v oblasti AI, strojového učení a datové analýzy. K dosažení úspěchu na trhu práce je důležité se neustále přizpůsobovat a rozvíjet nové dovednosti.

Nerovnost na pracovním trhu: Pokud se zaměříme na český pracovní trh, může rozvoj AI zvýšit nerovnosti mezi pracovníky s různou úrovní dovedností. Ti, kteří mají potřebné technologické znalosti a dovednosti, budou mít pravděpodobně větší příležitosti a vyšší platy než ti, kteří takové dovednosti nemají. To může vytvářet sociální a ekonomické nerovnosti mezi lidmi.

Etické a právní otázky: S rozšířením AI vznikají nové etické a právní otázky, které je třeba řešit. Patří sem například otázky soukromí a bezpečnosti dat, odpovědnosti za rozhodnutí založená na AI a diskriminace způsobená algoritmy s vlivem AI.

Vliv na odvětví: Různá odvětví budou mít různé úrovně vlivu AI na pracovní trh. Například v oblastech, které jsou založeny na analytických úkolech a velkém množství dat, jako je finanční sektor, marketing nebo zdravotnictví, se může očekávat větší vliv AI. Naopak, profesní oblasti, které vyžadují vysokou úroveň lidských interakcí a kreativity, jako je umělecká tvorba, sociální práce nebo vzdělávání, budou pravděpodobně méně ovlivněny.

Je důležité si uvědomit, že vliv AI na pracovní trh je komplexní a závisí na mnoha faktorech, včetně politiky, regulačního prostředí, investic do vzdělávání a technologického rozvoje.

Umělá inteligence (AI) má obrovský potenciál a může přinést mnoho výhod, ale také představuje určitá rizika. Podle průzkumu agentury NMS Research se 15 % Čechů obává, že kvůli AI přijde o práci. Oslovení experti se shodují, že některé pozice mohou zaniknout, ale AI hlavně výrazně zefektivní práci.⁸⁴

AI může zlepšit zdravotní péči, přinést bezpečnější auta a další dopravní prostředky a v neposlední řadě i levnější produkty s delší životností a služby přizpůsobené lidem na míru. V podnicích umožňuje AI vývoj nové generace produktů a služeb a může zlepšit údržbu strojů, zvýšit výkon a kvalitu produkce, úroveň služeb pro zákazníky a rovněž ušetří energii.⁸⁵

Je důležité se přizpůsobit novým trendům. Například ostrahy jsou nahrazovány chytrými kamerami v kombinaci s analýzou obrazu na základě umělé inteligence, přesto je ale stále potřeba lidský dohled a operátoři výroby se prostě vyškolí v ovládání robotických ramen. Podle studie týmu výzkumníků vedeného Princetonskou univerzitou jsou nejvíce ohrožená povolání operátoři call center a telemarketéři.⁸⁶ Další studie uvádí, že nejohroženější povolání jsou ta, která úzce souvisí se vzděláváním.⁸⁷

Především lidé, kteří pracují na počítači, zaznamenají výraznou proměnu práce. Nová generace nástrojů typu ChatGPT bude mít podle vědců výrazný dopad na lidskou práci. Některá odvětví a povolání – například třeba učitele, právníky, manažery, analytiku – čeká rapidní transformace atd.

Společnosti Nvidia, AMD a Intel jsou všechny aktivní v oblasti umělé inteligence a pomáhají ji zavádět do různých odvětví. Nvidia je nyní lídrem v oblasti

84 E15.cz: *informační portál o financích, obchodu a byznysu*. HORÁKOVÁ, Anna-Marie. *Umělá inteligence může zchladit přehřátý trh práce, vznikne ale taky řada nových pozic*. [online]. 2023. [cit. 20.6.2023]. Dostupné z: <https://www.e15.cz/byznys/technologie-a-media/umela-inteligence-muze-zchladit-prehraty-trh-prace-vznikne-ale-taky-rada-novych-pozic-1397681>

85 *Europarl.europa.eu: informační portál evropského parlamentu. Umělá inteligence: rizika i příležitosti*. [online]. 2023. [cit. 20.6.2023]. Dostupné z: <https://www.europarl.europa.eu/news/cs/headlines/society/20200918STO87404/umela-inteligence-jake-jsou-vyhody-a-nevyhody>

86 FELTEN, Ed, Manav RAJ a Robert SEAMANS. *How will language modelers like ChatGPT affect occupations and industries?* [online]. New York: NYU Stern School of Business, 2023. [cit. 20.6.2023]. Dostupné z: <https://arxiv.org/ftp/arxiv/papers/2303/2303.01157.pdf>

87 *Insmart.cz: informační portál o IT a všech věcech*. IIBOVÁ, Alena. *Přijďte o práci kvůli umělé inteligenci? Vědci zveřejnili seznam 5 nejohroženějších povolání*. [online]. 2023. [cit. 20.6.2023]. Dostupné z: <https://insmart.cz/pracovni-pozice-ohrozene-ai/>

hardwaru pro AI, ale Intel, AMD a další se rychle přibližují.⁸⁸ Intel má investice do vývojového společenství a partnerství s Googlem, Alibabou, US DOE a dalšími společnostmi.

Někteří odborníci se obávají, že by AI mohla být použita pro zlé účely a ohrožit pracovní místa. AI umožňuje počítači jednat a reagovat téměř jako člověk. Počítače mohou být naplněny obrovským množstvím informací a naučit se rozpoznávat vzory v nich, aby dělaly předpovědi, řešily problémy, a dokonce se učily ze svých vlastních chyb. Kromě dat se AI spoléhá na algoritmy – seznamy pravidel, které musí být dodržovány ve správném pořadí k dokončení úkolu. Technologie stojí za hlasově ovládanými virtuálními asistenty Siri a Alexa. Umožňuje Spotify, YouTube a BBC iPlayer navrhnout, co byste mohli chtít přehrát dál, a pomáhá Facebooku a Twitteru rozhodovat, které příspěvky na sociálních sítích ukázat uživatelům. AI umožňuje Amazonu analyzovat nákupní návyky zákazníků a doporučovat budoucí nákupy – a firma také používá technologii k potlačení falešných recenzí. Dvě silné aplikace nebo aplikace řízené AI, které se v posledních měsících staly velmi známými, jsou ChatGPT a Snapchat My AI. Jsou to příklady toho, co se nazývá „*generativní*“ AI. Tato používá vzory a struktury, které identifikuje v obrovském množství zdrojových dat, k vytváření nového a originálního obsahu, který působí jako by byl vytvořen člověkem. AI je spřažena s počítačovým programem známým jako chatbot, který „*mluví*“ s lidskými uživateli prostřednictvím textu. Aplikace mohou odpovídat na otázky, vyprávět příběhy a psát počítačový kód. Ale oba programy někdy generují nesprávné odpovědi pro uživatele a mohou reprodukovat zaujatost obsaženou v jejich zdrojovém materiálu, jako je sexismus nebo rasismus. S málem pravidel v současné době platných pro to, jak se AI používá, odborníci varovali, že její rychlý růst by mohl být nebezpečný. Někteří dokonce řekli, že by se měl výzkum AI zastavit. V květnu Geoffrey Hinton, široce považovaný za jednoho z kmotrů umělé inteligence, odešel ze své práce u Googlu s varováním, že chatboty AI by

88 *Marketwatch.com: informační portál o byznysu a všech věcech*. NEWMAN, Daniel. *Opinion: Nvidia is AI hardware's growth leader now, but Intel, AMD and others are closing fast*. [online]. 2023. [cit. 20.6.2023]. Dostupné z: <https://www.marketwatch.com/story/nvidia-is-ai-hardwares-leader-now-but-intel-amd-and-others-are-closing-fast-8ad6f23f>

mohly brzy být inteligentnější než lidé. Později v tomto měsíci americké Centrum pro bezpečnost AI zveřejnilo prohlášení podpořené desítkami předních odborníků na techniku. Tvrdí, že AI by mohla být použita ke generování dezinformací, které by mohly destabilizovat společnost. V nejhorším případě říkají, že stroje by mohly být tak inteligentní, že by převzaly kontrolu, což by vedlo k vyhynutí lidstva. Nicméně šéfka techniky EU Margrethe Vestagerová řekla BBC, že potenciál AI zesílit zaujatost nebo diskriminaci byl naléhavějším problémem.⁸⁹

Zprávy o globálních rizicích a budoucnosti práce Světového ekonomického fóra (WEF) jsou důležitými zdroji informací o současných a budoucích výzvách pro společnost a ekonomiku. Tyto zprávy se zabývají také roli umělé inteligence (AI) jako klíčového faktoru ovlivňujícího tyto výzvy a možné řešení.

Zpráva o globálních rizicích 2021 se zaměřuje na dopady pandemie COVID-19 na nerovnosti, fragmentaci společnosti a environmentální problémy. Zpráva varuje před rizikem „rozštěpené budoucnosti“, kdy by se svět rozdělil na nesourodé skupiny s odlišnými zdravotními, ekonomickými a technologickými příležitostmi. Zpráva zdůrazňuje potřebu spolupráce a solidarity mezi vládami, podniky, občanskou společností a mezinárodními organizacemi, aby se zabránilo dalšímu zhoršování situace. (WEF, 2021)

AI je v této zprávě zmíněna jako jedna z nejdůležitějších technologických inovací, která může přinést jak přínosy, tak rizika pro společnost a ekonomiku. AI může například pomoci zlepšit zdravotní péči, vzdělávání, energetiku a bezpečnost, ale také může způsobit ztrátu pracovních míst, narušení trhů, etické dilematy a kybernetické hrozby. Zpráva doporučuje vytvořit globální rámec pro spravedlivé a transparentní využívání AI v souladu s lidskými právy a demokratickými hodnotami. (WEF, 2021)⁹⁰

Zpráva o budoucnosti práce 2023 se zaměřuje na to, jak pandemie COVID-19 urychlila transformaci pracovního trhu a jaké jsou klíčové trendy a dovednosti

89. *Bbc.com: informační portál o všech věcech*. MCCALLUM, Shiona. *What is AI, is it dangerous and what jobs are at risk?* [online]. 2023. [cit. 20.6.2023]. Dostupné z:

<https://www.bbc.com/news/technology-65855333>

90 *Global Risks Report 2021 (16th ed.)*. [online]. World Economic Forum, 2021. [cit. 20.6.2023].

ISBN: 978-2-940631-24-7 Dostupné z:

https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

pro budoucí zaměstnanost. Zpráva analyzuje dopady automatizace, digitalizace, změny klimatu a sociální změny na poptávku po pracovní síle, kvalifikaci pracovníků a nerovnosti v přístupu ke práci. Zpráva také identifikuje nejžádanější role a dovednosti pro rok 2023 a nabízí doporučení pro podporu udržitelného a inkluzivního růstu. (WEF, 2023)

AI je v této zprávě považována za jeden z hlavních faktorů ovlivňujících budoucnost práce. AI může napomoci zvýšit produktivitu, inovaci a kvalitu služeb, ale také může vést k nahrazování lidských pracovníků stroji, polarizaci trhu práce a nerovnému rozdělování přínosů. Zpráva zdůrazňuje potřebu investovat do rekvalifikace a celoživotního učení pracovníků, aby byli schopni přizpůsobit se změnám v důsledku AI. Zpráva také navrhuje vytvořit sociální ochranu a spravedlivé pracovní podmínky pro všechny typy pracovníků, včetně těch, kteří pracují s AI nebo jsou jí ovlivňováni. (WEF, 2023)⁹¹

MOŽNOSTI ŘEŠENÍ DANÉ BEZPEČNOSTNÍ SITUACE

Existuje několik způsobů, jak se připravit na změny na trhu práce. Jedním z nich je neustálé vzdělávání a rozšiřování dovedností. Je důležité sledovat trendy ve svém oboru a učit se nové technologie a metody. Dalším způsobem je flexibilita a otevřenost novým příležitostem. Změny na trhu práce mohou přinést nové příležitosti pro ty, kteří jsou ochotni se přizpůsobit a vyzkoušet nové věci.

Je také důležité být aktivní a hledat nové příležitosti. To může zahrnovat networking, účast na konferencích a workshopech nebo hledání nových pracovních příležitostí. Nakonec je důležité mít pozitivní postoj a být připraven na změny. Trh práce se neustále vyvíjí a je důležité být připraven na nové výzvy.

Naštěstí se už začínají tyto technologie umělé inteligence podléhat standardizaci Mezinárodní organizace pro normalizaci (ISO) a Mezinárodní elektrotechnická komise (IEC) mají společný technický výbor JTC 1/SC 42, který se zabývá standardizací v oblasti umělé inteligence. Tento výbor slouží jako zdroj a propagátor standardizačního programu JTC 1 pro umělou inteligenci a poskytuje

⁹¹*Future of Jobs Report 2023*. [online]. World Economic Forum, 2023. [cit. 20.6.2023]. ISBN–13: 978–2–940631–96–4 Dostupné z: https://www3.weforum.org/docs/WEF_Future_of_Jobs_2023.pdf

pokyny výborům JTC 1, IEC a ISO, které vyvíjejí aplikace umělé inteligence.⁹² NIST (Národní institut pro standardy a technologie) také přispívá k rozvoji technických standardů pro AI.⁹³ Existují různé technické standardy pro AI, například ISO/IEC 23053:2022, který stanovuje rámec pro systémy umělé inteligence používající strojové učení.⁹⁴

Pokud si myslíme, že sami toho ovlivnit moc nemůžeme, tak se můžeme spolu s dalšími lidmi zapojit do vládních či nevládních organizací, které se zabývají umělou inteligencí. Například Světová banka, Mezinárodní organizace pro civilní letectví (ICAO), Dětský fond OSN (UNICEF) a Program rozvoje OSN (UNDP) využívají AI v iniciativách zaměřených na dosažení cílů.⁹⁵ Global Partnership on AI je multistakeholderská iniciativa založená skupinou G7, která pracuje na projektech zaměřených na regulaci a příležitosti pro rozvoj AI. Organizace pro hospodářskou spolupráci a rozvoj (OECD) založila AI Policy Observatory, které podporuje a informuje o vývoji politiky AI. Mnoho dalších mezinárodních organizací se také zabývá vývojem návrhů rámců pro zodpovědný rozvoj AI.⁹⁶

92 *Iso.org: informační portál standardizační instituce. ISO/IEC JTC 1/SC 42 Artificial intelligence.* [online]. 2023. [cit. 20.6.2023]. Dostupné z: <https://www.iso.org/committee/6794475.html>

93 *Nist.gov: informační portál standardizační instituce Spojených států amerických. Technical AI Standards.* [online]. 2023. [cit. 20.6.2023]. Dostupné z: <https://www.nist.gov/artificial-intelligence/technical-ai-standards>

94 *Iso.org: informační portál standardizační instituce. ISO/IEC 23053:2022 Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML).* [online]. 2023. [cit. 20.6.2023]. Dostupné z: <https://www.iso.org/standard/74438.html>

95 *Knowledge.insead.edu: informační portál znalostní instituce. MCLACHLIN, Ruth, Katherine TATARINOV, Tina AMBOS a Phanish PURANAM. Creating People-Centric International Organisations With AI.* [online]. INSEAD Knowledge, 2022. [cit. 20.6.2023]. Dostupné z: <https://knowledge.insead.edu/leadership-organisations/creating-people-centric-international-organisations-ai>

96 KERRY, Cameron F., Joshua P. MELTZER, Andrea RENDA, Alex C. ENGLER, Rosanna FANNI. *Strengthening international cooperation on AI: Progress report.* [online]. The Brookings Institution, 2021. [cit. 20.6.2023]. Dostupné z: https://www.brookings.edu/wp-content/uploads/2021/10/Strengthening-International-Cooperation-AI_Oct21.pdf

4. DOPORUČENÍ

Ze dříve řešených kauz moje doporučení pro jednotlivé kauzy zní následovně:

Pokud nám bude hrozit hrozba ze strany Číny, tak můžeme používat nejnovější technologie a nástroje pro kybernetickou bezpečnost, jako jsou antivirové programy, šifrování dat a monitorování síťového provozu.

Nutností je vzdělávat se o hrozbách a taktikách, státem sponzorovaných hackerů a sledovat aktuální zprávy a varování o jejich aktivitách či provádět pravidelné testy a simulace útoků na své systémy a zařízení, abychom odhalili slabá místa a zlepšili naši odolnost.

Rovněž pokud se chceme dozvědět o státem podporovaných skupinách tak můžeme najít zprávy a varování na různých webových stránkách a médiích, které se zabývají kybernetickou bezpečností a aktuálními hrozbami. Typu NIST (National Institute of Standards and Technology) nabízí nástroje a doporučení pro obranu proti státem sponzorovaným hackerům. CNBC zveřejňuje zprávy o čínských státem podporovaných hackerech, kteří pronikli do počítačových sítí alespoň šesti amerických států. Tech Republic informuje o tom, jak se státem sponzorovaní hackeři a skupiny ransomware mění své taktiky, aby způsobili více škody.

Používej silná hesla (16 a více znaků) a dvou faktorové ověřování pro všechny aplikace a služby spojené s tvým autem. Aktualizuj software a firmware tvého auta pravidelně a stahuj aktualizace pouze z oficiálních zdrojů. Vyvaruj se používání neznámých nebo podezřelých zařízení nebo USB klíčenek v tvém autě. Zvaž instalaci firewallu, který bude filtrovat komunikaci mezi tvým autem a ostatními entitami.

Pokud jsi umělec a bojíš se umělé inteligence a chceš si udržet svou práci, můžeš zvážit následující doporučení:

Používej nástroje a služby, které chrání tvé dílo před kopírováním nebo zneužitím umělou inteligencí. Například Lensa Stable Diffusion je nástroj, který přidává do obrázků šum, který je pro lidské oko neviditelný, ale znemožňuje umělé inteligenci generovat nové obrázky z nich.

Uč se o tom, jak funguje umělá inteligence a jak ji můžeš využít k tvorbě nových a originálních děl. Umělá inteligence není schopna vytvářet skutečné

umění bez lidského vstupu a kreativity. Můžeš ji použít jako spolupracovníka nebo inspiraci.

Zaměř se na to, co dělá tvé dílo jedinečné a osobité. Umělá inteligence nemůže napodobit tvůj styl, emoce, záměry nebo kontext. Můžeš také experimentovat s různými médii a technikami, které jsou pro umělou inteligenci obtížnější nebo nemožné.

ZÁVĚR

V této diplomové práci jsem Vás seznámil s mnoha bezpečnostními riziky, dopady a bezpečnostními situacemi týkajícími se použitím umělé inteligence, které mohou nastat a v současnosti již i probíhají. Zdroje jsem použil od roku 2016 až 2023. Téma, které jsem zde řešil je velice aktuální a velmi rozsáhlé. Kyberterorismus jsem zde řešil z pohledu roků 2022 až 2023 kvůli aktuální situaci ve světě. V posledních letech naše země Česká republika zažila přímo či nepřímo mnoho katastrof či nebezpečných situací jako jsou tornádo na Moravě, pandemie Covid-19 či válka na Ukrajině. V těchto situacích je umělá inteligence velkým pomocníkem v rychlém analyzování Big Dats (Velká data) a byla zde ku prospěchu použita. Vzhledem k tomu, že hardware a algoritmy se stále zdokonalují, dochází ke stále přesnějšímu a rychlejšímu výkonu. Z toho vyplývá nejen vyšší náročnost na obsluhu, ale také řešení i právní zodpovědnosti v dané oblasti. Právní základ je v různých zemích na různé úrovni, nejrozpracovanější normy jsou v Evropské unii nebo v USA. Zmínil jsem zde i organizace, jež se zabývají bezpečností, a proto je vysoce pravděpodobné, že budou rychle a přesně reagovat v případě bezpečnostních rizik spojených s použitím umělé inteligence. V praktické části jsem se zabýval elektromobilitou s autonomními systémy řízení, především kvůli tomu, že v době, kdy toto píšu, jsou podle EU a USA autonomní systémy brzkou budoucností, avšak má to stále spoustu bezpečnostních problémů. Popisoval jsem rovněž bezpečnostní riziko spojené s Čínou a jejími praktikami. V poslední době se již objevilo mnoho případů špionáže z jejich strany a jejich vývoj umělé inteligence má více patentů než EU a USA, což by nás mělo znepokojit, protože tento stát se chová agresivně ve sběru informací a jejich umělá inteligence se kromě zdravotnictví začíná používat i v armádě a jiných bezpečnostních oblastech. Jako poslední jsem rozebíral, co se děje v uměleckém světě. Z mého pohledu také patří v současnosti k nejohroženějším oborům lidské činnosti v souvislosti s riziky spojenými s použitím umělé inteligence a aktuálně je to tam už vidět. Cíle diplomové práce jsem, si myslím, do většinové míry splnil. K nalezení bylo mnoho zdrojů zahraničních i domácích, ale téma bezpečnostních rizik spojených s umělou inteligencí je tak rozsáhlé, že jsem ho omezil na vybraná témata. Ponaučení si z toho můžeme vzít takové, že se nacházíme uprostřed průmyslovo–technologické

revoluce, z našeho pohledu evoluce, započaté zpřístupněním PC veřejnosti následovaným internetem a aktuálně umělou inteligencí, která nás zasáhne všechny více či méně a je potřeba se na to adekvátně připravit.

SEZNAM OBRÁZKŮ

Obrázek 1 Centra NATO Excelence	28
Obrázek 2 Struktura společnosti Tencent	36
Obrázek 3 Možnosti, jak odemknout Teslu	45

SEZNAM LITERATURY

Monografie

- [1.] *BOZP a budoucnost práce: přínosy a rizika nástrojů umělé inteligence na pracovištích* [online]. Lucemburk: Úřad pro publikace Evropské unie, EU–OSHA (Evropská agentura pro bezpečnost a ochranu zdraví při práci), 05.07.2019. [cit. 27.2.2023]. Dostupné z: <https://osha.europa.eu/cs/publications/osh-and-future-work-benefits-and-risks-artificial-intelligence-tools-workplaces>
- [2.] *Etické pokyny pro zajištění důvěryhodnosti AI* [online]. Lucemburk: Publications Office, Evropská komise, Generální ředitelství pro komunikační sítě, obsah a technologie, 2019. <https://data.europa.eu/doi/10.2759/0856>. [cit. 1.2.2023]. Dostupné z: <https://op.europa.eu/cs/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1>
- [3.] FELTEN, Ed, Manav RAJ a Robert SEAMANS. *How will language models like ChatGPT affect occupations and industries?* [online]. New York: NYU Stern School of Business, 2023. [cit. 20.6.2023]. Dostupné z: <https://arxiv.org/ftp/arxiv/papers/2303/2303.01157.pdf>
- [4.] *Future of Jobs Report 2023*. [online]. World Economic Forum, 2023. [cit. 20.6.2023]. ISBN–13: 978–2–940631–96–4 Dostupné z: https://www3.weforum.org/docs/WEF_Future_of_Jobs_2023.pdf
- [5.] *Global Risks Report 2021 (16th ed.)*. [online]. World Economic Forum, 2021. [cit. 20.6.2023]. ISBN: 978–2–940631–24–7 Dostupné z: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf
- [6.] GUSKE, Walter. *Umělá Inteligence* [online]. Praha, 2021. Bakalářská Práce. Policejní akademie ČR, Fakulta bezpečnostního managementu, Katedra managementu a informatiky. Vedoucí práce Ing. Bc. Marek Čandík, Ph.D. [cit. 23.2.2023]. Dostupné z: https://pacr-my.sharepoint.com/personal/kmi_polac_cz/_layouts/15/onedrive.aspx?id=%2Fpersonal%2Fkmi%5Fpolac%5Fc%2FDocuments%2FKMI%2FStudijn%C3%AD%20opr%C3%A1ce%20KMI%2F2021%2FBP%2FGuske%20Walter%2FGuske%20Walter%2Epdf&parent=%2Fpersonal%2Fkmi%5Fpolac%5Fc%2FDocuments%2FKMI%2FStudijn%C3%AD%20opr%C3%A1ce%20KMI%2F2021%2FBP%2FGuske%20Walter&ga=1
- [7.] HAMON, Ronan, Henrik JUNKLEWITZ, Jose Ignacio SANCHEZ MARTIN, David FERNANDEZ LLORCA, Emilia GOMEZ GUTIERREZ, Antonio HERRERA ALCANTARA a Akos KRISTON. *Artificial Intelligence in Automated Driving: an analysis of safety and cybersecurity challenges*. Brusel: European Commission [online]. 2022. JRC127189. [cit. 25.2.2023]. Dostupné z: <https://publications.jrc.ec.europa.eu/repository/handle/JRC127189>
- [8.] HNÍK, Václav. *Manažerská informatika*. [online]. Praha: Policejní akademie České republiky v Praze. 2022. ISBN: 974–80–7251–530–1. [cit. 31.5.2023] Dostupné z <https://katalog.polac.cz/Record/POLAC.119852>
- [9.] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. Policejní akademie ČR v Praze a Česká pobočka AFCEA, Praha, 2014, ISBN 978–80–7251–397–0
- [10.] KARÁSKOVÁ, Ivana, Filip ŠEBOK a Veronika BLABLOVÁ. *Čína jako riziko pro bezpečnost výzkumu: doporučení pro akademické a výzkumné*

- institute* [online]. Praha: Asociace pro mezinárodní otázky (AMO), 2022. Analýza (Asociace pro mezinárodní otázky). ISBN: 978–80–88470–17–5. [cit. 26.2.2023]. Dostupné z: https://www.amo.cz/wp-content/uploads/2022/11/HTDTR_cina-jako-riziko-pro-bezpecnost-vyzkumu.pdf
- [11.] KERRY, Cameron F., Joshua P. MELTZER, Andrea RENDA, Alex C. ENGLER, Rosanna FANNI. *Strengthening international cooperation on AI: Progress report*. [online]. The Brookings Institution, 2021. [cit. 20.6.2023]. Dostupné z: https://www.brookings.edu/wp-content/uploads/2021/10/Strengthening-International-Cooperation-AI_Oct21.pdf
- [12.] KOLAŘÍKOVÁ, Linda a Filip HORÁK. *Umělá inteligence a právo*. Praha: Wolters Kluwer, 2020. [cit. 26.2.2023]. ISBN 978–80–7598–783–9.
- [13.] KOLOUCH, Jan., Pavel BAŠTA a kol. *CYBERSECURITY* [online]. Praha: CZ.NIC, 2019. [cit. 26.2.2023]. s.35 ISBN: 978–80–88168–34–8. Dostupné z: <https://knihy.nic.cz/files/edice/cybersecurity.pdf>
- [14.] MATÝS, Tomáš. *Hrozby V Kyberprostoru V Roce 2018* [online]. Praha, 2020. Bakalářská práce. Policejní akademie ČR, Fakulta bezpečnostního managementu, Katedra managementu a informatiky. Vedoucí práce Ing. Bc. Marek Čandík, Ph.D. [cit. 23.2.2023] Dostupné z: https://pacr-my.sharepoint.com/personal/kmi_polac_cz/_layouts/15/onedrive.aspx?id=%2Fpersonal%2Fkmi%5Fpolac%5Fcz%2FDocuments%2FKMI%2FStudijn%C3%AD%20opr%C3%A1ce%20KMI%2F2020%2FBP%2FMat%C3%BDs%20Tom%C3%A1%C5%A1%2FMat%C3%BDs%20Tom%C3%A1%C5%A1%2Epdf&parent=%2Fpersonal%2Fkmi%5Fpolac%5Fcz%2FDocuments%2FKMI%2FStudijn%C3%AD%20opr%C3%A1ce%20KMI%2F2020%2FBP%2FMat%C3%BDs%20Tom%C3%A1%C5%A1&ga=1
- [15.] *Nařízení evropského parlamentu a rady, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (Akt o umělé inteligenci) a mění určité legislativní akty unie* [online]. Brusel: Evropská komise, 21.4.2021. [cit. 1.2.2023] Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A52021PC0206>
- [16.] OSULA, Anna-Maria, Bríd NÍ GHRÁINNE, Dan Jerker B. SVANTESSON, et al. *Cybersecurity law casebook*. Brno: Masaryk University, 2021. ISBN 978–80–210–9773–5.
- [17.] RIGHI, Riccardo, Camila PINEDA LEON, Melisande CARDONA, Josep SOLER GARRIDO, Michail PAPAZOGLU, Sofia SAMOILI a Miguel VAZQUEZ-PRADA BAILLET. *AI Watch Index 2021* [online]. Lucemburk: Publications Office of the European Union, 2022. EUR 31039 EN. ISBN 978–92–76–53602–4. doi:10.2760/921564. JRC128744. [cit. 26.2.2023]. Dostupné z: <https://publications.jrc.ec.europa.eu/repository/handle/JRC128744>

Časopisecké články

- [18.] RECHTIK, Marek. *Kybernetická bezpečnost v automobilovém sektoru. Bezpečnostní Teorie a Praxe* [online]. 2021, roč. 2021, č. 2. Praha. Policejní akademie ČR v Praze. [cit. 25.2.2023]. s.121–132. ISSN 2571–4589. Dostupné z: <https://veda.polac.cz/wp-content/uploads/2021/07/Kyberneticka-bezpecnost-v-automobilovem-sektoru.pdf>

Webové stránky a elektronické zdroje

- [19.] *Abc.xyz: oficiální informační portál společnosti Alphabet, Inc.* [online]. [cit. 23.2.2023]. Dostupné z: <https://abc.xyz>
- [20.] *AI.gov: oficiální informační portál vlády USA* [online]. [cit. 8.2.2023]. Dostupné z: <https://www.ai.gov/>
- [21.] *Alibabagroup.com: informační portál obchodní společnosti Alibaba* [online]. 2023. [cit. 26.2.2023]. Dostupné z: <https://www.alibabagroup.com/en-US/about-alibaba>
- [22.] *Arstechnica.com: informační portál o technických věcech, Gone in 130 seconds. New Tesla hack gives thieves their own personal key* [online]. 06.08.2022. [cit. 23.2.2023]. Dostupné z: <https://arstechnica.com/information-technology/2022/06/hackers-out-to-steal-a-tesla-can-create-their-very-own-personal-key/>
- [23.] *Assets.publishing.service.gov.uk: oficiální informační úložiště britské vlády. National AI Strategy* [online]. 09.2021. [cit. 08.02.2023]. Dostupné z: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwj46eyif38AhXpIYsKHTNFAO0QFnoECAwQAQ&url=https%3A%2F%2Fassets.publishing.service.gov.uk%2Fgovernment%2Fuploads%2Fsystem%2Fuploads%2Fattachment_data%2Ffile%2F1020403%2FNational_AI_Strategy__mobile_version_.pdf&usg=AOvVaw0oHJzJcYsiGgkWE5jE5_66
- [24.] *Baidu.com: informační vyhledávací portál* [online]. 2023. [cit. 26.2.2023]. Dostupné z: <https://ir.baidu.com/company-overview>
- [25.] *Bbc.com: informační portál o všech věcech. MCCALLUM, Shiona. What is AI, is it dangerous and what jobs are at risk?* [online]. 2023. [cit. 20.6.2023]. Dostupné z: <https://www.bbc.com/news/technology-65855333>
- [26.] *Bis.cz: informační portál bezpečnostní informační služby* [online]. [cit. 31.5.2023]. Dostupné z: <https://www.bis.cz/public/site/bis.cz/content/vyrocnizpravy/2021-vz-cz-2.pdf>
- [27.] *Bloomberg.com: mediální informační portál o všech věcech. BASS, Dina a ANAND Priya. OpenAI Is Drawing Competition From Fleet of Startups* [online]. 06. 02. 2023. [cit. 27.2.2023]. Dostupné z: <https://www.bloomberg.com/news/articles/2023-02-06/openai-s-growing-list-of-competitors-anthropic-google-stability-ai-and-more>
- [28.] *Ccdcoe.org: informační portál CCD COE* [online]. [cit. 5.2.2023]. Dostupné z: <https://ccdcoe.org/about-us/>
- [29.] *Czdefence.cz: informační portál o armádních věcech. ŠIŠKA, Martin. Výroční zpráva Vojenského zpravodajství hovoří mimo jiné o fake news* [online]. 11. 10. 2021. [cit. 1.2.2023] Dostupné z: <https://www.czdefence.cz/clanek/vyrocnizprava-vojenskeho-zpravodajstvi-hovori-mimo-jine-o-fake-news>
- [30.] *Databaze-strategie.cz: informační portál databází ČR. Strategie AI České republiky. (2020)* [online]. Ministerstvo průmyslu a obchodu. [cit. 1.2.2023] Dostupné z: <https://www.databaze-strategie.cz/cz/mpo/strategie/narodni-strategie-umele-intelligence-v-cr>
- [31.] *Deviantart.com: oficiální informační portál společnosti* [online]. 2023. [cit. 27.2.2023]. Dostupné z: <https://www.deviantart.com/>
- [32.] *Digital-strategy.ec.europa.eu: oficiální informační portál Evropské unie. Evropská komise. Koordinovaný plán pro umělou inteligenci 2021 – přezkum*

- [online]. Brusel. 30.01.2023. [cit. 1.2.2023]. Dostupné z: <https://digital-strategy.ec.europa.eu/cs/library/coordinated-plan-artificial-intelligence-2021-review>
- [33.] *Digital-strategy.ec.europa.eu: oficiální informační portál Evropské unie. Evropská komise. European Declaration on Digital Rights and Principles* [online]. Brusel. 07.02.2023. [cit. 8.2.2023]. Dostupné z: <https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles>
- [34.] *Digital-strategy.ec.europa.eu: oficiální informační portál Evropské unie. Evropská komise. The European Union and the United States of America strengthen cooperation on research in Artificial Intelligence and computing for the Public Good* [online]. Brusel. 27.01.2023. [cit. 8.2.2023]. Dostupné z: <https://digital-strategy.ec.europa.eu/en/news/european-union-and-united-states-america-strengthen-cooperation-research-artificial-intelligence>
- [35.] *Eur-lex.europa.eu: informační portál Evropské komise. Evropská komise. Sdělení komise evropskému parlamentu Radě. Evropskému hospodářskému a sociálnímu výboru a výboru regionů* [online]. Brusel. 25.4.2018. [cit. 1.2.2023]. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52018DC0237&from=CS>
- [36.] *Eur-lex.europa.eu: informační portál Evropské komise. Rada EU. Rozhodnutí Evropského Parlamentu a Rady (EU) 2022/2481* [online]. Brusel. 19.12.2022. [cit. 1.2.2023]. Dostupné z: <https://eur-lex.europa.eu/eli/dec/2022/2481/oj>
- [37.] *Eur-lex.europa.eu: informační portál Evropské komise. Evropská komise. Nařízení Evropského parlamentu a rady o strojních výrobcích* [online]. Brusel. 21.4.2021. [cit. 1.2.2023]. Dostupné z: https://eur-lex.europa.eu/resource.html?uri=cellar:1f0f10ee-a364-11eb-9585-01aa75ed71a1.0023.02/DOC_1&format=PDF
- [38.] *Europarl.europa.eu: informační portál evropského parlamentu. Umělá inteligence: rizika i příležitosti.* [online]. 2023. [cit. 20.6.2023]. Dostupné z: <https://www.europarl.europa.eu/news/cs/headlines/society/20200918STO87404/umela-inteligence-jake-jsou-vyhody-a-nevyhody>
- [39.] *E15.cz: informační portál o financích, obchodu a byznysu. HORÁKOVÁ, Anna-Marie. Umělá inteligence může zchladit přehřátý trh práce, vznikne ale taky řada nových pozic.* [online]. 2023. [cit. 20.6.2023]. Dostupné z: <https://www.e15.cz/byznys/technologie-a-media/umela-inteligence-muze-zchladit-prehraty-trh-prace-vznikne-ale-taky-rada-novych-pozic-1397681>
- [40.] *Federalregister.gov: informační portál databáze právních spisů Spojených států amerických.* [online]. 2023. [cit. 20.6.2023]. Dostupné z: <https://www.federalregister.gov/documents/2023/03/16/2023-05321/copyright-registration-gAldance-works-containing-material-generated-by-artificial-intelligence>
- [41.] *GARCIA, Naomi. Trade Secrets. Exposing China-Russia Defense Trade in Global Supply Chains* [online]. C4ADS. July 15. 2022. 2022. s. 23 [cit. 26.2.2023]. Dostupné z: <https://c4ads.org/wp-content/uploads/2022/07/TradeSecrets-Report.pdf>
- [42.] *Gov.il: oficiální informační portál izraelské vlády. For the first time in Israel. The principles of the policy for the responsible development of the field of*

- artificial intelligence were published for public comment* [online]. 17.11.2022. [cit.8.2.2023]. Dostupné z: <https://www.gov.il/en/departments/news/most-news20221117>
- [43.] *Glaze.cs.uchicago.edu: informační portál nástroje Glaze univerzity Chicago*. [online]. 2023. [cit. 16.7.2023]. Dostupné z: <https://glaze.cs.uchicago.edu/what-is-glaze.html>
- [44.] *Hamparyan.com: informační portál právníků zaměřených na nehody. Tesla Autopilot Accident Statistics and Other Driver-Assist/Autonomous Driving Technology Crash Data Released* [online]. [cit. 23.2.2023]. Dostupné z: <https://www.hamparyan.com/tesla-autopilot-accident-statistics/>
- [45.] *Insmart.cz: informační portál o IT a všech věcech. IIBOVÁ, Alena. Přijdete o práci kvůli umělé inteligenci? Vědci zveřejnili seznam 5 nejohroženějších povolání*. [online]. 2023. [cit. 20.6.2023]. Dostupné z: <https://insmart.cz/pracovni-pozice-ohrozene-ai/>
- [46.] *It-slovník.cz: slovník IT pojmů* [online]. [cit. 3.2.2023]. Dostupné z: <https://it-slovník.cz/pojem/ddos-utok>
- [47.] *Iso.org: informační portál standardizační instituce. ISO/IEC JTC 1/SC 42 Artificial intelligence*. [online]. 2023. [cit. 20.6.2023]. Dostupné z: <https://www.iso.org/committee/6794475.html>
- [48.] *Iso.org: informační portál standardizační instituce. ISO/IEC 23053:2022 Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)*. [online]. 2023. [cit. 20.6.2023]. Dostupné z: <https://www.iso.org/standard/74438.html>
- [49.] *Keenlab.tencent.com: informační blog společnosti skupiny Keenlab patřící pod Tencent. Car Hacking Research: Remote Attack Tesla Motors* [online]. 19.09.2016. [cit. 23.2.2023]. Dostupné z: <https://keenlab.tencent.com/en/2016/09/19/Keen-Security-Lab-of-Tencent-Car-Hacking-Research-Remote-Attack-to-Tesla-Cars/>
- [50.] *Knowledge.insead.edu: informační portál znalostní instituce. MCLACHLIN, Ruth, Katherine TATARINOV, Tina AMBOS a Phanish PURANAM. Creating People-Centric International Organisations With AI*. [online]. INSEAD Knowledge, 2022. [cit. 20.6.2023]. Dostupné z: <https://knowledge.insead.edu/leadership-organisations/creating-people-centric-international-organisations-ai>
- [51.] *Lupa.cz: informační portál o informačních novinkách a softwaru SEDLÁK, Jan. Locked Shields 2022: Česko opět uspělo na kybercvičení NATO, ale pohoršilo si* [online]. 25. 4. 2022. [online]. [cit. 5.2.2023]. Dostupné z: <https://www.lupa.cz/aktuality/locked-shields-2022-cesko-opet-uspelo-na-kybercviceni-nato-ale-pohorsilo-si/>
- [52.] *Marketwatch.com: informační portál o byznyse a všech věcech. NEWMAN, Daniel. Opinion: Nvidia is AI hardware's growth leader now, but Intel, AMD and others are closing fast*. [online]. 2023. [cit. 20.6.2023]. Dostupné z: <https://www.marketwatch.com/story/nvidia-is-ai-hardwares-leader-now-but-intel-amd-and-others-are-closing-fast-8ad6f23f>
- [53.] *Merriam-webster.com: informační vyhledávací portál* [online]. 2023. [cit. 13.7.2023]. Dostupné z: <https://www.merriam-webster.com/dictionary/superintelligence>

- [54.] *Midjourney.com: oficiální informační portál nezávislé laboratoře společnosti* [online]. 2023. [cit. 27.2.2023]. Dostupné z: <https://www.midjourney.com/home/?callbackUrl=%2Fapp%2F>
- [55.] *Microsoft.com: oficiální informační portál společnosti Microsoft*. KARLIN, Primož. *Classical AI. Umělá inteligence otvírá nové obzory nejen v umění* [online]. 2023. [cit. 27.2.2023]. Dostupné z: <https://news.microsoft.com/cs-cz/features/classical-ai-umela-inteligence-otvira-nove-obzory-nejen-v-umeni/>
- [56.] *Mpost.io: informační portál o všech věcech*. YALALOV, Damir. *7 nejlepších generátorů umění AI roku 2023: Midjourney, DALL-E, NightCafe, Artbreeder* [online]. 25. února 2023. [cit. 27.2.2023]. Dostupné z: <https://mpost.io/cs/7-nejlep%C5%A1%C3%ADch-gener%C3%A1tor%C5%AF-ai-artu-2022-midjourney-dall-e-nightcafe-artbreeder/>
- [57.] *Mvcr.cz: informační portál Ministerstva vnitra* [online]. [cit. 5.2.2023]. Dostupné z: <https://www.mvcr.cz/chh/clanek/specialni-dokumenty-faq.aspx>
- [58.] *Nato.int: oficiální informační portál NATO. Summary of the NATO Artificial Intelligence Strategy* [online]. Brusel. 22.10.2021. [cit. 8.2.2023]. Dostupné z: https://www.nato.int/cps/en/natohq/official_texts_187617.htm
- [59.] *Nato.int: oficiální informační portál NATO*. SNETSELAAR, David, Georg FRERKS, Lauren GOULD, Sebastiaan RIETIENS, Tim SWEIJS. *Knowledge security. Insights for NATO* [online]. Brusel, 30.09.2022. [cit. 8.2.2023]. Dostupné z: <https://www.nato.int/docu/review/articles/2022/09/30/knowledge-security-insights-for-nato/index.html>
- [60.] *Neurazitely.cz: informační portál o kybernetice*. PĚCHOUČEK, Michal. *Umělá Inteligence a život zitrka* [online]. 13.5.2019. [cit. 3.2.2023]. Dostupné z: <https://neurazitely.cz/umela-inteligence-zivot-zitrka-michal-pechoucek>
- [61.] *Nic.cz: informační portál sdružení CZ.NIC* [online]. [cit. 5.2.2023]. Dostupné z: <https://www.nic.cz/page/351/>
- [62.] *Nic.cz: informační portál sdružení CZ.NIC* [online]. [cit. 31.5.2023]. Dostupné z: https://www.nic.cz/files/nic/doc/Koncepce_CZNIC_2020-2024.pdf
- [63.] *Nist.gov: informační portál standardizační instituce Spojených států amerických. Technical AI Standards*. [online]. 2023. [cit. 20.6.2023]. Dostupné z: <https://www.nist.gov/artificial-intelligence/technical-ai-standards>
- [64.] *Nhtsa.gov: oficiální informační portál vládní agentury USA* [online]. [cit. 23.2.2023]. Dostupné z: <https://www.nhtsa.gov/about-nhtsa>
- [65.] *Novinky.cz: informační portál mediální společnosti. Baidu ukáže příští měsíc vlastního chatovacího robota* [online]. 23.2.2023. [cit. 23.2.2023]. Dostupné z: <https://www.novinky.cz/clanek/internet-a-pc-baidu-ukaze-pristi-mesic-vlastniho-chatovaciho-robota-40423800>
- [66.] *Npr.org: informační portál mediální společnosti. Nearly 400 car crashes in 11 months involved automated tech, companies tell regulators* [online]. 15.06.2022. [cit. 23.2.2023]. Dostupné z: <https://www.npr.org/2022/06/15/1105252793/nearly-400-car-crashes-in-11-months-involved-automated-tech-companies-tell-regul>
- [67.] *Nukib.cz: informační portál Národního řádu kybernetické bezpečnosti* [online]. [cit. 5.2.2023]. Dostupné z: <https://www.nukib.cz>

- [68.] *Nukib.cz: informační portál Národního řádu kybernetické bezpečnosti* [online]. [cit. 31.5.2023]. Dostupné z: <https://www.nukib.cz/cs/o-nukib/o-uradu/>
- [69.] *Osveta.nukib.cz: edukační portál Nukibu* [online]. [cit. 1.2.2023]. Dostupné z: <https://osveta.nukib.cz/course/view.php?id=145#section-3>
- [70.] *Policie.cz: informační portál policie ČR* [online]. [cit. 5.2.2023]. Dostupné z: <https://www.policie.cz/clanek/ukonceni-provozu-hotline.aspx>
- [71.] *Policie.cz: informační portál policie ČR* [online]. [cit. 5.2.2023]. Dostupné z: <https://www.policie.cz/clanek/kyber-kampan-nepindej.aspx>
- [72.] *Policie.cz: informační portál policie ČR* [online]. [cit. 5.2.2023]. Dostupné z: <https://www.policie.cz/clanek/kyberkriminalita.aspx>
- [73.] *Ris3.cz: informační portál dotačního programu ČR. Dotační program RIS3 pro podniky a organizace účastníci se AI* [online]. (2023). Ministerstvo průmyslu a obchodu. [cit. 1.2.2023]. Dostupné z: <https://www.ris3.cz/o-ris3/narodni-dimenze/priority/tematicke-vertikalni-prioritydomeny-specializace/tri-dimenze-domeny-vyzkumne-a-inovacni-specializace/klicove>
- [74.] *Stability.ai: oficiální informační portál společnosti STABILITY AI LTD* [online]. 2023. [cit. 27.2.2023]. Dostupné z: <https://stability.ai/>
- [75.] *Stablediffusionlitigation.com: informační portál o soudních sporech a umění. BUTTERICK, Matthew. We've filed a law-suit challenging Stable Diffusion, a 21st-century collage tool that violates the rights of artists. Because AI needs to be fair & ethical for every-one* [online]. 13. 1. 2023. [cit. 27.2.2023]. Dostupné z: <https://stablediffusionlitigation.com/>
- [76.] *Strategie.avcr.cz: webový portál Akademie věd ČR* [online]. [cit. 16.7.2023]. Dostupné z: <https://strategie.avcr.cz/programy/technologie-1>
- [77.] *Sinopsis.cz: informační portál projektu neziskové organizace AcaMedia z.ú. realizovaný za odborné spolupráce s Katedrou sinologie FF UK v Praze. Čínský zákon o celonárodní špionáži* [online]. 27.2.2019. [cit. 26.2.2023]. Dostupné z: <https://sinopsis.cz/cinsky-zakon-o-celonarodni-spionazi/>
- [78.] *Tencent.com: informační portál mediální a investiční společnosti Tencent* [online]. 2023. [cit. 26.2.2023]. Dostupné z: <https://www.tencent.com/en-us/about.html#about-con-1>
- [79.] *Tesla.com: oficiální informační portál společnosti Tesla. Tesla Vehicle Safety Report* [online]. [cit. 23.2.2023]. Dostupné z: <https://www.tesla.com/VehicleSafetyReport>
- [80.] *Tesla.com: oficiální informační portál společnosti Tesla* [online]. [cit. 23.2.2023]. Dostupné z: <https://www.tesla.com/about>
- [81.] *Vortex.cz: informační portál o technických věcech, hrách a umění. SULKOVÁ, Kristýna. Umělci žalují autory AI generátorů kvůli krádežím děl, cílem jsou Stable Diffusion, Midjourney, ale i DeviantArt. Žalobu podalo i Getty Images* [online]. 18. 1. 2023. [cit. 23.2.2023]. Dostupné z: <https://www.vortex.cz/umelci-zaluji-autory-ai-generatoru-kvuli-kradezim-del/>
- [82.] *Youtube.com: oficiální informační portál společnosti Youtube © 2023 Google LLC. HUTCHINS. Marcus. Can ChatGPT Write Malware Better Than Me* [online] 22.01.2023. [cit. 8.2.2023]. Dostupné z: https://www.youtube.com/watch?v=L9w_k2ypRr0

- [83.] *Wikipedia.org: informační portál o všech věcech. Artificial intelligence* [online]. [cit. 26.2.2023]. Dostupné z: https://en.wikipedia.org/wiki/Artificial_intelligence
- [84.] *Wikipedia.org: informační portál o všech věcech* [online]. [cit. 23.2.2023]. Dostupné z: https://en.wikipedia.org/wiki/Tesla,_Inc
- [85.] *Wikipedia.org: informační portál o všech věcech* [online]. [cit. 3.2.2023]. Dostupné z: https://cs.wikipedia.org/wiki/Denial_of_service
- [86.] *Wikiwand.com: doplněk pro wikipedii. informační portál o všech věcech* [online]. [cit. 5.2.2023]. Dostupné z: https://www.wikiwand.com/cs/Centrum_proti_terorismu_a_hybridn%C3%ADm_hrozb%C3%A1m
- [87.] *Wikiwand.com: doplněk pro wikipedii. informační portál o všech věcech* [online]. [cit. 5.2.2023]. Dostupné z: <https://www.wikiwand.com/cs/N%C3%A1rodn%C3%AD%20%C3%BA%C5%99ad%20pro%20kybernetickou%20a%20informa%C4%8Dn%C3%AD%20bezpe%C4%8Dnost>