POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostně-právní

Katedra kriminální policie

Vliv umělé inteligence na činnost zpravodajských služeb

Diplomová práce

The Impact of Artificial Intelligence on the Activities of Intelligence Services

Master Thesis

VEDOUCÍ PRÁCE

doc. JuDr. Ladislav Pokorný, Ph.D.

AUTOR PRÁCE

Bc. Jana Pallová

PRAHA

2024

ČESTNÉ PROHLÁŠENÍ

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

V Praze, dne 15.3.2024

Bc. Jana PALLOVÁ

ANOTACE A KLÍČOVÁ SLOVA

Anotace

Tato práce se zabývá možným využitím umělé inteligence při plnění úkolů zpravodajských služeb a vlivem, jaký toto využití může mít na jejich činnost. Teoretická část práce poskytuje stručný úvod do problematiky umělé inteligence a jejích schopností a omezení. Dále se zabývá zpravodajstvím včetně teorie zpravodajského cyklu a zpravodajskými službami České republiky, jejich působností a úkoly. V empirické části autorka provádí analýzu možných použití umělé inteligence při jednotlivých fázích zpravodajského cyklu a vyjádření jejich dopadů. Na závěr identifikuje jako oblast s největším možným potenciálem pro využití umělé inteligence fázi shromažďování informací, především informací z otevřených zdrojů a jiných technických zpravodajských oborů.

Klíčová slova

umělá inteligence, zpravodajské služby, zpravodajský cyklus, nastupující a přelomové technologie, OSINT, SIGINT, IMINT

Annotation

This thesis deals with the topic of possible use of the artificial intelligence in conducting tasks of the intelligence services and the possible impact of this use on their activities. The theoretical part provides a brief introduction into the issue of artificial intelligence and its abilities and limitations, intelligence including the theory of the intelligence cycle, and the intelligence services of the Czech republic, their competence and tasks. In the empirical part the author conducted an analysis of the possible use of the artificial intelligence within the individual phases of the intelligence cycle. In conclusion the author identifies the collection phase as having the biggest possible potential for the use of artificial intelligence, mostly related to open source intelligence and other technical disciplines.

Keywords

artificial intelligence, intelligence services, intelligence cycle, emerging and disruptive technologies, OSINT, SIGINT, IMINT

OBSAH

1. ÚVOD

V úvodu autorka objasní své důvody pro výběr daného tématu práce a představí cíle a plánovanou strukturu práce.

1.1. Důvody výběru práce

Hlavním důvodem pro výběr tohoto tématu byl zájem autorky o nastupující a přelomové technologie a jejich vliv na oblast bezpečnosti.

O umělé inteligenci jako o technologii, která hraje a bude hrát zásadní roli v otázkách bezpečnosti, se na úrovni NATO již nějakou dobu hovoří.[1] V loňském roce se v Česku poprvé objevil pojem umělá inteligence i v Bezpečnostní strategii České republiky. Otázka jejího využití při zajištění bezpečnosti je v dnešních dnech tedy více než aktuální.

Ačkoliv se čím dál častěji skloňuje využití umělé inteligence ve vojenské sféře nebo v kybernetickém prostoru, její používání dalšími subjekty podílejícími se zajišťování bezpečnosti – konkrétně zpravodajskými službami – je ale v současnosti v České republice stále velmi málo diskutovaným tématem.

Důvodem pro to ale dozajista není fakt, že by umělá inteligence neměla zpravodajským službám při plnění jejich úkolů co nabídnout. Autorka si proto zvolila toto téma práce, aby mohla prozkoumat možný vliv umělé inteligence na činnost zpravodajských služeb, a identifikovat některé oblasti, které by z využívání umělé inteligence mohly nejvíce profitovat.

1.2. Cíle a struktura práce

Cílem této práce je prozkoumat možný vliv umělé inteligence na činnost zpravodajských služeb. Autorka nejprve v práci poskytne teoretický základ v oblasti umělé inteligence a zpravodajských služeb a v empirické části pomocí analýzy identifikuje konkrétní možné aplikace umělé inteligence na plnění úkolů zpravodajských služeb České republiky. Na základě analýzy určí oblasti, ve

[1] READING, D. F., a EATON, J. *Science & Technology Trends 2020-2040* [online]. Brusel: NATO Science & Technology Organization, 2020 [cit. 11.3.2024]. Dostupné z: https://securitydelta.nl/media/com_hsd/report/406/document/190422-ST-Tech-Trends-Report-2020-2040.pdf

kterých by umělá inteligence mohla mít největší dopad na činnost zpravodajských služeb.

V teoretické části autorka představí pojmy a koncepty klíčové pro pochopení obsahu empirické části. Nejprve objasní pojem umělá inteligence, její dělení a vývoj s cílem poskytnout čtenáři bez předchozích znalostí tématu vhled do současných možností umělé inteligence. Dále se v této podkapitole autorka bude zabývat legislativou upravující umělou inteligenci v rámci EU včetně legislativy připravované. Druhá podkapitola představí pojem zpravodajství s cílem přiblížit čtenáři obsah zpravodajské činnosti. Toho bude docíleno především objasněním základních fází tzv. zpravodajského cyklu a rozborem nejvýznamnějších zpravodajských oborů. Na závěr teoretické části autorka vysvětlí pojem zpravodajská služba a představí zpravodajské služby České republiky s důrazem na jejich legislativu, působnost a oprávnění.

V empirické části autorka nejprve poskytne shrnutí cílů, omezení a metod této části. Poté se bude krátce zabývat obecnou premisou využívání umělé inteligence zpravodajskými službami s cílem identifikovat některé možné překážky. Hlavním obsahem empirické části je analýza možných aplikací umělé inteligence při plnění úkolů zpravodajských služeb ČR, a následná identifikace oblastí s největším možným vlivem na plnění těchto úkolů.

Na závěr autorka práci shrne, představí své výsledky a formuluje závěry vyplývající z empirické části práce.

2. TEORETICKÁ ČÁST

V této části práce autorka shrne teoretický základ potřebný pro pochopení empirické části práce. Nejprve představí fenomén umělé inteligence, související pojmy, dělení a legislativu, následně se bude zabývat pojmem zpravodajství v rozsahu klíčovém pro pozdější zpracování analýzy v empirické části, a na závěr teoretické části představí institut zpravodajských služeb s akcentem na zpravodajské služby České republiky.

2.1. Umělá inteligence

Umělá inteligence se především v posledních letech stává čím dál více skloňovaným pojmem. Ze stránek sci-fi románů se ale dokázala přesunout do reálného světa a výrazným způsobem ovlivnit lidské životy. Umělá inteligence dnes kreslí obrazy a píše knihy[2], diagnostikuje onemocnění jako infarkt nebo rakovina plic[3], odhaluje podvodné transakce v bankovnictví[4], chrání náš kyberprostor[5], a mnoho dalšího.

V rámci této podkapitoly se autorka pokusí odpovědět na otázku, co to umělá inteligence je, a nastínit čtenáři některé druhy jejího dělení a současný stav vývoje umělé inteligence. V závěru podkapitoly shrne současný a připravovaný legislativní rámec umělé inteligence v EU.

2.1.1. Definice umělé inteligence

Myšlenka strojů, které jsou schopné vykazovat znaky myšlení, chování a rozhodování srovnatelného s lidmi, není nic nového. S pojmem **umělá**

[2] DAVENPORT, Thomas H. a MITTAL, Nittin. How Generative AI Is Changing Creative Work. *Harvard Business Review* [online]. 14.11.2022 [cit. 8.2.2024]. Dostupné z: https://hbr.org/2022/11/how-generative-ai-is-changing-creative-work

[3] KWINT, Jemma. Artificial intelligence: 10 promising interventions for healthcare. *National Institute for Care and Health Research Evidence* [online]. Červenec 2023 [cit. 8.2.2024]. Dostupné z: https://evidence.nihr.ac.uk/collection/artificial-intelligence-10-promising-interventions-for-healthcare/

[4] NUNN, Jeremy. How AI And Machine Learning Help Detect And Prevent Fraud. *Forbes* [online]. 1.11.2023 [cit. 8.2.2024]. Dostupné z: https://www.forbes.com/sites/forbestechcouncil/2023/11/01/how-ai-and-machine-learning-help-detect-and-prevent-fraud/

[5] AI and Cybersecurity: A New Era. *Morgan Stanley* [online]. 15.9.2023 [cit. 8.2.2024]. Dostupné z: https://www.morganstanley.com/articles/ai-cybersecurity-new-era

inteligence (*Artificial Intelligence, AI*) přišel v roce 1955 Professor John McCarthy[6]. Podle něj se jednalo o "používání vědy a inženýrství k vytváření inteligentních strojů". Tato definice tedy přímo souvisí pouze s vlastnostmi systémů, vyplývající z obsahu slova "inteligence". Ta je nejčastěji definována jako schopnost se učit a pracovat způsobem umožňujícím řešení problémů a dosahováním cílů správným způsobem s ohledem na velkou míru nejistoty v reálném světě.

V dnešní době je ale pojem umělá inteligence užíván v mnohem širším kontextu, a ani v rámci akademické obce neexistuje jasná shoda na tom, co je umělá inteligence a co ne. Různé myšlenkové proudy v rámci výzkumu inteligentních systémů kladou rozdílný důraz na schopnost těchto systémů konat inteligentně, vykazovat znaky inteligentního myšlení, a nebo se ve svém chování či myšlení co nejvíce přibližovat lidským bytostem i s uvážením prvků emoční a sociální inteligence.

Některé další definice pak přímo souvisí s použitím algoritmů v rámci inteligentních systémů, které umožňují nápodobu fungování lidského mozku (např. umělé neurální sítě) nebo učení způsobem podobným lidem (např. *unsupervised learning*).

Pro účely této práce není nezbytné se touto definiční nejednoznačností dlouze zabývat. Postačí, když za umělou inteligenci budeme považovat vše, co s využitím těchto specifických algoritmů svými schopnostmi vnímání, učení, vyvozování a rozhodování překračuje schopnosti klasických počítačových programů.

2.1.2. Základní pojmy související s umělou inteligencí

S dnešním vnímáním umělé inteligence se pojí některé pojmy, se kterými bude možné se v práci dále setkat. Tato kapitola poskytne jejich krátké vysvětlení.

Autonomní systémy (*Autonomous Systems*) jsou systémy, které jsou schopné se nezávisle rozhodovat a plánovat své další kroky za účelem dosažení

[6] ANDRESEN, S.L. John McCarthy: Father of AI. *Intelligent Systems*. IEEE, 2002, 17(5):84 – 85. DOI: 10.1109/MIS.2002.1039837.

stanoveného cíle bez nutnosti využití rozhodovacích stromů k mikromanagementu tohoto postupu. Pojem “autonomní” se v tomto kontextu nevztahuje k míře sebeuvědomění a sebeřízení ve smyslu stanovování svých vlastních cílů.

Strojové učení (*Machine Learning, ML*) je část umělé inteligence, která se zabývá výzkumem učení na základě předchozích dat nebo zkušeností. Tento proces učení rozvíjí nejen schopnost rozhodování, ale i vnímání, myšlení nebo utváření znalostí. Strojové učení staví především na poznatcích z informatiky, ale i neurovědy, psychologie, statistiky nebo ekonomie.

Hluboké učení (*Deep Learning, DL*) je pak specifickým typem strojového učení, které využívá umělé neurální sítě ve snaze se co nejvíce přiblížit lidskému způsobu myšlení. Jedná se o v současnosti nejúspěšnější metodu strojového učení, použitelná takřka v každé aplikaci strojového učení. Její největší výhodou je výrazná schopnost generalizace a učení se na relativně menších datasetech, což snižuje nároky na čas a výpočetní kapacitu.

Umělé neurální sítě (*Artificial Neural Networks, ANN*) jsou specifickým typem výpočetní architektury, vycházejícím z poznatků neurovědy o fungování lidského mozku. Základními výpočetními jednotkami jsou neurony, uspořádané do vrstev. Neurony z různých vrstev mezi sebou komunikují a zajišťují přenos informací a transformaci dat ze vstupní vrstvy po výstupní za pomocí vah, které jsou v každém neuronu přiřazeny některé ze vstupních hodnot. Hlavní výhodou tohoto přístupu je schopnost neurálních sítí přirozeně postihnout nelinearitu vztahů mezi vstupy a výstupy a variabilita v postupech trénování sítí, což umožňuje jejich využití v široké škále případů (od rozpoznávání objektů na fotkách a generování textu po nalézání výherních strategií ve hrách).[7]

2.1.3. Druhy umělé inteligence

Jedním z nejvýznamnějších dělení umělé inteligence je podle jejích schopností na slabou a silnou AI.[8]

---

[7] MANNING, CHRISTOPHER. *Artificial Intelligence Definitions* [online]. Stanford University, 2020. Dostupné z: https://hai.stanford.edu/sites/default/files/2020-09/AI-Definitions-HAI.pdf

[8] RAIKOV, A. N. Weak Vs. Strong Artificial Intelligence. *Informatization and Communication*. 3/2020. DOI: 10.34219/2078-8320-2020-11-1-81-88.

Slabá, někdy také **úzká umělá inteligence** (*Weak or Narrow AI*) se vyznačuje tím, že je schopná plnit jen úzký okruh úkolů – tedy ty, na které je přímo určená a na které byla přímo natrénována. Při plnění těchto úkolů AI vykazuje vlastnosti, které jsou běžně přisuzovány pouze lidem (příp. zvířatům) jako vnímání, učení se z předchozích zkušeností a odůvodněné rozhodování. Slabá umělá inteligence najde uplatnění téměř ve všech systémech využívajících počítačovou algoritmizaci – od jednoduchých spam filtrů, programů na rozpoznávání objektů, generativní AI až po virtuální asistenty a inteligentní systémy pro podporu rozhodování. I přes svůj název je některá slabá AI ve svých úkolech schopná překonat člověka – příkladem je program Deep Blue, který byl již v roce 1997 schopen ve hře šachu porazit úřadujícího světového šampiona Garryho Kasparova.[9]

I přes pokročilost některých komplexních AI systémů – například zmíněných virtuálních asistentů jako Alexa od Amazonu nebo Siri od Applu nebo generativní AI jako ChatGPT – je všechna umělá inteligence, kterou máme v současnosti k dispozici, dle tohoto dělení slabá. Není tedy v zásadě schopná plnit jiné než předem určené úkoly a přenášet své znalosti a zkušenosti do použití k jiným účelům.

Silná nebo také **obecná umělá inteligence** (*Strong or General AI, GAI*) někteří autoři považují za další krok ve vývoji AI, někteří za koncept naprosto odlišný od dnešní AI. Silná umělá inteligence by měla být schopna plnit veškeré úkoly, kterých je člověk schopen, na úrovni s ním srovnatelné. Stejný program by tedy měl být schopen například vést konverzaci s použitím knihovny znalostí a zpracování přirozeného jazyka, pak vyřešit křížovku, udělat optimální rozhodnutí ohledně položek v inventáři a nakonec nakreslit obraz podle zadání.

Taková umělá inteligence v současnosti neexistuje a je otázkou, jestli někdy v budoucnosti bude dosaženo jejího sestrojení. Objevují se i hlasy, které říkají, že obecné umělé inteligence pravděpodobně nikdy dosaženo nebude.[10] Ačkoliv je velmi těžké vytvářet jakékoliv predikce, je velmi pravděpodobné, že

[9] Deep Blue. *IBM* [online, cit. 9.2.2024]. Dostupné z: https://www.ibm.com/history/deep-blue

[10] LIU, Bin. "Weak AI" is Likely to Never Become "Strong AI", So What is its Greatest Value for us?. *ArXiv: Artificial Intelligence* [online]. 29.3.2021 [cit. 9.2.2024]. Dostupné z: https://doi.org/10.48550/arXiv.2103.15294

i pokud by obecné umělé inteligence někdy dosaženo bylo, jedná se spíše o otázku následujících dekád než nejbližších let.

V některých případech je možné narazit i na pojem **super umělá inteligence**.[11] Označuje AI systém, který by nejen byl schopen vykonávat veškeré činnosti a plnit úkoly jako člověk, ale byl by schopen ve všech těchto úkolech dosahovat lepších výsledků, než člověk. Častou vlastností, která je mu přisuzována na základě takto rozvinutých kognitivních schopností, je **pocit sebeuvědomění**. Ten doprovází schopnost vykazovat další typy inteligence jako emocionální nebo sociální nebo schopnost vytvářet si vlastní názory, přesvědčení a přání.

Sestrojení takového konceptu je úzce navázáno na sestrojení obecné umělé inteligence a v současnosti nepředstavitelné.

2.1.4. Vývoj umělé inteligence

Umělá inteligence od svých počátků v 50. letech minulého století ušla dlouhou cestu až k technologiím, které známe dnes. Pro poskytnutí kontextuálního povědomí o vývoji AI bez dlouhého historického výkladu autorka zvolila teorii o třech vlnách umělé inteligence.[12]

Podstatou první vlny umělé inteligence, nazývané jako **ručně zpracované znalosti** (*Handcrafted Knowledge*) nebo **expertní systémy** (*Expert Systems*), byly **znalosti**. Tyto systémy byly schopné využívat expertních znalostí, které jim byly poskytnuty, k logickému rozhodování při řešení problémů. AI z této vlny byla schopná dosahovat velmi dobrých výsledků v úzkém okruhu úkolů ve velmi stabilním a neměnném prostředí. Znalost tohoto prostředí a pravidel, podle kterých se toto prostředí řídilo, postačily k tomu, aby tyto systémy v těchto úkolech byly schopné překonávat člověka. Typickým příkladem AI z první vlny jsou například programy na hraní her (jako výše zmíněný Deep Blue v šachu) nebo třeba programy na výpočet daní. Nevýhodou těchto systémů bylo, že zcela

[11] KANADE, Vijay. What Is Super Artificial Intelligence (AI)? Definition, Threats, and Trends. *SpiceWorks* [online]. 11.3.2022 [cit. 9.2.2024]. Dostupné z: https://www.spiceworks.com/tech/artificial-intelligence/articles/super-artificial-intelligence/

[12] LAUCHBURY, John. A DARPA Perspective on Artificial Intelligence. *Defense Advanced Research Projects Agency* [online, cit. 10.2.2024]. Dostupné z: https://www.darpa.mil/attachments/AIFull.pdf

postrádají schopnost vnímat, učit se, přizpůsobit změně prostředí nebo operovat s vyšší mírou nejistoty.

Druhá vlna umělé inteligence nastala s příchodem strojového učení. **Statistické učení**, jak je tato vlna také nazývána, umožnilo systémům velmi dobré vnímání okolního světa. Krom svých přímých zkušeností se AI druhé vlny může učit i z datasetů. Postrádá ale schopnost logického odůvodňování a rozhodování předchozí vlny. Tyto systémy jsou tedy velmi dobré v poznávání, třídění a nalézání vzorců ve velkém množství informací, pokud jim je poskytnut kontext, ale nejsou schopné tento kontext "pochopit" nebo na základě něho dále operovat. Přesto se jedná o výkonné systémy, které proměňují dnešní svět, jako třeba automatické odemykání obrazovky na základě obličeje, hlasové ovládání, programy na odhalení podvodů v bankovních transakcích, ochrana počítačových systémů před kybernetickými útoky, a další.

Třetí vlna by do budoucna měla představovat kombinaci silných stránek obou předchozích vln – schopnosti logického odůvodňování a rozhodování první vlny se schopností vnímání, učení a předvídání vlny druhé. Výrazným krokem vpřed by měla být i schopnost **kontextuální adaptace**, tedy porozumět kontextu informací, které jsou systému předkládány, a schopnost na základě tohoto porozumění operovat. Rozdíl mezi algoritmem druhé a třetí vlny lze demonstrovat například na procesu rozpoznávání objektu na obrázku.[13] Algoritmus druhé vlny vyhodnotí, že na obrázku se nachází kočka, protože udělá výpočet přes všechny pixely obrázku a na základě předchozího učení sestaví žebříček pravděpodobností možných objektů, na jejímž vrcholu je kočka. Pokud by ten stejný obrázek dostal algoritmus z třetí vlny, měl by vyhodnotit, že se jedná o kočku, protože na obrázku je malý savec s packami, ušima, kožešinou, ocasem a dalšími atributy, které přísluší kočce – tedy provést identifikaci stejným způsobem, jako by ji prováděl člověk.

Krom pochopení kontextu je tedy výraznou vlastností AI systémů třetí vlny i přiblížení se ve svých postupech k myšlení člověka. Základem by měla být

[13] ZARAKI, Abolfazl. An excellent talk from DARPA on the three waves of Artificial Intelligence (AI) – The Contextual Adaptation is the right direction to go: Explainable AI. *Cardiff University Blogs* [online]. 18.7.2020 [cit. 10.2.2024]. Dostupné z: https://blogs.cardiff.ac.uk/ai-robotics/an-excellent-talk-on-the-three-waves-of-artificial-intelligence-ai-the-contextual-adaptation-is-a-way-to-go-explainable-ai/

schopnost učení z poskytnutých datasetů, věrně kopírující reálné situace, spolu se schopností vnímat případné změny a nuance. Dalším pokrokem by měl být důraz na schopnost abstrakce, tedy přenášení zkušeností z původních situací do nových, a zobecňování poznatků získaných při trénování na datasetech. Všechny tyto schopnosti by měly sloužit především jako základ pro rozhodování v neznámých prostředích nebo s vyšší mírou nejistoty. V případě rozhodnutí by měl být schopen poskytnout dostatečně podrobné a jednoduché vysvětlení svých kroků, aby mu člověk mohl porozumět.

2.1.5. Právní rámec umělé inteligence

V případě umělé inteligence můžeme vidět, že nastupující a přelomové technologie se často vyvíjí a začínají prakticky aplikovat dříve, než je možné je v rámci legislativního procesu na úrovni států nebo nadnárodních celků ošetřit. To s sebou přináší jistá úskalí, kdy technologie po určitou dobu existují v jakémsi právním vakuu – současná legislativa se na ně buď nevztahuje, nebo postihuje pouze některé aspekty těchto technologií (v případě umělé inteligence třeba GDPR[14]) nebo jen některé jejich využití (např. NIS2[15]), a nová legislativa, která se problematikou této technologie zabývá, ještě není platná nebo účinná.

S rostoucím vlivem této technologie pak roste tlak na legislativce pro přijetí zákonných opatření, ale zároveň v důsledku rychlého vývoje technologie tyto zákony často musí být měněny v průběhu jejich přijímání, aby postihovaly danou technologii v co nejširší míře. To legislativní proces dále zpomaluje (např. otázka ChatGPT v AIA).

Proto není divu, že komplexní legislativa týkající se umělé inteligence je v současnosti stále ve většině států buď neexistující, nebo v procesu vytváření nebo přijímání. Existující legislativní normy týkající se AI jsou většinou velmi

[14] European Parliament Research Service. The impact of the General Data Protection Regulation (GDPR) on artificial intelligence. *European Parliament* [online]. Červen 2020 [cit. 12.2.2024]. Dostupné z: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf

[15] ALLEN, John. The Implications of NIS2 on Cyber Security and AI. *DarkTrace* [online]. 5.12.2023 [cit. 12.2.2024]. Dostupné z: https://darktrace.com/blog/the-implications-of-nis2-on-cyber-security-and-ai

úzce zaměřené a mají za cíl “překlenout” období tohoto legislativního vakua, než bude přijata nějaká komplexní legislativa.

Cílem této kapitoly je představit čtenáři současnou legislativní situaci ohledně umělé inteligence na úrovni Evropské unie včetně plánovaného evropského Artificial Intelligence Act.

2.1.5.1. Legislativní úprava umělé inteligence v Evropské unii

Není neobvyklé, že se Evropská unie stává průkopníkem v přinášení komplexní legislativy s primárním cílem chránit evropské občany i za cenu omezování některých práv právnických osob nebo jiných organizací. Příkladem může být třeba již zmíněné **Obecné opatření o ochraně osobních údajů** (*General Data Protection Regulation, GDPR*), které ve své době nemělo ve světě obdoby. Je to jednou z ukázek toho, že v případě přijímané evropské legislativy je spíše kladen důraz na bezpečnost než absolutní svobodu.

Jinak tomu není ani v případě legislativy ohledně umělé inteligence. Ta se začala rodit v dubnu 2018, kdy byla zveřejněna **Evropská strategie pro umělou inteligenci** (*European Strategy for AI*). Na základě té byla v únoru 2020 Evropskou komisí vydána **Bílá kniha o umělé inteligenci** (*White Paper on Artificial Intelligence*),[16] ve které Komise představila svůj návrh přístupu k AI. Ten rozdělila na dva “ekosystémy” – **ekosystém excelence**, v rámci kterého navrhovala podporu rozvoje a výzkumu umělé inteligence na akademické i podnikové úrovni, včetně podpory start-upů, a **ekosystém důvěry**, který vymezil klíčové prvky budoucích omezení týkajících se umělé inteligence s cílem zajistit dodržování evropské legislativy.[17] Spolu s Bílou knihou byly otevřené i veřejné konzultace, kdy měli všichni občané EU, zástupci členských států a jiných zainteresovaných stran včetně občanského společenství, firem a akademické sféry možnost vyjádřit se k navrhovanému přístupu.

[16] White Paper on Artificial Intelligence: a European approach to excellence and trust. *European Commission* [online]. 19.2.2020 [cit. 12.2.2024]. Dostupné z: https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

[17] WAHL, Thomas. Commission: White Paper on AI. *Eucrim* [online]. 1.4.2020 [cit. 12.2.2024]. Dostupné z: https://eucrim.eu/news/commission-white-paper-ai/

V dubnu 2021 zveřejnila Komise návrh na regulaci umělé inteligence v EU. To zahájilo roky dlouhé vyjednávání zainteresovaných stran včetně Komise a Evropského parlamentu a jeho výborů. Zatím poslední krok k přijetí nařízení, nazvaného **Zákon o umělé inteligenci** (*Artificial Intelligence Act, AIA*), proběhl 9. prosince 2023, kdy Parlament a Rada EU dospěly k předběžné dohodě o podobě zákona.[18] K finální dohodě obou těchto legislativních institucí a přijetí AIA by mělo dojít v průběhu roku 2024. Pokud se tak stane, dá se očekávat, že zákon bude platný od roku 2025.

2.1.5.2. Artificial Intelligence Act

Konečný návrh AIA rozděluje systémy využívající umělou inteligenci podle rizika, které představují, do čtyř kategorií – neakceptovatelné, vysoké, omezené a minimální. Povinnosti poskytovatelů systému se odvíjí od zařazení do jedné z těchto kategorií. Zvláštní kategorii pak tvoří tzv. ***general purpose artificial intelligence*** (univerzální systémy používající umělou inteligenci, *GPAI*).[19]

Systémy využívající AI představující **neakceptovatelné riziko** budou až na výjimky zakázány. Jedná se především o systémy, které

a) používají klamných nebo manipulativních technik k ovlivnění chování nebo rozhodování jedinců,

b) zneužívají zranitelností osob s ohledem na jejich věk, postižení nebo socioekonomickou situaci,

c) využívají biometrické údaje ke kategorizaci,

d) zajišťují sociální bodování,

e) sestavují databáze k rozpoznávání obličejů z necílených kamerových záznamů nebo internetu,

f) využívají algoritmy na rozpoznávání emocí na pracovištích a vzdělávacích institucí (s výjimkou zdravotních a bezpečnostních důvodů).

Dále do této kategorie patří i vzdálená identifikace na základě biometrických údajů (tzn. rozpoznávání obličejů) na veřejně přístupných místech

[18] Developments. *EU Artificial Intelligence Act* [online, cit. 12.2.2024]. Dostupné z: https://artificialintelligenceact.eu/developments/

[19] AI Act Overview. *Artificial Intelligence Act* [online]. 24.1.2024 [cit. 13.2.2024]. Dostupné z: https://artificialintelligenceact.eu/wp-content/uploads/2024/01/AI-Act-Overview_24-01-2024.pdf

a v reálném čase law enforcement složkami. Výjimku tvoří pátrání po pohřešovaných osobách, případy, kdy je to nutné z důvodu předcházení podstatné a přímo hrozící hrozbě (např. teroristický útok) nebo identifikace pachatelů závažné trestné činnosti. Tyto výjimky jsou dále omezené např. registrací daného systému nebo získáním předchozího povolení soudce.

Systémy využívající AI představující **vysoké riziko** jsou sice pod AIA povoleny, zákon ale dává jejich poskytovatelům a provozovatelům řadu povinností, které mají za cíl toto riziko mitigovat. Extenzivní výčet těchto systémů se nachází v Dodatku III AIA a jedná se především o použití

a) v systémech zpracovávajících biometrická data,
b) v kritické infrastruktuře,
c) ve vzdělávání a odborné přípravě,
d) v zaměstnání a přístupu k zaměstnání,
e) pro přístup k základním službám,
f) v oblasti vymáhání práva (*law enforcement*),
g) v oblasti migrační a azylové politiky a ochraně státních hranic,
h) v oblasti výkonu spravedlnosti (soudnictví) a jiných demokratických procesů (např. při volbách).

Zároveň do této kategorie patří všechny systémy, které zpracovávají osobní údaje pro účely profilování osob z hlediska různých aspektů lidského života jako jsou pracovní výkony, ekonomická situace, zdraví, chování atd.

U systémů představujících vysoké riziko musí po celou dobu jejich životního cyklu probíhat **řízení rizik**. Důraz je kladen na data, na kterých je umělá inteligence trénována, ověřována a testována – především na **relevantnost**, **dostatečnou reprezentativnost** a **bezchybnost dat**. Ke každému takovému systému musí být zpracována **technická dokumentace**, ve které provozovatel dokazuje dodržování povinností vyplývajících ze zákona. Z provozu těchto systémů se musí **uchovávat záznamy** tak, aby bylo umožněno automatické zaznamenávání událostí relevantních pro identifikaci rizik a souvisejících se změnami v průběhu životního cyklu systému. V neposlední řadě tyto systémy musí splňovat nároky na **přesnost**, **robustnost**, **kybernetickou bezpečnost** a musí podléhat **lidskému dozoru**.

Na systémy představující **omezené riziko** budou kladeny pouze minimální požadavky na transparentnost. Jejich cílem je, aby bylo konečnému uživateli vždy jasné, že v rámci systému interaguje s umělou inteligencí nebo ji jinak využívá. Jedná se především o aplikace jako jsou chatboti nebo deepfakes.

Systémy představující **minimální riziko** nebudou tímto zákonem nijak regulovány. Jedná se o většinu aplikací AI, které v současnosti lze na evropském trhu nalézt, jako třeba spam filtry nebo umělá inteligence v počítačových hrách.

Velkou změnu do přípravy AIA přinesl příchod ChatGPT a s ním dalších GPAI a generativní AI. Po identifikaci nutnosti byla vytvořena pro tyto systémy vlastní kategorie omezení a povinností v rámci AIA.

Provozovatelé těchto systémů musí připravit **technickou dokumentaci**, která bude zahrnovat proces trénování a testování a výsledky hodnocení systému, a **dokumentaci a informace pro navazující dodavatele**, kteří tyto systémy mohou integrovat do vlastních produktů s cílem předat kompletní přehled schopností a omezení systému a umožnit dodržování povinností vyplývajících ze zákona. Dále jsou provozovatelé povinni zajistit dodržování **Směrnice o autorských právech** a zveřejnit dostatečně podrobný přehled obsahu, na kterém byl daný systém trénován.

Další povinnosti mají provozovatelé GPAI systémů, které naplňují podmínku **systémovosti**. Ta je dána výpočetní kapacitou použitou pro trénování modelu. Tyto systémy musí projít **hodnocením**, včetně provádění a zaznamenávání negativního testování s cílem snížit rizika, která systém může představovat. Dále musí **vyhodnocovat a mitigovat systematická rizika**, včetně jejich zdrojů. Systémy musí také **sledovat, zaznamenávat a oznamovat bezpečnostní incidenty** a způsoby, jakými byly vyřešeny, příslušným národním autoritám. V neposlední řadě musí provozovatel zajistit dostatečnou **kybernetickou ochranu** systému.

Po nabytí platnosti zákona budou mít provozovatelé systémů využívajících AI lhůtu na to, zajistit dodržování povinností z něj vyplývajících. Tyto lhůty se liší podle typu systému. Pro systémy představující neakceptovatelné riziko to je 6 měsíců, pro GPAI systémy 12 měsíců, a pro systémy představující vysoké riziko 24 až 36 měsíců v závislosti na typu systému.

2.2. Zpravodajství

Už od počátku věků platilo, že vědět znamená mít výhodu nad ostatními a přežít. Informace byly to, co nejdříve v prvních populacích zajišťovalo získání obživy, vody a úkrytu a umožnilo vyhnout se nebezpečí. S rozvojem civilizací a vznikem lidských společenství význam informací ještě stoupl. Vědět znamenalo mít moc nad ostatními a zajistit své místo ve společnosti a naplnění svých cílů.

Záměrné získávání informací za účelem zajištění převahy nad protivníkem se objevilo s usazováním populací a kladením si nároků na tato území, a přirozenou potřebou je bránit před jinými, nebo naopak uzmout území či přírodní zdroje někomu dalšímu – tedy s rozvojem něčeho, co bychom mohli nazvat za počátek válčení. Tyto boje už nebyly jen přímé, bezprostřední střety s jinými skupinami s cílem přežít, ale objevily se prvky rozvahy a plánování. Pro tyto procesy jsou klíčové informace – o pozici, síle a vybavení nepřítele, ale i o jeho pohybech a záměrech. Vědět tedy opět představovalo rozdíl mezi životem a smrtí.

Potřeba informací se pak ještě umocnila se vznikem prvních státních útvarů. Pro udržení svrchované moci nad územím a obyvatelstvem bylo třeba nejen shromažďovat informace o možných vnějších nepřátelích, kteří se mohli pokusit stát napadnout, ale i o hrozbách pramenících zevnitř samotného státu. Tato činnost musela být nejen záměrná, ale bylo třeba ji začít organizovat a provádět systematicky. Začaly tedy vznikat první státní složky nebo organizace, které by dnes šlo považovat za zpravodajské služby.

Tato potřeba vědět plně přetrvává do dnešních dní, a z původní potřeby se vyvinul celý obor zpravodajství, který se v širším pohledu zabývá vším, co souvisí s potřebou informací – od zadání přes shromažďování a vyhodnocování až po předávání tak, aby tyto informace mohly sloužit k rozhodovacím procesům vedoucích osob na různých místech a úrovních státní správy.

V rámci této kapitoly autorka poskytne krátký rozbor definice zpravodajství a souvisejících základních pojmů, a pro potřeby praktické části rozebere jednotlivé fáze zpravodajského procesu a zpravodajské obory.

2.2.1. Definice zpravodajství

Pro pojem **zpravodajství** neexistuje jednotná definice. Ačkoliv v českém jazyce "zpravodajství" evokuje primárně informační činnost novinářů a médií, v kontextu bezpečnosti se jedná o pojem významově shodný s anglickým ***intelligence***.

Tento samotný pojem je do jisté míry vícevýznamový. Kromě vyjádření zpravodajské činnosti, tedy procesu získávání a zpracovávání informací, může pojem *intelligence* znamenat i výsledek této činnosti, čili samotnou zpravodajskou informaci získanou a vyhodnocenou na základě zpravodajského požadavku, nebo zpravodajskou službu či organizaci, tedy organizovanou složku zabývající se prováděním zpravodajské činnosti.[20] Je tedy třeba být poměrně pozorný při určování správného významu pojmu v daném kontextu.

V rámci této práce autorka představí několik definic pojmu zpravodajství.

První z definic vychází z **Terminologického slovníku pojmů a definic NATO** (*NATO Glossary of Terms and Definitions, AAP-6*). Její přítomnost zde je nasnadě – jelikož je Česká republika zemí NATO a Severoatlantická aliance hraje významnou roli v bezpečnosti ČR nejen na strategické úrovni, tato definice je zavedena i v rámci ČR.

"Produkt vzniklý zpracováním informací, které se týkají cizích zemí, vojsk nebo jejich částí u protivníka nebo potenciálního protivníka, prostorů současných nebo potenciálních operací. Tento pojem se také používá ve vztahu k činnosti, v důsledku které vzniká tento produkt a organizacím, které se zabývají podobnou činností."[21]

Tato definice zmiňuje mimo jiné i možnou mnohoznačnost pojmu, jak bylo demonstrováno výše.

Trochu odlišnou definici pak lze nalézt i ve **Společné spojenecké doktríně zpravodajství, kontrazpravodajství a bezpečnosti** (*Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security, AJP-2*).

---

[20] SHULSKY, A. N. a SCHMITT, G. J. *Silent Warfare: Understanding the World of Intelligence*. Washington, D. C.: Brassey's, Inc., 2002. ISBN 978-15-7488-345-9. Str. 1–3.

[21] APP-6. Terminologický slovník pojmů a definic NATO. Praha, 2002.

“Pojem zpravodajství (Intelligence) je definován jako produkt, vycházející z řízeného shromažďování a zpracování informací vztahujících se k prostředí, schopnostem a záměrům aktérů s cílem identifikovat hrozby a navrhnout možnosti řešení pro funkcionáře s rozhodovací pravomocí.”[22]

Tato definice již zmiňuje dvě z konkrétních součástí zpravodajského procesu – shromažďování a zpracovávání informací – a zdůrazňuje roli zpravodajství jako nezastupitelné složky v rozhodovacím procesu vedoucích osob.

Poslední zmíněná definice nevychází z Aliančních dokumentů, ale jedná se o definici českou, pocházející z publikace Petra Zemana.[23]

“Zpravodajství je záměrná a systematická lidská činnost, která zahrnuje všechny fáze utajovaného získávání a zpracovávání utajených či latentních informací protihráče či protivníka a dále následné jejich předání oprávněnému příjemci. Jejich účelem je odpovědět na relevantní otázky a/nebo získat včasné varování, potřebné k naplánování a uskutečnění budoucích kroků. Součástí zpravodajské činnosti jsou aktivity chránící vlastní utajované skutečnosti. Jeho součástí také mohou být utajené preventivní a aktivní zásahy do protivníkova prostředí.”

Tato definice, na rozdíl od předchozích, klade důraz na **utajenost** procesu zpravodajství i získávaných informací. Rovněž představuje i myšlenku, že součástí zpravodajství je i **ochrana vlastních utajovaných informací** před zpravodajskou činností cizích subjektů.

2.2.2. Vysvětlení pojmů data, informace a zpravodajská informace

Ústřední roli ve zpravodajství hrají informace. Tento pojem je ale často používán v širším kontextu a zaměňován významově s pojmem data a zpravodajská informace. V této kapitole autorka vysvětlí jednotlivé pojmy, rozdíly a vztahy mezi nimi.

---

[22] AJP-2. Spojenecká společná doktrína zpravodajství, kontrazpravodajství a bezpečnosti, Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security (Edition B, Version 1, vydání 2020).

[23] ZEMAN, P. *Co je zpravodajství* [online]. Květen 2008 [cit. 14.2.2024]. Dostupné z: http://www.absd.sk/co_je_ zpravodajstvi

Základním stavebním kamenem jsou **data**. Ta jsou nejčastěji výsledkem pozorování nebo měření a objektivně popisují jevy nebo vlastnosti pozorovaného objektu.[24] Data představují soubor vlastností těchto objektů, které jsou vhodně převedeny do čísel, písmen nebo jiné vhodné podoby, která umožňuje jejich zaznamenání, uchování a zpracování. Z dat lze tvořit databáze, ve kterých je možné pomocí vhodných nástrojů vyhledávat.

Data lze dělit na strukturovaná a nestrukturovaná. **Strukturovaná data** představují většinou číselné údaje, které lze zaznamenávat v tabulkách a vyhodnocovat běžnými matematickými a statistickými metodami, což umožňuje jejich automatizované vyhodnocování. **Nestrukturovaná data** jako obrázky, fotografie nebo audio soubory musí být pro případy automatizovaného vyhodnocování popsány metadaty, v opačném případě musela do nedávna být vyhodnocována člověkem. V praxi je jich mnohem více, než strukturovaných dat.

Příklady dat mohou být seznam IP adres, ze kterých byla navštívena internetová stránka, počet osob, které v pozorované době vstoupily do zájmového objektu, množství vyslaných signálů, fotografie pořízené během sledování atd.

Informace jsou základním materiálem pro vytváření zpravodajských výstupů, a jsou tvořeny jedním nebo více soubory dat, kterým byl dán nějaký význam nebo byly zasazeny do určitého kontextu. To znamená, že informace jsou vždy vázány na osobu příjemce – tedy toho, kdo s těmito daty pracuje. Dva různí lidé s odlišným vzděláním a zkušenostmi mohou ze stejných dat vyvodit odlišné informace.

Samotné informace ale nemohou být vlastním výstupem zpravodajské činnosti. Přijaté informace je v procesu zpravodajského cyklu nutné zpracovat a odpovědět na několik otázek. Je tato informace relevantní, tzn. souvisí se zkoumaným jevem? Je tato informace přesná, tzn. byla původní data pravdivá a nebyla informace zkreslena výkladem? Je tato informace cenná, tzn. má dostatečnou hodnotu pro vysvětlení zkoumaného jevu? Až informace, které projdou tímto procesem, teprve lze použít v analytické činnosti při tvorbě zpravodajského výstupu.

---

[24] HORÁK, Oldřich, a KUTĚJ, Libor. *Základy zpravodajství*. Brno, 2016. ISBN 978-80-7231-457-7. Str. 11.

Zpravodajská informace je pak výsledkem celého zpravodajského cyklu. S co největší mírou pravděpodobnosti snižuje nejistotu a přesně popisuje buď uplynulé jevy, současný stav, nebo s určitou mírou pravděpodobnosti předvídá budoucí vývoj. Až zpravodajská informace se pak v podobě zprávy předává adresátům.

Je tedy jasné, že kvalitní a relevantní zpravodajská informace závisí na množství, správnosti a kvalitě výchozích dat a jejich správném shromáždění a vyhodnocení.

2.2.3. Zpravodajský proces

Zpravodajství je, jak již bylo zmíněno, záměrnou činností, která se vyznačuje jistou kontinuitou a diferenciací jednotlivých aspektů. Naplnění požadavků na zpravodajství – tedy vytvoření výsledného produktu – je charakterizováno tzv. **zpravodajským procesem** nebo **zpravodajským cyklem** (*Intelligence Process or Cycle*). Ten rozděluje proces zpravodajství na několik postupných fází, od poskytnutí podnětu zadavatelem až po předání hotového zpravodajského produktu.

Ačkoliv pojem zpravodajský cyklus nebo proces lze nalézt v téměř jakékoliv literatuře zabývající se zpravodajstvím, názvy, obsahy a často i počet jednotlivých fází v cyklu se liší dle autora. Autorka práce v této kapitole vychází z dělení podle AJP-2 – Spojenecké společné doktríny zpravodajství, kontrazpravodajství a bezpečnosti,[25] které zahrnuje čtyři fáze – řízení, shromažďování, zpracovávání a distribuci.

Toto dělení patří mezi ty jednodušší. Někteří autoři dále rozdělují fázi řízení (někdy také nazývanou fází plánování) na fáze zadání a definování problému a fázi plánování postupu[26], nebo fázi zpracovávání na fázi zpracování a využití a fázi analýzy a produkce informací[27], pro účely této práce je ale dělení podle AJP-2 dostačující.

---

[25] AJP-2. Spojenecká společná doktrína zpravodajství, kontrazpravodajství a bezpečnosti, Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security (Edition B, Version 1, vydání 2020).

[26] ZEMAN, Petr. Zpravodajský cyklus – ; klišé nebo nosný koncept? *Obrana a strategie*. Brno: Univerzita obrany, 2010, 10(1), str. 45-64. ISSN 1802-7199.

[27] Joint Publication 2-01. *Joint and National Intelligence Support to Military Operations* [online]. 5.7.2017 [cit. 26.2.2024]. Dostupné z: https://irp.fas.org/doddir/dod/jp2_01.pdf

2.2.3.1. Řízení

Fáze **řízení** (*Direction*) je výchozí a zásadní pro celý zpravodajský proces. Celá teorie zpravodajského cyklu vychází z předpokladu, že adresát zpravodajské informace vysloví konkrétní požadavky na to, o jaké zpravodajské informace má zájem a které chce obdržet. Tato fáze plní zároveň řídící funkci vůči ostatním fázím zpravodajského cyklu. Stanovuje směr, kterým se zpravodajská činnost ubírá, a je také podkladem pro kontrolu zpravodajského procesu ve všech jeho fázích.[28]

V této fázi tedy zpravodajská agentura buď dostává úkoly od svého oprávněného zadavatele (tzn. orgánu, který je ze zákona způsobilý dané agentuře zadávat úkoly) – vnější autority, nebo na základě svého zákonného mandátu začínají konat z vlastní iniciativy (tzn. zadavatelem je samotné vedení agentury) – vnitřní autority.

Tyto úkoly lze dělit na úkoly nejobecnější, dlouhodobé úkoly a jednorázové nebo krátkodobé úkoly.[29]

Nejobecnější úkoly vychází většinou ze zakládajících dokumentů agentury (typicky ze zákonů, na základě kterých jsou zřizovány), a jsou jediné veřejně dostupné. Vytvářejí jakýsi rámec úkolů a činností, na které se daná zpravodajská agentura zaměřuje.

Dlouhodobé úkoly jsou agentuře zadávány jejich zadavateli periodicky (většinou ročně) a měly by krom poslání agentury, vycházejících ze zřizovacích dokumentů, reflektovat i současnou bezpečnostní situaci na základě předchozí analýzy hrozeb a rizik a národních zájmů.

Do rámce dlouhodobých úkolů lze řadit i povinnosti vyplývající z mezinárodních smluv nebo ze závazků vyplývajících z členství v mezinárodních organizacích (EU, NATO).

S **jednorázovými** nebo **krátkodobými úkoly** se většinou lze setkat především na nižších úrovních zpravodajství (taktické nebo operační), mohou

---

[28] HORÁK, Oldřich, a KUTĚJ, Libor. *Základy zpravodajství*. Brno, 2016. ISBN 978-80-7231-457-7. Str. 15-16.

[29] MICHÁLEK, Luděk, POKORNÝ, Ladislav, STIERANKA, Jozef, MARKO, Michal, VAŠKO, Adrián. *Zpravodajské služby a zpravodajská činnost.* Praha: Wolters Kluwer ČR, 2021. ISBN 978-80-7598-726-6. Str. 270.

být ale zadány i zadavatelem na strategické úrovni v případě neočekávaného vývoje nebo krizové situace, kde vznikne náhlá potřeba po informacích.

Druhou část této fáze pak tvoří proces plánování uvnitř samotné agentury. Jednotlivým úkolům, tzv. **zpravodajským požadavkům**, se na základě analýzy hrozeb přisuzuje v rámci plánovacího procesu priorita, což umožňuje jednodušší rozhodování o konkrétním využití omezených zdrojů agentury.

2.2.3.2. Shromažďování

Ve fázi **shromažďování** (*Collection*) dochází ke shromažďování informací od zdrojů, které jsou relevantní pro daný zpravodajský požadavek. Vstupem této fáze je tedy požadavek na konkrétní okruh informací, příp. na jejich podobu, a výstupem jsou výsledné informace, které budou v rámci analýzy využity na tvorbu zpravodajské informace.

Požadavky na informace určují, co přesně by zpravodajská agentura v této části cyklu měla získat, a zdrojové součásti agentur (tzn. ty, které se zaměřují na sběr informací přímo od zdrojů) by v ní měly postupovat v souladu s plánem, který byl vytvořen ve fázi řízení.

Průběh samotného shromažďování je velmi závislý na **druhu zpravodajského zdroje**, ze kterého jsou informace získávány. Různými zdroji informací a způsoby shromažďování informací z nich se zabývají tzv. **zpravodajské obory**, kterými se budeme podrobněji zabývat v následujícím oddíle. Příkladem zpravodajského zdroje může být např. internet nebo sociální sítě v případě získávání informací z otevřených zdrojů, osoba jednající ve prospěch zpravodajské agentury v případě zpravodajství z lidských zdrojů, satelitní snímky pro obrazové zpravodajství, neveřejný rádiový nebo telekomunikační provoz v případě signálového zpravodajství, lékařské zprávy při lékařském zpravodajství aj.

Dále průběh této fáze cyklu ovlivňují **zásady shromažďování informací**[30].

[30] HORÁK, Oldřich, a KUTĚJ, Libor. *Základy zpravodajství*. Brno, 2016. ISBN 978-80-7231-457-7. Str. 18-23.

První zásadou je **plánování**. To by mělo předcházet všem dalším akcím v průběhu fáze shromažďování. Součástí plánování shromažďování by měla být analýza zkoumaného problému, včetně možných hrozeb a příležitostí, a z ní by měl vyjít plán, který zajistí, že ke shromažďování dojde ve správné chvíli na správném místě, že budou naplněny požadavky na informace z předchozí fáze, a že dojde v co největší možné míře k vyvarování se chybám v průběhu shromažďování.

Druhá zásada je **výběr a využití zdrojů**. Tato zásada by měla především zajistit, že budou využity všechny zdroje agentury, které mohou poskytnout informace týkající se zkoumaného problému. Shromažďování by mělo být naplánováno tak, aby, kdykoliv je to možné, byla paleta využívaných zdrojů co nejširší. To umožňuje ověřování informací, což je klíčové pro vyhnutí se zavádějící či lživé informaci od jednoho zdroje. Dále je třeba zvážit, jestli má agentura k dispozici dostatek relevantních zdrojů pro získání potřebného množství informací o daném problému, a pokud tomu tak není, je třeba identifikovat a aktivovat zdroje nové.

Další zásadou je otázka **času**. Ačkoliv platí, že čas strávený nad plánováním nikdy není čas ztracený, může rychlost a včasnost fáze shromažďování nejen výrazně urychlit průběh celého zpravodajského procesu, ale i například umožnit získání informací, které by po nějaké době již nemusely být k dispozici. Časový rámec v této fázi tedy musí být dostatečně dobře zvládnutý, aby mohla být reálně splněna následující opatření:

a) plánování;
b) identifikace a příprava zdrojů;
c) úkolování zdrojů;
d) nasazení technických zdrojů;
e) shromažďování informací;
f) poskytnutí zpětné vazby;
g) analýza a výklad informací;
h) šíření finálního zpravodajského produktu.

Důležitou zásadou je dále **relevance**. Je třeba zajistit, aby shromažďované informace měly (ideálně příčinnou, ale aspoň místní nebo časovou) souvislost se zkoumaným problémem. Nedodržení této zásady může

vést nejen k plýtvání cenných zdrojů agentury a časové ztrátě, ale množství irelevantních informací může výrazně negativně ovlivnit kvalitu výsledného zpravodajského produktu.

Zbývajícími zásadami shromažďování je **řízení** (které je předpokladem hospodárnému a účelnému využití zdrojů), **přístup** (který musí být zajištěn pro umožnění získání informací o objektu zájmu a měla by být k dispozici i záloha řešení pro nepředvídatelné případy), a **flexibilita** (která umožňuje pružně reagovat na nastalé situace a závisí na správně naplněných zásadách plánování a přístupu).

2.2.3.3. Zpracování

Fáze **zpracování** (*Processing*), během které dochází k přeměně dat a informací z fáze shromažďování do finálního zpravodajského produktu, je ne nadarmo považována za nejdůležitější fázi zpravodajského cyklu. Dobrou analytickou prací v této fázi je možné vyvážit některé nedostatky v množství a kvalitě shromážděných informací, ale ani nejlepší a nejpřesnější informace nemohou vynahradit jejich špatné zpracování.

Během této fáze, někdy také označované jako **zpravodajská analýza**, určený pracovník agentury (analytik) porovnává jednotlivé skutečnosti ve shromážděných informacích, identifikuje významné skutečnosti a souvislosti mezi nimi, a poté vysloví hypotézu o vzájemném vztahu. Celá tato činnost, zabývající se zkoumaným problémem, by v této části měla být zasazena do širšího kontextu prostředí, ve kterém se pozorovaný jev nachází, a to včetně možných dopadů jevu na národní bezpečnost a další zájmy chráněné státem. Po dosažení dostatečně odůvodněných závěrů je vytvořen finální zpravodajský produkt – co nejpřesnější popis současného stavu jevu, nebo podložený odhad možného budoucího vývoje.

Zpracování má své čtyři fáze – hodnocení shromážděných informací, jejich analýza, integrace do celku a interpretace. Jejich úspěšné splnění je základním předpokladem vytvoření kvalitního zpravodajského produktu.[31]

---

[31] HORÁK, Oldřich, a KUTĚJ, Libor. *Základy zpravodajství*. Brno, 2016. ISBN 978-80-7231-457-7. Str. 24-26.

Prvním krokem je **hodnocení**. Během něho jsou shromážděné informace z předchozí fáze cyklu hodnoceny na základě jejich důvěryhodnosti (jestli je informace pravdivá za všech okolností), spolehlivosti zdroje, od kterého informace pochází (na základě vyhodnocení úspěšnosti předchozích informací pocházejících od tohoto zdroje), vhodnosti (jestli informace souvisí se zkoumaným jevem) nebo přesnosti. K vyjádření těchto kvalit informace se většinou používá alfanumerická škála.

Je zřejmé, že spolehlivost zdroje lze uvažovat především v případě, že informace pochází od lidského zdroje (HUMINT, OSINT, případně MASINT). Pokud se jedná o informace pocházející např. ze SIGINT nebo IMINT, hodnocení spolehlivosti zdroje ztrácí na významu.

Po hodnocení následuje **analýza**. V té analytik již pracuje se samotným obsahem informací a snaží se o vymezení pravdivosti skutečností. Při tom využívá nejen hodnocení informací z předchozího kroku, ale vychází i z jiných objektivních skutečností, svých zkušeností a skutečností obsažených v již potvrzených zprávách.

Základními složkami kvalitní analýzy jsou fakta, hypotézy a předpoklady. Hypotéza je podložený odhad vysvětlení zkoumaného jevu, jejichž pravdivost nebo nepravdivost je odhalována pomocí faktických dat. Předpoklady pak slouží k vyplnění mezer v hypotézách tam, kde chybí relevantní fakta, a mohou sloužit jako vodítko pro dohledávání informací relevantních pro zkoumaný jev. Pro dobrou analýzu je důležité vzít do úvahy celé množství možných hypotéz, a ty poté přijímat nebo zamítat na základě faktů, nikoli domněnek.

Po analytické části následuje fáze syntetická neboli **integrace**. V té analytik nejprve třídí své hypotézy a rozhoduje o jejich přijetí či zamítnutí, případně se vrací do analytické fáze a zvažuje nové hypotézy, porovnává všechny své přijaté hypotézy s dalšími důležitými daty a důkazy, a poté je použije k sestavení jednotného celku, který poskytuje věrný obraz zkoumaného jevu – model. Pro vytvoření modelu co nejpodobnějšího realitě je klíčová kombinace informací z různých zpravodajských zdrojů.

Závěrečnou částí je **interpretace**. V ní analytik vyjde z přijatých hypotéz a informací, které je podporují, a následně zkoumá jejich význam ve vztahu k aktuálním faktům. Dává tak výslednému zpravodajskému produktu smysl

a posouvá ho z pouhého souhrnu relevantních informací ke zprávě, která naplňuje požadavky zadavatele.

Při interpretaci vychází analytik krom dostupných informací především ze svých vlastních zkušeností a znalostí zkoumaného jevu, zájmových objektů, které s jevem souvisí a prostředí, ve kterém se nachází. Samotná interpretace je pak z velké části založena na deduktivní činnosti, kdy analytik z jednotlivých aspektů modelu hypotéz vyvozuje další závěry (např. o důvodech činnosti zájmového objektu, jeho motivaci a cílech jednání, o kontinuitě způsobů jednání, o možné přítomnosti klamných informací aj.).

2.2.3.4. Šíření

Šíření (*Dissemination*), někdy také distribuce, je závěrečnou fází zpravodajského cyklu. Ta zajišťuje, že se zpracovaný zpravodajský produkt dostane k zadavateli, který v první části cyklu vyslovil požadavek na tento produkt.

Ačkoliv se na první pohled zdá, že se jedná o tu nejméně důležitou součást procesu, není tomu tak. Až předáním zpravodajské informace příslušnému orgánu nebo instituci může dojít k praktickému využití informace pro další rozhodovací činnost těchto subjektů. Je tedy třeba, aby předání informace bylo dostatečně včasné (aby byly informace ve zprávě v době, kdy na ní orgán stihne reagovat, stále aktuální) a ve vhodné formě (v závislosti na požadavcích zadavatele – krom písemné formy předávané v tištěné podobě nebo elektronicky je možné produkt dodat i v podobě např. grafů, map nebo jiné grafiky, případně ve formě prezentace jako např. PowerPoint).

Dalším velkým nárokem na šíření zpravodajského produktu je jeho utajení. V případě, kdy produkt vychází z informací protivníkem utajovaných, je nezbytné, aby zůstala utajená i skutečnost, že agentura získala k takovýmto informacím přístup – a to nejen z důvodu zachování aktuálnosti informací, ale především z důvodů utajení zdrojů (např. spolupracujících osob) nebo metod (např. schopnost prolomit šifrování protivníka).[32]

[32] MICHÁLEK, Luděk, POKORNÝ, Ladislav, STIERANKA, Jozef, MARKO, Michal, VAŠKO, Adrián. *Zpravodajské služby a zpravodajská činnost.* Praha: Wolters Kluwer ČR, 2021. ISBN 978-80-7598-726-6. Str. 273-274.

Málokdy se stane, že zpravodajský produkt dokáže plně odpovědět na všechny požadavky zadavatele, příp. že není potřeba na tento produkt navázat dalším zkoumáním. Po vyhodnocení informací zadavatelem by tedy mělo dojít k upřesnění stávajících požadavků, příp. zadání nových. Tím se zpravodajský cyklus uzavírá a vrací se zpátky na začátek.

2.2.4. Zpravodajské obory

Zpravodajské obory, někdy také zpravodajské disciplíny, jsou různými typy zpravodajské činnosti. Vychází z použití různých zpravodajských zdrojů – původců vstupních dat a informací – a na jejich základě používají rozdílné metody při shromažďování a vyhodnocování informací.

V této kapitole autorka představí čtyři nejrozšířenější zpravodajské obory – zpravodajství z otevřených zdrojů (OSINT), zpravodajství z lidských zdrojů (HUMINT), signálové zpravodajství (SIGINT) a obrazové zpravodajství (IMINT). Především s rozvojem moderních technologií a možnostmi získávání informací pro zpravodajskou činnost dochází ke vzniku nových zpravodajských oborů, na které v této práci bohužel není prostor.

Hranice mezi jednotlivými obory nejsou v některých situacích ostré a mohou se prolínat. Příkladem může být třeba televizní nebo rozhlasové vysílání. Pokud se jedná o běžně přístupné vysílání, lze ho zařadit pod OSINT, pokud by se ale jednalo o vysílání šifrované, bude spíše spadat pod SIGINT. Dále na sebe jednotlivé obory při získávání jednoho výstupu mohou navazovat. Za pomocí HUMINTu lze například získat snímky zachycené cizím satelitem, které mohou být dále předány k dalšímu zpracování IMINTem. Je na místě tedy zpravodajské obory brát spíše jako různé disciplíny stejné zpravodajské činnosti než jako naprosto odlišné vědní obory.

2.2.4.1. OSINT

Zpravodajství z otevřených zdrojů (*Open Source Intelligence, OSINT*) je v současné době jedním z nejdůležitějších zpravodajských oborů. Ačkoliv se ve své podstatě nejedná o novou disciplínu – již od rozšíření písma lze mluvit o možném využívání veřejných písemností jako knih, listin aj.

k získávání informací – její význam nepochybně stoupl v posledních několika set letech s rozšířením knihtisku a poté počátky médií jako jsou noviny, časopisy (LITINT, neboli **zpravodajství z literárních zdrojů**, je možné považovat za předchůdce dnešního OSINTu) nebo později rádia a televizní vysílání. Obrovským převratem pro OSINT byl pak vznik internetu, který umožňuje komukoliv s internetovým připojením přístup k obrovskému množství informací téměř odkudkoli s vysokou mírou anonymity. Výraznou roli v současném OSINTU pak hrají i sociální sítě, kde je možné nalézt informace v podobě zpráv, fotografií nebo videí od samotných uživatelů v reálném čase, z velké části bez cenzury nebo jiné kontroly obsahu.

V případě OSINTu je zdrojem jakýkoliv otevřeně zveřejněná, neutajovaná informace, která může mít zpravodajskou hodnotu. Jedná se tedy z většiny o tzv. **"bílé" zdroje**. Krom typických zdrojů vypsaných výše se ale může jednat i veřejně přístupné databáze, mapy, obrázky, patenty atd. Do zdrojů OSINTu lze z části zařadit i tzv. **"šedé" zdroje** – tedy ty, které nepodléhají žádnému stupni utajení, ale přístup k nim je do jisté míry omezen, buď personálně (kdo k němu má přístup) nebo finančně (je nutné zaplatit např. poplatek). Může se jednat o zprávy z různých konferencí, meetingů, firemní brožury, akademické výzkumy, studie think-tanků aj.

Na rozdíl od jiných zpravodajských oborů se jedná o poměrně otevřenou, ne nutně vysoce strukturalizovanou disciplínu, která sice získává čím dál více vlastních specifických nástrojů (např. k prohledávání sociálních sítí, k analýze metadat obrázku, k třídění informací v databázích atd.), z velké části ale stále záleží na kritickém uvažování a analytickém myšlení samotného zpravodajce při práci se zdroji.

Hlavní výhodou použití OSINTu je relativní jednoduchost při práci se zdroji, její nízká časová a finanční náročnost a včasnost informací. Ačkoliv se dřív OSINT používal především k přístupu k datům o vědeckých a technologických vývojích, s vývojem internetu a sociálních sítích je možné prostřednictvím OSINT získat informace – alespoň částečné – o čemkoliv, co není kompletně utajované. OSINT je tedy možné použít například k prvotní analýze zadaného problému, a na základě této analýzy teprve mohou být

nasazeny jiné, časově, finančně a technologicky náročnější zpravodajské obory, které už mohou být přesně zaměřené na úzký okruh požadovaných informací.[33]

Hlavní nevýhodou OSINTu v dnešní době je, možná paradoxně, množství informací. Jedná se o poměrně novodobý problém. Zatímco ještě v polovině minulého století byl největší překážkou často nedostatek informací o zkoumaném jevu, v dnešní době internetu a sociálních sítí je informační prostor přehlcen. Je tedy náročné v tomto množství nejen najít informace, které jsou pro zadaný úkol zpravodajsky relevantní, ale také ověřovat pravdivost těchto informací. Z těchto důvodů bývá OSINT často – nezaslouženě – považován za "podřadnou" zpravodajskou disciplínu.

Spoléhat na OSINT jako na jediný zpravodajský obor na cestě k vytvoření zpravodajského produktu by tedy byla, ve valné většině případů, chyba. Pokud je ale správně použit v kombinaci s dalšími zpravodajskými disciplínami, může celý zpravodajský cyklus zrychlit, zlevnit a přispět k hospodárnějšímu využívání kapacit dalších oborů.

2.2.4.2. HUMINT

Zpravodajství z lidských zdrojů (*Human Intelligence, HUMINT*) je dozajista nejstarší zpravodajskou disciplínou. Jedná se o proces shromažďování informací získaných od fyzických osob předáním jednou osobou druhé, a to buď přímo, nebo nepřímo. HUMINT na rozdíl od jiných zpravodajských oborů nevyužívá technické prostředky – nebo na nich z většiny nespočívá – a ústřední roli v tomto zpravodajském oboru tedy hrají především samotní zpravodajci, jejich znalosti, schopnosti a zkušenosti.

Zdroji pro HUMINT jsou samotné fyzické osoby a informace, které mají a jsou schopné poskytnout. Metody využívané v rámci HUMINTu se pak diametrálně liší podle typu zdroje. Ty můžeme rozdělit například na **přátelské zdroje** – ty, co jsou ochotné se zpravodajci spolupracovat, jako např. příslušníci vlastních bezpečnostních sborů, diplomaté, členové obchodních, kulturních nebo

[33] MERCADO, S. C. Reexamining the Distinction Between Open Information and Secret [online, cit. 21.2.2024]. Dostupné z: https://www.cia.gov/static/5d8a8df615f1bb014e49bb1452991991/Difference-Open-Info-Secrets.pdf

vědeckých delegací cestujících do zájmových zemí, osoby pracující nebo se jinak stýkající s osobami představující zpravodajský zájem, představitelé neziskových organizací, místní obyvatelstvo, aj. – a na **nepřátelské zdroje**, u kterých lze předpokládat, že se zpravodajci nechtějí spolupracovat a ačkoliv mají cenné informace, nebudou je chtít poskytnout, nebo naopak budou poskytovat informace zavádějící až falešné – například osoby zadržené kontrarozvědkou nebo váleční zajatci.

U všech zdrojů HUMINTu je rozhodující, aby u nich byly přítomné tři atributy – **možnosti** (mají zpravodajsky významnou informaci, nebo jsou schopni k nim získat přístup – buď přímo, nebo prostřednictvím dalších osob), **schopnosti** (mají osobní vlastnosti, které jim umožňují zpravodajsky významné informace získat a předat v dostatečně kvalitní podobě zpravodajci) a **motivaci** (důvod jednat ve prospěch zpravodajské služby, ať již pozitivní jako finanční odměna, ideologické přesvědčení, pocit uspokojení z vlastní výjimečnosti a významu, vykonání osobní msty, nebo negativní jako vydírání[34]).

HUMINT má nespornou výhodu v tom, že jako jediný ze zpravodajských oborů je schopen odhalit myšlenky a záměry osob. Je tedy nepostradatelný v případě odhalování budoucího vývoje dříve, než k němu může dojít – v případě technických zpravodajských oborů jsou zpravodajci typicky omezeni časem mezi přípravou na vývoj, resp. nežádoucí jev (útok), který jsou schopni technickými prostředky zaznamenat, a samotným jevem. Dále je HUMINT (s výjimkou v některých případech OSINTu) nejlevnější variantou zpravodajství, protože jak již bylo nastíněno, není potřeba při něm využívat nákladných technických prostředků. Zároveň nepodléhá tak rychlému vývoji v trendech jako jiné zpravodajské obory (např. OSINT).

Má ale i své nevýhody. Jednou z nich je možná nebezpečnost procesu shromažďování informací od lidských zdrojů ať už pro zpravodajce, tak i pro samotný zdroj. Na rozdíl od jiných oborů často vyžaduje osobní přítomnost osoby zpravodajce v zájmové oblasti – tedy v oblasti, kde se zdroj nachází. Další jsou nároky kladené na osobu samotného zpravodajce. Informace pocházející od zdroje mohou mít různou míru pravdivosti a důležitosti, a je na zpravodajci,

[34] HITZ, Frederick. P. *Why Spy? Espionage in an Age of Uncertainty*. Thomas Dunne Books, 2009. ISBN 978-03-1256-173-4. Str. 3.

aby byl schopen tyto faktory co nejsprávněji vyhodnotit. Stejně jako v případě jiných zpravodajských oborů je žádoucí získané informace ověřit i za pomocí dalších prostředků, je-li to možné – což v případě HUMINTu, kde se může jednat o získání utajovaných, jinak nepřístupných informací, může být problematické.

2.2.4.3. SIGINT

Signálové zpravodajství (*Signal Intelligence, SIGINT*) je zpravodajský obor založený na zachytávání a využívání elektromagnetických signálů. Jedná se o jednu z technických zpravodajských disciplín. SIGINT je používán jako zastřešující pojem pro dva "podobory" – COMINT a ELINT.[35]

Komunikační zpravodajství (*Communication Intelligence, COMINT*) se zabývá elektromagnetickými signály přenášející komunikaci (krom otevřeného rozhlasového a televizního vysílání, které spadá pod OSINT). Zdrojem jsou tedy nejčastěji hovory mezi koncovými uživateli (přes mobilní telefon, vysílačku atd.) a příjem fonických nebo datových přenosů vysílání rádiových stanic a jiných komunikačních zařízení.

Elektronické zpravodajství (*Electronic Intelligence, ELINT*) se pak zabývá zachytáváním a analyzováním elektromagnetických signálů, které nejsou nositeli komunikace. Může se jednat například o zaměřovací systémy, radiolokátory, letecké naváděcí systémy či počítačové sítě.

SIGINT může být využit vždy, když jsou v zájmovém prostředí využívány elektromagnetické signály. Na rozdíl například od HUMINTu se jedná o pasivní zpravodajskou disciplínu, při které nehrozí odhalení prováděného shromažďování informací, a obecně je možné provádět SIGINT bez fyzické přítomnosti v oblasti sledovaného objektu nebo v její blízkosti. V běžné zpravodajské činnosti má větší význam COMINT, v rámci kterého lze sledovat komunikaci zájmových osob a zjistit tak jejich záměry, plány, schopnosti a jiné informace, které dříve bylo možné zjistit pouze HUMINTem. ELINT hraje významnější roli v případě vojenského zpravodajství.

[35] National Security Council Intelligence Directive No. 6. *Signals Intelligence* [online]. 26.4.2010 [cit. 21.2.2024]. Dostupné z: https://www.cia.gov/readingroom/docs/CIA-RDP05T00644R000100110006-6.pdf

Nese sebou ale i jisté nevýhody. Hned první je nutnost přítomnosti dostatečně kvalitních technických zařízení, které jsou schopny signály odhalit a zachytit. To se pojí s typicky nutnou potřebou předchozí znalosti o technických možnostech zájmových osob a prostředků, které ke komunikaci využívají. Další je velký vliv terénu a prostředí na efektivitu použitých technických prostředků. V případě hustě osídlených oblastí, např. měst, nebo velmi nerovného a kopcovitého terénu se může snižovat efektivní vzdálenost mezi vysílačem, který se snažíme zachytit, a našim přijímačem. V současnosti je také velkou překážkou COMINTu šifrování a fakt, že většina používaných komunikačních zařízení provoz na nich šifruje takovými prostředky, že je nutné k jejich dešifrování využití speciálních technických dešifrovacích prostředků. V neposlední řadě, stejně jako v případě HUMINTu, se lze setkat s klamnými až lživými informacemi v přijímaných signálech, a je na pečlivé práci analytiků vyhodnotit, jestli se jedná skutečně o použitelné informace.

2.2.4.4. IMINT

Obrazové zpravodajství (*Imagery Intelligence, IMINT*) představuje zpravodajský obor, který k získání informací využívá obrazů. Ty mohou pocházet například z mobilního telefonu, fotoaparátu, kamery, skeneru, satelitu, nebo jiného zobrazovacího zařízení. Jeho význam spočívá v tom, že často představuje jediný způsob, jak lze skutečně potvrdit existenci nebo činnost zájmového objektu nebo osoby.

Součástí IMINT je tedy nejen plánování a pořízení snímků, ale i jejich následná analýza a vyhodnocení, které umožňuje plné využití informační hodnoty obrazů. Při tom je třeba přihlížet krom obsahu snímku i k řadě dalších politických, sociálních a ekonomických faktorů, a vnímat získané informace v souvislostech. Proto je třeba metody IMINTu doplňovat vhodnými dalšími informacemi z jiných zpravodajských oborů.

Reálné možnosti IMINT se odvíjí především od technických možností (použitá optika, povětrnostní podmínky, proces záznamu a přenosu informací), ale taky od složitosti zachycení zkoumaných objektů.

Výhodou IMINTu je, že umožňuje poskytnout konkrétní, detailní a přesné informace o umístění a fyzických charakteristikách zájmového objektu a jeho prostředí, příp. o zkoumaných jevech. Je primárním informačním zdrojem v případě zjišťování rysů prostoru, infrastruktury a situaci objektu, čímž se v kombinaci s kvalitním vyhodnocením a informacemi z dalších zdrojů stává nepostradatelnou součástí zpravodajství.

Omezení IMINTu vychází například z času potřebného pro využití, kdy po rozhodnutí o použití prostředků IMINTu musí dojít k naplánování získání obrazu, jeho samotného pořízení a následnému vyhodnocení, než mohou být informace využity pro další zpravodajskou činnost. Jedná se tedy o časově poměrně náročný obor. Dále klade nárok na technické prostředky, jako mohou být nejen kamery a fotoaparáty, ale i průzkumné letouny nebo bezpilotní průzkumné prostředky, vybavení samotných zpravodajců zpracovávajících snímky včetně dostatečné paměti, výpočetních kapacit a grafických programů, ale i speciální vyškolení personálu. Dále mohou činnost IMINTu negativně ovlivnit povětrnostní podmínky, které v některých případech mohou snížit kvalitu pořízeného materiálu (déšť, sníh, kouř), ale také znemožnit použití některých technických prostředků (např. bezpilotních prostředků za silného větru).

2.3. Zpravodajské služby České republiky

Nedílnou součástí státní moci jsou instituce, které se zabývají zpravodajstvím a zpravodajskou činností a hrají nezastupitelnou informační roli pro státní orgány s rozhodovacími pravomocemi. Zpravodajské služby jsou tak integrální součástí systému veřejné moci každého státu, spadající do oblasti národní bezpečnosti.

V této kapitole autorka nejprve představí definici zpravodajských služeb a některá jejich dělení, a poté se již bude věnovat zpravodajským službám České republiky. Součástí kapitoly je obecný právní rámec zpravodajských služeb v ČR, vyplývající ze zákona č. 153/1994 Sb., o zpravodajských službách České republiky, a poté představení jednotlivých zpravodajských služeb ČR s akcentem na popis úkolů, které jsou jim zákonem ukládány.

2.3.1. Definice zpravodajské služby

Zpravodajské služby jsou specifickými státními orgány zodpovědnými za vytváření zpravodajských produktů klíčových pro bezpečnost státu a jeho obyvatel. Jejich primárním úkolem je poskytovat vládním orgánům (resp. všem zákonným adresátům) informace o možných hrozbách pro národní bezpečnost.[36]

Pro zpravodajské služby je tedy nejvíce typická **informační (rozvědná) činnost**, během které získávají, shromažďují a vyhodnocují (neboli **zabezpečují**) informace, na základě kterých mohou ústavní činitelé určovat národní zájmy, vyvíjet národní bezpečnostní a vojenské strategie a politiky, určovat poslání, doktríny a strategie ozbrojených sil a jiných bezpečnostních institucí, připravovat se na národní krize a na hrozby pro národní bezpečnost a občany státu a předcházet jim.

Další činností vykonávanou zpravodajskými službami je obrana před špionáží, rozvratné činnosti a sabotáži cizími zpravodajskými službami nebo jinými subjekty – tzv. **kontrarozvědná činnost**. Jejím cílem je ochrana vlastních zpravodajských zdrojů a metod na svém území i v zahraničí. Kontrarozvědná činnost může být prováděna použitím opatření defenzivní povahy (jako vyšetřování podezřelé činnosti, prověřování vlastních příslušníků i informačních zdrojů a kontrola) nebo ofenzivní povahy (jako provádění vlastních operací s cílem proniknout do cizí organizace, narušit její činnost, oklamat nebo zmanipulovat její pracovníky atd.)

Zpravodajské služby ale mohou plnit i další úkoly v rámci zabezpečování národní bezpečnosti, které jsou jim přímo svěřeny zákonem (např. zajišťování kybernetické obrany Vojenským zpravodajstvím).

Pro zpravodajství a činnost zpravodajských služeb v demokratických zemích jsou uplatňovány základní principy[37] – princip podřízenosti ústavě a zákonům, princip vlastní bezpečnosti a utajení, princip nezbytné znalosti (*need-to-know*), princip efektivity, nezbytnosti a proporcionality, princip předběžné opatrnosti a princip ochrany dat.

---

[36] Geneva Centre for the Democratic Control of Armed Forces. Intelligence Services. *SSR Backgrounder* [online]. Geneva: DCAF, 2017 [cit. 23.2.2024]. Dostupné z: https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_12_Intelligence%20Services.pdf

[37] ZEMAN, Petr. České zpravodajské služby po roce 1989. In BALABÁN, M., STEJSKAL, L. a kol. *Kapitoly o bezpečnosti.* Praha: Karolinum, 2010. ISBN 978-80-246-1440-3. Str. 234.

Za zmínku stojí především princip podřízenosti ústavě a zákonům. Jako pro ostatní orgány státní moci pro zpravodajské služby platí **zásada legality výkonu veřejné moci** – což znamená, že zpravodajské služby mohou své pravomoci uplatňovat, jen pokud to dovolí zákon, tedy jen v případech, mezích a způsoby, které jsou zákonem dovoleny.[38] Zpravodajské služby tedy mohou jednat vždy jen v souladu s mandátem, určeným zákonem, a v rámci zákonem vymezené působnosti plnit jen ty úkoly a používat jen ta oprávnění a prostředky, které jsou službě příslušnou legislativou svěřeny.

2.3.2. Klasifikace zpravodajských služeb

Ačkoliv de facto každý stát na světě má své zpravodajské služby, neexistuje pro ně jeden univerzální model. Jednotlivé služby se liší především svou působností, oprávněními a postavením s ohledem na velikost státu, jeho lokaci, typ státního zřízení, historický vývoj, převládající politickou situaci aj.

Základním kritériem pro klasifikaci zpravodajských služeb bývá zpravidla jejich působnost – především **územní** (dělení na služby vnitřní a vnější) a **věcná** (dělení na služby civilní a vojenské). Dále můžeme služby dle rozsahu působnosti dělit na služby **ústřední** a **resortní** nebo dle metody sběru informací na služby ***all source*** a **technické**.[39]

Vnitřní služby mají působnost na území vlastního státu, a zaměřují se především na vnitřní bezpečnost a na hrozby vnitrostátního původu, nebo ty, které mohou ohrozit ústavní pořádek země, národní bezpečnost, významné ekonomické zájmy nebo utajované informace. Tyto služby, někdy také nazývané jako služby bezpečnostní, defenzivní nebo kontrarozvědné, se tedy zabývají především hrozbami jako je terorismus, etnický a náboženský extremismus, organizovaný zločin a trestná činnost s ním spojená jako výroba, distribuce a prodej omamných a psychotropních látek, padělání a praní peněz, obchod s lidmi, nelegální migrace, nebo působení zpravodajských služeb cizí moci.

---

[38] V ČR viz § 2 odst. 3 ústavního zákona č. 1/1993 Sb., Ústavy České republiky, a § 2 odst. 2 usnesení č. 2/1993 Sb., Listiny základních práv a svobod.

[39] MICHÁLEK, Luděk, POKORNÝ, Ladislav, STIERANKA, Jozef, MARKO, Michal, VAŠKO, Adrián. *Zpravodajské služby a zpravodajská činnost.* Praha: Wolters Kluwer ČR, 2021. ISBN 978-80-7598-726-6. Str. 58-62.

Ačkoliv se často označují za kontrarozvědné, tyto služby provádí krom opatření proti působení cizích zpravodajských složek i vlastní rozvědnou činnost, zaměřenou na hrozby vnitřní bezpečnosti země.

Příkladem vnitřních služeb je *Federal Bureau of Investigation* (*FBI*) *v* USA, *MI5* ve Velké Británii, *Bundesamt für Verfassungsschutz* (*BfV*) v Německu nebo Bezpečnostní informační služba (BIS) v České republice.

Vnější služby, někdy též rozvědné nebo ofenzivní, mají působnost vně území vlastního státu. Zabezpečují informace, které mají původ v zahraničí nebo týkající se cizích zemí. Jejich cílem je především zjištění úmyslů jiných států nebo jiných nestátních aktérů, které svou činností mohou ovlivňovat bezpečnost nebo ekonomiku vlastního státu, pro potřeby vedení zahraniční politiky vlastního státu.

Již z toho vyplývá, že jejich okruh zájmu je širší, než je tomu u vnitřních služeb. To často reflektuje legislativní vymezení úkolů, které u vnějších služeb bývá obecnější než u služeb vnitřních. Mezi některé jejich úkoly patří například informační podpora bezpečnostní a zahraniční politiky, odhalování zahraničních činností, které mohou být hrozbou pro bezpečnostní nebo národní zájmy, podpora vojenských operací nebo obranného plánování, ekonomické zpravodajství atd.

Příkladem vnějších služeb je *Central Intelligence Agency* (*CIA*) v USA, *Secret Intelligence Service* (*SIS, MI6*) ve Velké Británii nebo Úřad pro zahraniční styky a informace (ÚZSI) v České republice.

Vojenské služby se zabývají veškerou problematikou související se zajištěním obranyschopnosti země – otázky obrany a obranného plánování, vojenského průmyslu, podpora vojenských činností nebo ochrana utajovaných informací v oblasti obrany.

Příkladem je *Defense Intelligence Agency* (*DIA*) v USA nebo Vojenské zpravodajství v České republice.

Civilní služby se zabývají všemi ostatními otázkami v oblasti bezpečnosti, politiky nebo ekonomie. Všechny zmíněné vnitřní a vnější služby jsou příkladem civilních služeb.

2.3.3. Právní rámec zpravodajských služeb v ČR

Existence, působnost a oprávnění zpravodajských služeb musí být, podobně jako u jiných státních orgánů, vymezena v zákoně.

Nejvýznamnějším zákonem v České republice upravujícím zpravodajské služby je tzv. "střechový" zákon – zákon č. 153/1994 Sb., o zpravodajských službách České republiky. Ten upravuje zejména postavení, působnost, koordinaci, spolupráci a kontrolu zpravodajských služeb, ukládání úkolů zpravodajským službám, podávání zpráv těmito službami a poskytování informací zpravodajským službám.[40] Vymezuje existenci tří zpravodajských služeb, působících v České republice – **Bezpečnostní informací službu** (BIS), **Úřad pro zahraniční styky a informace** (ÚZSI) a **Vojenské zpravodajství** (VZ), kterými se podrobněji budou zabývat nadcházející kapitoly. Z tohoto zákona dále vyplývá například odpovědnost vlády za činnost zpravodajských služeb a jejich koordinaci[41] nebo vymezení okruhu zákonných adresátů zpravodajských informací spolu s povinnostmi a režimy podávání zpráv zpravodajskými službami.[42] Tento zákon se zabývá i kontrolou činnosti zpravodajských služeb.[43]

Dvě ze tří zpravodajských služeb působících v České republice – BIS a VZ – dále upravují zákony č. 154/1994 Sb., o Bezpečnostní informační službě a č. 289/2005 Sb., o Vojenském zpravodajství. Tyto zákony upravují především používání specifických prostředků získávání informací a vedení evidencí obsahujících údaje o osobách.[44] Pro Úřad pro zahraniční styky a informace speciální zákon v době psaní práce stále neexistuje, některé další oprávnění jsou jim tedy přiřčena ve Zvláštních ustanoveních o Úřadu pro zahraniční styky a informace v rámci střechového zákona.

Částečně pak lze do právního rámce zpravodajský služeb v ČR začlenit ještě zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, který upravuje postavení zpravodajských služeb v ochraně utajovaných informací a v řízení o bezpečnostní způsobilosti, a zákony č.

---

[40] §1 odst. 1 zákona č. 153/1994 Sb., o zpravodajských službách České republiky.
[41] §7 zákona č. 153/1994 Sb., o zpravodajských službách České republiky.
[42] §8 zákona č. 153/1994 Sb., o zpravodajských službách České republiky.
[43] §12-13 zákona č. 153/1994 Sb., o zpravodajských službách České republiky.
[44] §1 odst. 2 zákona č. 153/1994 Sb., o zpravodajských službách České republiky.

361/2003 Sb., o služebním poměru příslušníků bezpečnostních sborů, a č. 221/1999 Sb., o vojácích z povolání, které upravují náležitosti ohledně vzniku, průběhu, změn a zániku služebních poměrů příslušníků zpravodajských služeb a jiné další náležitosti související s jejich službou.

2.3.4. Bezpečnostní informační služba

Bezpečnostní informační služba je **civilní vnitřní zpravodajská služba** České republiky. Je zřízena jako **ozbrojená** zpravodajská služba, tzn. příslušníci jsou oprávněni držet a nosit služební střelnou zbraň a použít ji v případech nutné obrany nebo krajní nouze.[45]

V jejím čele stojí ředitel, který je po projednání ve výboru Poslanecké sněmovny jmenován vládou. Z výkonu své funkce je ředitel BIS odpovědný vládě, která ho také odvolává.[46] Příjmy a výdaje BIS tvoří samostatnou kapitolu státního rozpočtu.[47]

Ze zákona BIS zabezpečuje informace

a) o záměrech a činnostech namířených proti demokratickým základům, svrchovanosti a územní celistvosti České republiky,
b) zpravodajských službách cizí moci,
c) o činnostech ohrožujících státní a služební tajemství,
d) o činnostech, jejichž důsledky mohou ohrozit bezpečnost nebo významné ekonomické zájmy České republiky,
e) týkající se organizovaného zločinu a terorismu.[48]

K plnění svých úkolů je BIS oprávněna používat specifické prostředky získávání informací – zpravodajské prostředky, zpravodajskou techniku, krycí prostředky a krycí doklady, sledování a osoby jednající ve prospěch BIS[49]. Způsoby, podmínky a omezení využívání těchto specifických prostředků je vymezeno v zákoně o BIS. Dále je BIS oprávněna k plnění svých úkolů vést evidence údajů o fyzických a právnických osobách.[50]

---

[45] §5 zákona č. 154/1994 Sb., o Bezpečnostní informační službě.
[46] §4 odst. 1 a 2 zákona č. 153/1994 Sb., o zpravodajských službách České republiky.
[47] §3 a) zákona č. 153/1994 Sb., o zpravodajských službách České republiky.
[48] §5 odst. 1 zákona č. 153/1994 Sb., o zpravodajských službách České republiky.
[49] §6-15 zákona č. 154/1994 Sb., o Bezpečnostní informační službě.
[50] §16 zákona č. 154/1994 Sb., o Bezpečnostní informační službě.

2.3.5. Úřad pro zahraniční styky a informace

Úřad pro zahraniční styky a informace je **civilní vnější zpravodajská služba** České republiky. Tato služba jako jediná v ČR není dále upravena ve speciálním zákoně, její existence tedy právně vyplývá ze střechového zákona.

V čele ÚZSI stojí ředitel, kterého jmenuje a odvolává ministr vnitra se souhlasem vlády. Z výkonu své funkce je ředitel ÚZSI odpovědný ministru vnitra.[51] Rozpočet ÚZSI je součástí rozpočtové kapitoly Ministerstva vnitra.[52]

Ze zákona ÚZSI zabezpečuje informace mající původ v zahraničí, důležité pro bezpečnost a ochranu zahraničně politických a ekonomických zájmů České republiky.[53]

Zvláštní ustanovení o Úřadu pro zahraniční styky a informace ve střechovém zákoně pak mimo jiné upravuje prostředky, které může ÚZSI používat pro plnění úkolů ve své působnosti – sledování osob a věcí, krycí doklady a krycí prostředky, nástrahová a zabezpečovací technika a osoby jednající ve prospěch ÚZSI.[54]

2.3.6. Vojenské zpravodajství

Vojenské zpravodajství je jednotná ozbrojená **vojenská zpravodajská služba** České republiky. Krom odlišné věcné působnosti se od BIS a ÚZSI liší i tím, že kromě zabezpečování informací má zákonem stanovený ještě jeden úkol – podílení se na zajišťování obrany České republiky v kybernetickém prostoru.[55]

V čele VZ stojí ředitel, kterého po projednání ve výboru Poslanecké sněmovny jmenuje ministr obrany se souhlasem vlády. Z výkonu své funkce je ředitel VZ odpovědný ministru obrany, který ho se souhlasem vlády odvolává.[56] Vojenské zpravodajství je organizačně součástí Ministerstva obrany.[57]

---

[51] §4 odst. 1 a 3 zákona č. 153/1994 Sb., o zpravodajských službách České republiky.
[52] §3 b) zákona č. 153/1994 Sb., o zpravodajských službách České republiky.
[53] §5 odst. 2 zákona č. 153/1994 Sb., o zpravodajských službách České republiky.
[54] §17-18 zákona č. 153/1994 Sb., o zpravodajských službách České republiky.
[55] §2 odst. 2 zákona č. 153/1994 Sb., o zpravodajských službách České republiky.
[56] §4 odst. 1 a 4 zákona č. 153/1994 Sb., o zpravodajských službách České republiky.
[57] §3 c) zákona č. 153/1994 Sb., o zpravodajských službách České republiky.

Vojenské zpravodajství ze zákona zabezpečuje informace

a) mající původ v zahraničí, důležité pro obranu a bezpečnost České republiky,
b) o zpravodajských službách cizí moci v oblasti obrany,
c) o záměrech a činnostech namířených proti zabezpečování obrany České republiky,
d) o záměrech a činnostech ohrožujících utajované skutečnosti v oblasti obrany České republiky.[58]

K plnění svých úkolů je VZ oprávněno v oboru své působnosti používat specifické prostředky získávání informací – zpravodajské prostředky (zpravodajská technika, krycí doklady, krycí prostředky a sledování osob a věcí) a využívání osob jednajících ve prospěch vojenského zpravodajství.[59] Způsoby, podmínky a omezení využití těchto prostředků jsou dále specifikovány v zákoně o Vojenském zpravodajství.

Dále jsou do působnosti VZ svěřeny činnosti, jimiž se VZ podílí na zajišťování obrany státu v kybernetickém prostoru (tzv. **kybernetická obrana**). K těm patří provádění cílené detekce kybernetických útoků a hrozeb majících původ v zahraničí a směřujících proti důležitým zájmům státu, jejichž zajišťování je předmětem obrany ČR podle zákona o zajišťování obrany ČR, identifikace a vyhodnocování detekovaných kybernetických útoků a hrozeb a jejich dopadů a opatření k odvracení detekovaných kybernetických útoků a hrozeb.[60] Zároveň s nimi má Vojenské zpravodajství oprávnění za určitých podmínek provést aktivní zásah v kybernetickém prostoru.[61] Tyto podmínky, omezení a další povinnosti vyplývající z tohoto oprávnění jsou obsaženy v zákoně o Vojenském zpravodajství.

[58] §5 odst. 3 zákona č. 153/1994 Sb., o zpravodajských službách České republiky.
[59] §7-16 zákona č. 289/2005 Sb., o Vojenském zpravodajství.
[60] §16a odst. 1 zákona č. 289/2005 Sb., o Vojenském zpravodajství.
[61] §16g zákona č. 289/2005 Sb., o Vojenském zpravodajství.

3. EMPIRICKÁ ČÁST

V empirické části práce autorka naváže na teoretické poznatky z předchozí části a zpracuje analýzu vlivu umělé inteligence na plnění úkolů zpravodajských služeb České republiky s cílem prozkoumat jednotlivé možnosti aplikace umělé inteligence zpravodajskými službami, dále je porovnat a identifikovat oblasti s největším potenciálem pro využívání při plnění těchto úkolů.

3.1. Cíl a omezení empirické části

Cílem empirické části je prozkoumat možný vliv umělé inteligence na činnost zpravodajských služeb České republiky skrze využití jednotlivých aplikací AI při plnění úkolů zpravodajských služeb a identifikovat oblasti, na které může umělá inteligence mít největší vliv.

Autorka v této části bude považovat "úkoly zpravodajských služeb ČR" za zákonem svěřené úkoly, tzn. úkoly, které jsou zpravodajským službám ČR uloženy zákonem č. 153/1994 Sb., o zpravodajských službách České republiky, při vymezování jejich působnosti – tedy především zabezpečování informací.

Druhým úkolem, který je v České republice svěřen Vojenskému zpravodajství – mimo zabezpečování informací – je podílení se na zajišťování obrany ČR v kybernetickém prostoru. Autorka se ale nakonec rozhodla v empirické části práce tímto úkolem Vojenského zpravodajství nezabývat. Důvodů k tomu je několik. Především se jedná o relativně nový úkol, který je ale velmi odlišný od úkolů, které zpravodajské služby plnily před jeho přiznáním. Oblast kybernetické obrany je sama o sobě velmi široké a složité téma, k jejímuž pochopení by byl zapotřebí poměrně značný teoretický základ – který autorka není schopna v omezeném rozsahu této práce poskytnout. Jelikož se jedná pouze o malou část toho, čím se zpravodajské služby v České republice zabývají, přišlo autorce účelné zaměřit se především na kvalitní zpracování oblasti zabezpečování informací, tedy stěžejního úkolu všech zpravodajských služeb ČR, než se snažit povrchově pojmout obě oblasti úkolů.

V rámci empirické části této práce se dále nebude zabývat úkoly, které zpravodajským službám ukládá zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti.

3.2. Struktura a metody empirické části

Nejprve autorka v empirické části identifikuje a popíše úkoly zpravodajských služeb s využitím poznatků z teoretické části práce, za účelem umožnění pozdější analýzy možné aplikace umělé inteligence při plnění těchto úkolů.

Poté se bude autorka krátce zabývat obecnou premisou využívání umělé inteligence zpravodajskými službami, především na základě legislativy, etiky či dosaženého vývoje. Cílem práce není odpovědět na otázku, zda by měla být umělá inteligence zpravodajskými službami využívána či zda si autorka myslí, že je toto využívání možné. Jelikož se ale autorka ve své analýze vlivu umělé inteligence na činnost zpravodajských služeb snaží o co největší možný přesah do reálného světa, přijde ji nezbytné tyto faktory při zkoumání možných aplikací AI na plnění úkolů zpravodajských služeb minimálně vzít v potaz.

V následující části již autorka provede analýzu možných aplikací umělé inteligence při plnění úkolů zpravodajských služeb. Pro pozdější možné porovnání vlivu jednotlivých využití AI na činnost zpravodajských služeb použije autorka následující nástroje – odhad možného dopadu technologie a určení stupně připravenosti technologie.

Odhad možného dopadu technologie je velmi problematický a bez dostupnosti velkého množství dat o současném stavu, stupni vývoje, překážkách, využitelnosti a ceně se vždy jedná do velké míry skutečně pouze o odhad a ne poznatek podložený důkazy. Autorka přesto považuje za nezbytné pro určení možného vlivu na činnost zpravodajských služeb použít klasifikaci jednotlivých aplikací, která je schopna alespoň do jisté míry vyjádřit, jak převratná tato technologie má potenciál být ve smyslu výkonnosti při plnění úkolu – rychlosti, přesnosti, dostupnosti, ceny atd. Pro účely této práce se

autorka rozhodla převzít dělení Michaela O'Hanlona[62] na technologie, jejichž dopad bude **mírný**, **velký**, nebo **revoluční**.

Tabulka 1: Dopad technologií

Dopad	**Zlepšení výkonu**
mírný	10 – 50 %
vysoký	50 – 100 %
revoluční	více než 100 %, a nebo plnění úkolů, které bylo považováno za nemožné

Zdroj: STO Tech Trends 2020-2040, přeloženo autorkou.

Každá technologie na cestě od prvního nápadu po běžný provoz prochází různými stádii vývoje. Uvědomění si, v jaké fázi vývoje se technologie nachází, je především užitečné pro posouzení možného dopadu technologie v krátkodobém horizontu. V této práci autorka pro klasifikaci vyspělosti jednotlivých aplikací AI využije **stupně připravenosti technologie** (*Technology Readiness Levels, TRL*), což je nástroj původně vytvořen NASA.[63] Jednotlivé stupně jsou blíže popsány v tabulce 2. Pro zajištění relevance navrhovaných aplikací AI při plnění úkolů zpravodajských služeb se autorka bude především soustředit na systémy, které jsou buď již používány v odlišném prostředí, jsou vyvinuty a testovány, a nebo je u nich velká pravděpodobnost, že se tak v následujících letech stane – tedy systémy se stupni TLR 5 až 9.

Tabulka 2: Stupně připravenosti technologie

TRL 9	Skutečný systém ověřený úspěšnými misemi.
TRL 8	Dokončení skutečného systému a kvalifikace skrz testy a demonstrace.

[62] O'Hanlon, M. *Forecasting change in military technology, 2020-2040* [online]. Tech. Rep., Foreign Policy at Brookings Institution, Washington, D.C. 2018 [cit. 28.2.2024]. Dostupné z: https://www.brookings.edu/wp-content/uploads/2018/09/FP_20181218_defense_advances_pt2.pdf.

[63] MANNING, Catherine G. Technology Readiness Levels. *NASA* [online]. 27.9.2023 [cit. 29.2.2024]. Dostupné z: https://www.nasa.gov/directorates/somd/space-communications-navigation-program/technology-readiness-levels/

TRL 7	Demonstrace prototypu systému v kosmickém prostředí.
TRL 6	Demonstrace model systému/subsystému nebo prototypu v reálném prostředí.
TRL 5	Ověření součástky a/nebo pokusného modelu v reálném prostředí.
TRL 4	Ověření součástky a/nebo pokusného modelu v laboratorním prostředí.
TRL 3	Analytické a experimentální ověření kritické funkce a/nebo charakteristiky.
TRL 2	Koncept technologie a/nebo její aplikace formulovány.
TRL 1	Základní principy pozorovány a popsány.

Zdroj: NASA, přeloženo autorkou.

V závěru empirické části pak autorka shrne své poznatky a na základě použitých nástrojů identifikuje oblasti působnosti zpravodajských služeb České republiky, na které by mohla mít umělá inteligence největší vliv.

3.3. Úkoly zpravodajských služeb ČR

Podle zákona[64] jsou zpravodajské služby státními orgány pro získávání, shromažďování a vyhodnocování informací – tzv. **zabezpečování informací**. To je podstatou zpravodajské činnosti a tedy i činnosti zpravodajských služeb ČR.

V teoretické části bylo vysvětleno, že základem zpravodajské činnosti je opakovaný průběh zpravodajského cyklu/procesu. Při analýze vlivu umělé inteligence na plnění úkolů zpravodajských služeb ČR tedy autorka vychází z poznatků o fázích zpravodajského cyklu a činnostech, které v nich musí být pro úspěšné splnění cyklu naplněny.

Mimo to se autorka rozhodla ve fázi shromažďování informací věnovat zvláštní pozornost hlavním druhům zdrojového zpravodajství – OSINTu, HUMINTu, SIGINTu a IMINTu – jako specifickým oblastem, které se liší způsoby možných využití umělé inteligence.

[64] §2 odst. 1 zákona č. 153/1994 Sb., o zpravodajských službách České republiky.

3.4. Využívání umělé inteligence zpravodajskými službami

Jak bylo na začátku práce demonstrováno, umělá inteligence je v současnosti v civilním prostředí využívána k plnění řady úkolů, a ačkoliv se jedná "jen" o specifické počítačové algoritmy, je zřejmé, že svými schopnostmi a dopady zdaleka přesahuje počítačové systémy nevyužívající umělou inteligenci.

Jejich využívání s sebou ale kromě řady výhod přináší i množství úskalí – od relativně velké pořizovací ceny, která se odvíjí od potřebného množství dat, času a výpočetní kapacity na trénování systémů, přes otázky úzce související s etikou jako je transparentnost, vysvětlitelnost a omezení předsudků až po zabezpečení systémů proti kybernetickým hrozbám a útokům.

První praktická využití umělé inteligence tedy tvořily tzv. *low risk, low reward* systémy – tedy ty, určeny hlavně pro zábavu nebo jinou činnost, kde by nefunkčnost nebo jiné nepředvídatelné chování systému nezpůsobovalo vysokou míru rizika. A podobně jako tomu je poslední desetiletí u nových technologií, průkopníkem v AI a jejich praktickém použití se staly velké, civilní firmy, u kterých rizika – představující možnost, že se jim nevrátí investice do vývoje systémů – byla nižší, než možné zisky.

Především kvůli těmto vysokým vstupním nákladům a nižší míře společenské odpovědnosti je využívání umělé inteligence převážně doménou civilního sektoru. Zatímco státy a nadnárodní organizace vytváří legislativu, kterou chtějí sami sebe do budoucna omezovat ve využívání umělé inteligence,[65] nebo přemýšlí nad principy, které musí splňovat AI systémy, než je začnou využívat[66], civilní sektor každý den produkuje nové a nové aplikace a systémy, využívající umělou inteligenci.

Přesto není pravděpodobné, že tomu tak zůstane napořád. Umělá inteligence je příliš mocným nástrojem na to, aby si ho státní sektor nechal protéct mezi prsty. Cesta k používání AI státními orgány ale právě především

[65] Viz 2.1.5.2, Artificial Intelligence Act.

[66] STANLEY-LOCKMAN, Zoe, a CHRISTIE, Edward Hunter. An Artificial Intelligence Strategy for NATO. *NATO Review* [online]. 25.10.2021 [cit. 29.2.2024]. Dostupné z: https://www.nato.int/docu/review/articles/2021/10/25/an-artificial-intelligence-strategy-for-nato/index.html

z důvodů rizik, které je třeba brát v úvahu, a “vyšších sázek” při jejich využívání, bude výrazně delší a pomalejší.

3.4.1. Legislativa

Využívání umělé inteligence státními orgány – v případě této práce zpravodajskými službami – má některá úskalí. Prvním z nich je přijímaná legislativa. Zákon o umělé inteligenci, který bude pravděpodobně tento rok schválen, do jisté míry omezí, jakým způsobem mohou státní orgány umělou inteligenci využívat, a stanoví pro toto využívání podmínky.

Je otázkou, jestli se tento zákon platností dotkne i zpravodajských služeb. Zákon hovoří jasně o omezení využívání tzv. *law enforcement forces*. Tento pojem se často překládá jako **policejní složky**, doslovně by se ale mělo jednat o všechny složky “vymáhající právo” – tedy ty, které mohou vystupovat jako policejní orgán v trestním řízení.

České zpravodajské služby z důvodu požadavku na respektování tzv. oddělovacího imperativu v tomto slova smyslu *law enforcement forces* **nejsou**, neplatí to ale pro zpravodajské služby všech států v Evropě, kterých se bude Zákon o umělé inteligenci dotýkat. Příkladem je polská *Agencja Bezpieczeństwa Wewnętrznego* (*ABW*).

Dalším specifikem Zákona o umělé inteligenci je skutečnost, že se netýká využívání AI pro **vojenské účely**, bez ohledu na to, kdo je provozovatelem systému.[67] Ustanovení v něm by se tak v důsledku neměla dotýkat vojenských zpravodajských služeb.

Na základě těchto důvodů autorka předpokládá, že **Zákon o umělé inteligenci využívání umělé inteligence zpravodajskými službami v ČR přímo neomezí**. Nepřímo by ale mohlo dojít na trhu k omezení dostupnosti a dalšího vývoje takových systémů, které nebude možné podle AIA volně provozovat jinými subjekty, což by mohlo ovlivnit jejich dostupnost pro využívání zpravodajskými službami.

[67] 12a. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS [online, cit. 22.2.2024]. Dostupné z: https://artificialintelligenceact.eu/wp-content/uploads/2024/01/AI-Act-FullText.pdf

3.4.2. Cena a dostupnost

Dalším omezením ve využívání je cena vývoje systémů využívajících umělou inteligenci a jejich dostupnost.

Podobně jako tomu je u jiných softwarů, ceny systémů využívajícího umělou inteligenci se budou značně lišit na základě svého určení, typu, doby trénování a množství využitých tréninkových dat, které zvyšují spolehlivost systému, mechanismu kontroly, zajišťující kvalitu výsledků, aj. V praxi nejčastěji využívané AI systémy fungují na principu ***knowledge-based*** **systémů** (resp. vycházející z první vlny umělé inteligence) nebo na principu **strojového učení** (vycházející z druhé vlny umělé inteligence). Pro první typ systémů je klíčové velké množství dat neboli expertních znalostí, ze kterých systém vychází, samotná implementace systému není tak zdlouhavá nebo nákladná jako u systémů druhého typu. U těch je potřeba počítat především nejen s potřebou správně vybraných a setříděných trénovacích datasetů, ale také s dobou potřebnou pro natrénování systémů – která se může podle systému pohybovat v řádu týdnů, měsíců i déle.

Cena každého systému využívajícího AI se tedy bude výrazně lišit. Již z principu umělé inteligence ale vyplývá, že tyto systémy jsou **drahé**, výrazně dražší než systémy bez umělé inteligence. Ačkoliv to může být překážkou i v jejich civilním využívání, ještě větší vliv to bude mít ve veřejném sektoru, který je typický omezeným množstvím zdrojů a menší flexibilitou v jejich využívání.

Jedním příkladem za všechny je porovnání rozpočtu zpravodajské služby a ceny generativního AI systému. Zatímco Bezpečnostní informační služba má podle zákona č.433/2023 Sb, o státním rozpočtu České republiky na rok 2024 plánované výdaje bezmála 2,15 mld. Kč., firmu OpenAI, tvůrce známého ChatGPT, stálo jeho vytvoření 14 mld. USD, tzn. v přepočtu téměř 330 mld. Kč.[68]

Samozřejmě, že systém jako ChatGPT je představitelem jednoho z nejdražších v současnosti provozovaných systémů využívajících AI na světě, a to především kvůli množství dat, na kterých byl trénován, času, který k tomu byl potřeba, a příslušné výpočetní kapacitě, která to umožnila. Tento příklad ale má především za úkol čtenáři ukázat, že ačkoliv je možná zajímavé zabývat se

[68] AHERNE, Nathan. Cost of training AI models. *LinkedIn* [online]. 7.11.2023 [cit. 2.3.2024]. Dostupné z: https://www.linkedin.com/pulse/cost-training-ai-models-nathan-aherne-8ojtc

myšlenkami etiky a využitelnosti takovýchto pokročilých systémů ve zpravodajské činnosti, pravdou je, že v případě českých zpravodajských služeb to v současnosti je (a s největší pravděpodobností ještě nějakou dobu bude) bezpředmětné.

Množství a možnosti AI systémů, které zpravodajské služby budou moci získat a používat, tedy budou omezené – a to především na *knowledge-based* systémy, nebo jednodušší systémy využívající strojové učení, pravděpodobně adaptované ze systémů, které jsou již v civilním sektoru využívány.

3.5. Analýza využití umělé inteligence pro zabezpečování informací

V této části se již autorka zabývá konkrétním využíváním umělé inteligence v jednotlivých fázích nejdůležitější činnosti zpravodajských služeb České republiky – zabezpečování informací důležitých pro ochranu ústavního zřízení, významných ekonomickým zájmů, bezpečnost a obranu České republiky.[69]

3.5.1. Řízení

Ve fázi řízení zpravodajského cyklu autorka nevidí významnější potenciál pro využívání umělé inteligence.

Důvodů k tomu je několik. Prvním z nich je samotný obsah činností v této fázi, během které zákonní adresáti zadávají úkoly zpravodajským službám, a tyto úkoly jsou případně specifikovány a upřesňovány tak, aby vytvořily přesné podněty pro další zpravodajskou činnost.

Je tedy zřejmé, že podstatou této fáze je především oboustranná komunikace mezi danými subjekty, a případná optimalizace této činnosti nezahrnuje faktory využívající silných stránek umělé inteligence, jako je schopnost pracovat s velkým množstvím dat, učit se, hledat vzorce nebo vytvářet predikce.

[69] §2 odst. 1 zákona č. 153/1994 Sb., o zpravodajských službách České republiky.

Jiné činnosti, které by obsahově mohly mít potenciál pro využití umělé inteligence – jako analýzy rizik, na základě kterých jsou úkoly vytvářeny, nebo rozhodovací procesy zákonných adresátů, s jejichž pomocí určují své priority při směřování zpravodajské činnosti – jsou procesy nacházející se mimo samotný zpravodajský proces a prováděny jinými subjekty než samotnými zpravodajskými službami.

Druhým důvodem je rozsah činností v této fázi. V kontextu zpravodajských služeb České republiky lze část řízení rozdělit na úkoly vycházející ze zákona na základě zákonného mandátu (dlouhodobé úkoly), zpravodajské priority určovány zákonnými adresáty v pravidelných intervalech, typicky 1x do roka, a případné operativní úkoly kdykoliv, kdy to zákonní adresáti vyhodnotí za žádoucí. Vzhledem k omezenému množství úkolů, které jsou zpravodajským službám ČR zadávány, a jejich nižší frekvenci (v porovnání s velkými zahraničními zpravodajskými službami, nebo se zpravodajskou činností např. na taktické úrovni ve vojenském sektoru), nedává velký smysl se zabývat ani systémy využívající umělou inteligenci na klasifikaci a třídění přijatých požadavků na informace.

3.5.2. Shromažďování

Naopak, ve fázi shromažďování informací se podle autorky skrývá největší potenciál pro využívání umělé inteligence zpravodajskými službami.

Bez ohledu na podobu zdroje, dnešní informační prostor – ze kterého jsou informace relevantní pro dané zadání shromažďovány – je přehlcený. Jedním z nejtěžších úkolů pracovníků zpravodajských služeb, majících na starost sběr informací, se tedy stává orientovat se v obrovském množství dat, vyhodnocovat jejich důvěryhodnost, relevanci, spojitost s dalšími jevy a vybírat pro fázi zpracování ty, které přináší největší hodnotu pro zkoumání zájmového jevu nebo objektu.

Dokonale postihnout byť jen vybranou část informačního prostoru ale v současnosti již není v lidských silách. Nedílnou součástí tohoto procesu se tedy stávají technologie – a to nejen v podobě technických prostředků ke sběru

dat, ale i těch na ukládání, shromažďování a předběžné vyhodnocování dat. Právě v nich může hrát umělá inteligence rozhodující roli.

Konkrétní způsob využití umělé inteligence při sběru informací se bude značně lišit na základě podoby zdroje informace. Autorka poznatky v této kapitole tedy dále člení podle typů zdrojových zpravodajství.

3.5.2.1. OSINT

Svět veřejně dostupných informací je perfektním prostředím pro využívání nástrojů umělé inteligence. Zpracování obrovského množství dat, které je z hlediska shromažďování relevantních informací největší překážkou dnešního OSINTu, je jednou ze silných stránek algoritmů využívajících umělou inteligenci. Spolu s dalšími schopnostmi dnešní AI, jako je rozpoznávání vzorců v datech nebo zpracování přirozeného jazyka, tak mají potenciál naprosto proměnit shromažďování informací z veřejně dostupných zdrojů.

Prvním možným využitím je tedy sběr a zpracování dat velkého rozsahu. Umělá inteligence, fungující na bázi **vyhledávacích strojů** (*Search Engines*), je schopna v krátkém čase projít velké množství dat ze zájmového prostředí – články, zprávy, příspěvky na sociálních sítích – a vyhodnotit, zda se jedná o informaci relevantní pro zkoumaný jev nebo zájmový objekt. V porovnání s klasickými vyhledávacími stroji – které nejsou schopné postihnout kontext a vyhledávají typicky jen na základě přítomnosti textového řetězce nebo jeho části – jsou vyhledávací stroje nejen efektivnější ve smyslu menšího procenta "falesně pozitivních výsledků" (tedy těch, které označí za zájmové, ačkoliv nijak nesouvisí se zkoumaným jevem), ale mohou například využívat vestavěné překladače, umožňující vyhledávání v různých jazycích nebo vyhledávat i v jiných typech médií jako jsou obrázky nebo videa.

Přesnost a výkonnost AI vyhledávacích strojů se bude vždy velmi lišit na základě architektury programu, procesu trénování atd. Ve snaze využít především přednosti těchto programů – rychlost a výkonnost – a nesnižovat kvalitu výsledků jejich slabými stránkami – jako je rozhodování – mohou být využity především jako primární filtr informací pro pracovníka zpravodajské

služby, na kterém je ponecháno finální rozhodnutí, jestli je daná informace pro zkoumaný jev relevantní, nebo ne.

Vyhledávací nástroje využívající AI lze použít nejen aktivně na vyhledávání, ale i pasivně v podobě **monitoringu**, tzn. průběžné sledování předem určených informačních zdrojů (např. sociálních sítí, tradičních médií, databází) a sbírání informací o předem určených zájmových jevech, které se v zadaném časovém úseku v těchto zdrojích objeví. Z takto shromážděných informací je umělá inteligence pak schopna pracovníkovi zpravodajské služby poskytovat reporty shrnující zjištěné informace, včetně odůvodnění, proč byly konkrétní informace identifikovány jako relevantní. Pro tuto činnost je klíčové především **určení priorit** – tedy definovat, které jevy jsou pro službu zájmové a které mají být monitorovány, a následně toto zadání dostatečně přesně předat vyhledávacímu stroji, včetně oblastí, které má program monitorovat. Zde není omezující nejen výpočetní kapacita dané umělé inteligence (tedy to, kolik zdrojů je fyzicky schopna prohledat), ale i cena některých zdrojů informací (např. přístupů k online článkům tradičních médií nebo přístupů do databází).

Dalším možným využitím jsou algoritmy využívající **zpracování přirozeného jazyka** (*Natural Language Processing, NLP*). To zjednodušeně umožňuje AI systémům porozumět a zpracovávat lidskou řeč. Typickým příkladem jsou programy na **analýzu sentimentu** (*Sentiment Analysis*). Ty umožňují klasifikaci textu na základě emocionálního zabarvení na pozitivní, neutrální nebo negativní.[70] Tento nástroj, běžně používaný obchodními společnostmi ke kontextuální analýze recenzí nebo komunikace se zákazníky, může být v kontextu zpravodajských služeb použit například pro zjišťování nálady ve společnosti nebo zájmových skupinách, nebo monitoring sociálních sítí před projevy extremismu nebo jiných činností směřujících proti demokratickým základům společnosti.

Dalším možným použitím zpracování přirozeného jazyka je **shrnování textového obsahu**. Potřebné kontextuální chápání těchto algoritmů umožňuje kromě vyhledávání i vytváření souhrnů dlouhých textů. To může být použito

[70] GUPTA, Shanshank. Sentiment Analysis: Concept, Analysis and Applications. *Towards Data Science* [online]. 7.1.2018 [cit. 4.3.2024]. Dostupné z: https://towardsdatascience.com/sentiment-analysis-concept-analysis-and-applications-6c94d6f58c17

k optimalizaci využití času pracovníků zpravodajských služeb, kteří mohou na základě souhrnu vyhodnotit, jestli je pro jejich činnost přínosné zabývat se obsahem celého textu.

Silnou stránkou AI systémů je i **rozpoznávání vzorců** (*Pattern Recognition*). Schopnost v krátkém časovém úseku zpracovat velké množství dat a na základě matematické analýzy odhalit vzorce a vztahy mezi daty je s prací lidského analytika nesrovnatelná.[71] Znalost těchto vzorců pak může nabídnout zásadní vhled do vývoje bezpečnostních trendů, hrozeb nebo vztahů, což umožňuje i přesnější předpovědi budoucího vývoje. Zároveň mohou být tyto algoritmy použity nejen pro zpracování informací z otevřených zdrojů, ale i v dalších fázích zpravodajského cyklu při vyhodnocování informací z jiných zdrojů, což tento nástroj činí ještě hodnotnějším.

3.5.2.2. HUMINT

V současnosti bude u HUMINTu pravděpodobně umělá inteligence hrát nejmenší roli ze všech zde zmíněných zdrojových zpravodajství.

Hlavním důvodem je fakt, že se nejedná o technické zpravodajství. To znamená, že informace od lidských zdrojů nejsou získávány technickými prostředky, ale prostřednictvím zpravodajských důstojníků. Největší hodnotu tedy přináší schopnosti – jako je emocionální a sociální inteligence – a zkušenosti samotných pracovníků zpravodajské služby, které umožňují navázání kontaktu se zdrojem a získání jeho důvěry, správné vyhodnocení motivačních faktorů zdroje a jeho důvěryhodnosti, a zajištění úspěšného průběhu spolupráce zdroje s mateřskou organizací.

To jsou schopnosti, které umělá inteligence v současnosti nemá. Její silné stránky leží především v aplikacích kognitivní inteligence jako je učení, odůvodňování nebo rozhodování. Ačkoliv jednou z cest, kterou se výzkum umělé

[71] KNOWLES, Graham. AI is better than humans at seeing patterns. *LinkedIn* [online]. 1.6.2023 [cit. 4.3.2024]. Dostupné z: https://www.linkedin.com/pulse/ai-better-than-humans-seeing-patterns-use-ld-graham-knowles#:~:text=AI's%20superior%20pattern%20recognition%20capabilities,the%20biases%20we%20inherently%20hold.

inteligence ubírá, je automatické rozpoznávání lidských emocí[72], tyto algoritmy nejsou schopné vykazovat emocionální inteligenci, kterou lze nalézt u lidí. Je tedy téměř jisté, že nahrazení zpravodajských důstojníků v komunikaci se zdroji umělou inteligencí by vedlo k výrazně horším výsledkům.

Jediným důvodem, proč by něco takového bylo možné uvažovat, by byla situace velkého množství potenciálních zdrojů, které současné kapacity zpravodajských služeb nejsou schopné zabezpečit. Je velmi nepravděpodobné, že by taková situace nastala v případě strategického zpravodajství, kde je každý zdroj pečlivě vybírán na základě možností přístupu k žádaným (utajovaným) skutečnostem, schopnostem je získat a předat zpravodajskému důstojníkovi, a motivace k tomu spolupracovat se zpravodajskou službou.

Situace z probíhající ruské útočné války na Ukrajině ale ukazují i nové možné tváře HUMINTu v kontextu používání sociálních sítí. Příkladem je používání seznamovací aplikace Tinder k zjišťování skutečností o pohybu ruských vojáků na ukrajinském území.[73] V takovém případě je možné se zamyslet např. nad možným použitím programů vytvořených za účelem simulace konverzace s lidskými uživateli využívajících umělou inteligenci (tzv. *Artificial Intelligence Chatbots*), které by umožnily vedení velkého množství souběžných konverzací s potenciálními lidskými zdroji přes vybranou internetovou platformu za účelem využití informací získaných z obsahu konverzací, nebo metadat např. o poloze uživatelů. Taková aplikace má ale spíše potenciál pro vojenské využití.

3.5.2.3. SIGINT

OSINT není jediný zpravodajský obor, který byl v posledních desetiletí proměněn k nepoznání obrovským nárůstem množství dostupných dat. Množství osobních mobilních telefonů již překonalo počet obyvatel světa[74], a elektromagnetické spektrum je v současnosti přehlceno signály z civilní

[72] KHARE, Smith K., BLANES-VIDAL, Victoria, NADIMI, Esmaeil S., a ACHARYA, U. Rajendra. Emotion recognition and artificial intelligence: A systematic review (2014–2023) and research recommendations. *Information Fusion.* Volume 102, 2024, 102019. ISSN 1566-2535.

[73] BIELSKYTE, Severija. How Tinder Became a Weapon In The Russia-Ukraine War. *Huck* [online]. 21.3.2022 [cit. 3.3.2024]. Dostupné z: https://www.huckmag.com/article/how-tinder-became-a-weapon-in-the-russia-ukraine-war

[74] Charted: There are more mobile phones than people in the world. *World Economic Forum* [online]. 11.4.2023 [cit. 7.3.2024]. Dostupné z: https://www.weforum.org/agenda/2023/04/charted-there-are-more-phones-than-people-in-the-world/

telekomunikační sítě, Wi-Fi sítí, satelitů a rádií. S omezenými zdroji v podobě limitovaného počtu pracovníků zpravodajských služeb se jako jediné možné řešení jeví automatizace.

Při COMINTu bývá časově nejnáročnější částí procesu **detekce signálu** v přijatých datech rádiové frekvence, **izolace jednotlivých signálů**, a **klasifikace signálu podle typu modulace** – procesy, které lze automatizovat pomocí systémů založených na principu využívání neurálních sítí.[75] To hraje zásadní význam především při taktickém COMINTu, potenciál ale tyto systémy – s vyšší dostupnou výpočetní kapacitou – mají i při zpracování většího množství signálů na vyšší úrovni.

Další otázkou, na kterou může být odpovědí umělá inteligence, je **zpracování metadat**. V době, kdy většina "zájmových" informací předávaných signály je zašifrovaná – a prostředky, které mají zpravodajské služby k dispozici, buď neumějí informaci rozšifrovat, nebo tak neumí učinit v dostatečně krátkém čase, aby informace byla využitelná – mohou být metadata jediným způsobem, jak získat nějakou informační hodnotu z těchto signálů.

Metadata mohou obsahovat informace o poloze a nadmořské výšce vysílače, čase, použité frekvenci, šířce pásma, amplitudě, identifikaci konkrétního vysílače, multiplexoru aj.[76] V případě telefonních hovorů přes síť GSM lze určit i příjemce hovoru. To umožňuje vytvoření sítí s informacemi o hovorech.

Umělá inteligence může být použita k analyzování metadat především v případech, kdy je potřeba zpracovat velké množství dat. Vhodné použití ale může být i program na rozpoznávání vzorců v datech. Vztahy mezi jednotlivými vysílajícími a příjemci hovorů mohou odhalit kontakty mezi zájmovými osobami, záznamy o místech vysílání zase mohou pomoci určit oblast, na které se zájmové subjekty pohybují nebo operují.

---

[75] RAMIREZ, David. SignalEye: Machine Learning Automation for SIGINT. *General Dynamics Mission Systems* [online]. Květen 2019 [cit. 7.3.2024]. Dostupné z: https://gdmissionsystems.com/-/media/General-Dynamics/Cyber-and-Electronic-Warfare-Systems/PDF/Brochures/SignalEye-Machine-Learning-ML-Automation-for-SIGINT-Whitepaper.ashx?la=en&hash=9BE22EBA836C06B65F577F39BDB732B89058CF20

[76] UNDERWOOD, Kimberly. The Secret Life of Metadata on the Battlefield. *AFCEA* [online]. 1.11.2018 [cit. 7.3.2024]. Dostupné z: https://www.afcea.org/signal-media/secret-life-metadata-battlefield

Posledním možném využití umělé inteligence, které zde autorka zmíní, je **kryptografie**. AI může být teoreticky použita k prolamování šifrování, které do této doby byly považovány za neproniknutelné (jako AES-192).[77] V současné době je to ale zatím spíše otázkou teorie než praxe.

3.5.2.4. IMINT

IMINT je další z technických zdrojových oborů, kde může umělá inteligence hrát převratnou roli.

K vyhledávacím a monitorovacím kapacitám, popsaných v rámci předchozích technických oborů, se přidává **rozpoznávání obrázků** (*Image Recognition*). To je jednou ze součástí tzv. **počítačového vidění** (*Computer Vision*) neboli oblasti umělé inteligence, která se zabývá zpracováním obrázků a videí. Pro rozpoznávání obrázků, resp. objektů na nich, bylo klíčové rozvoj strojového učení a především metod, využívajících hluboké učení.[78]

Tyto algoritmy jsou na vstupních datech – typicky fotografiích, video souborech, satelitních snímcích aj. – schopné rozpoznat objekty a zařadit je do kategorií. Jsou tedy schopné nahradit člověka a lidské oko především v případech, kdy je nutné procházet velké množství obrazových záznamů a monitorovat na nich výskyt některých zájmových objektů.

Rozpoznávání objektů umělou inteligencí samozřejmě není bezchybné. Jelikož současné algoritmy vychází z druhé vlny umělé inteligence, která zaostává v kontextuálním pochopení, samotné rozpoznávání vychází z matematické podobnosti zkoumaných objektů. To znamená, že každý výsledek z takového algoritmu je jistý jen s určitou mírou pravděpodobnosti. To může být zčásti vyřešeno především ujasněním si požadavků na algoritmus a následné správné nastavení hranice citlivosti (tzn. vyvážení mezi množstvím případných falešně pozitivních výsledků a šancí, že hledaný objekt nebude identifikován). Zároveň jsou v těchto algoritmech poznatky z jednoho učení (natrénování na jeden objekt) jen těžko přenositelné na jiný, byť podobný objekt.

---

[77] MALLINDER, Jamie. Decoding the Future: OpenAI's Q* Algorithm and Ethical AI Innovation. *LinkedIn* [online]. 29.11.2023 [cit. 7.3.2024]. Dostupné z: https://www.linkedin.com/pulse/decoding-future-openais-q-algorithm-ethical-ai-jamie-mallinder--cfatc

[78] BOESCH, Gaudenz. Image Recognition. *Viso.ai* [online]. 2024 [cit. 6.3.2024]. Dostupné z: https://viso.ai/computer-vision/image-recognition/

Na druhou stranu, podobně jako je tomu v případě OSINTu, použití této technologie umožňuje získání alespoň nějakých informací v případech, které by za běžných okolností skrze obrovské množství dat nebylo možné zpracovat. To nabízí příležitosti hlavně v případě rozsáhlého monitoringu (např. satelitních snímků) nebo pátrání po objektech v případě velkého množství snímků (např. z databází, sociálních sítích).

Specifickým typem image recognition software je **program na rozpoznávání obličejů** (*Facial Recognition Software*). Ten funguje na stejném principu využití hlubokého učení, ale rozpoznávanými objekty jsou jednotlivé lidské tváře. Vzhledem k relativně malým odlišnostem mezi objekty má ale výrazně vyšší nároky na množství cvičných datasetů, výpočetní kapacitu a čas. Velký význam hraje především v pátrání po osobách nebo při pokusu o identifikaci neznámé osoby v blízkosti zájmového objektu.

Dalším možným využitím umělé inteligence v IMINTu jsou programy na **zlepšení kvality fotografií a videí** odstraněním šumu, zrnitostí a jiných nečistot. To zvyšuje využitelnost snímků, které by jinak skrze špatné podmínky při jejich pořízení využitelné nebyly, např. fotky z dronů pořízené při dešti, mlze, kouři či jiných špatných světelných podmínek.

3.5.3. Zpracování

Využití umělé inteligence při fázi zpracování informací je, dle názorů autorky, poměrně sporné. Na jednu stranu v této fázi mohou být využity některé ze silných stránek umělé inteligence, jako je rozpoznávání vzorců nebo potlačení zaujatosti. Na stranu druhou se jedná pravděpodobně o nejvýznamnější část zpravodajského procesu, která závisí nejen na kognitivních schopnostech analytika, ale i na jeho zkušenostech, kreativitě, smyslu pro detail a dalších vlastnostech, které nejsou u AI garantovány. Ne nadarmo se říká, že výborný analytik dokáže vytvořit alespoň ucházející zpravodajský produkt i ze špatně shromážděných dat, ale špatná analytická činnost je schopna naprosto znehodnotit i velmi kvalitní shromážděná data.

Nicméně převažující kvality umělé inteligence není na místě zavrhnout úplně. V současnosti existují některé nástroje, které místo nahrazení analytika

jeho práci rozšiřuje a doplňuje. Autorka nicméně v této fázi – se současnými schopnostmi umělé inteligence – nevidí velký potenciál pro využití automatizace.

Za největší příležitost pro využití AI při zpracování informací autorka považuje **prediktivní analýzu** (*Predictive Analytics*). Ta umožňuje na základě analýzy historických dat vytvářet předpovědi budoucích událostí nebo výsledků. Programy využívající strojové učení mohou významně přispět ke zpřesnění těchto odhadů tím, že jsou schopné svou schopností identifikovat trendy, chování a vzorce v datech nezávisle na tom, kde je analytik předpokládá nebo předpovídá – což ve výsledku snižuje možnou zaujatost. Dále jsou schopné detekovat korelaci mezi více proměnnými než "klasické" programy, a nahrazení některých opakujících se kroků, které jsou běžně vykonávané manuálně, znamená úsporu času a zdrojů.[79]

Prediktivní analýza může být ve zpravodajství použita např. k předpovědi chování zájmového objektu na základě dříve pozorovaného chování, k předpovědi vývoje interakce více subjektů a jejich vzájemných vztahů, k předpovědi možných hrozeb a účinností opatření k jejich předcházení, k předpovědi nabídky a poptávky atd. Rovněž může být použita k testování hypotéz, což je důležitou součástí integrační části fáze zpracování.[80]

Dalším možným využitím AI je **hodnocení informací**, pocházejících z fáze shromažďování. Kupříkladu hodnocení spolehlivosti zdroje je vyhodnocením úspěšnosti předcházejících informací od tohoto zdroje, které může být s pomocí umělé inteligence automatizováno. Hodnoty vyjadřující veličiny jako spolehlivost zdroje a důvěryhodnost informace mohou být nahrazeny pravděpodobností a dále zpracovávány, což umožňuje analytikovi tyto skutečnosti lépe postihnout v dalších krocích této fáze.

Umělá inteligence může být v neposlední řadě použita na závěr této fáze např. k **vizualizaci dat** ve finálním zpravodajském produktu, které ukazují opodstatněnost závěrů a usnadňují pochopení pro konečného adresáta. Jedná

[79] The Data Analyst's Guide to AI. *Pecan.ai* [online]. 15.11.2023 [cit. 9.3.2024]. Dostupné z: https://www.pecan.ai/blog/ai-for-data-analysts-guide/

[80] MAHARAJ, Sahir. How can you use AI for predictive analytics? *LinkedIn* [online]. 22.1.2024 [9.3.2024]. Dostupné z: https://www.linkedin.com/advice/0/how-can-you-use-ai-predictive-analytics.

se ale o velmi okrajové využití, které slouží především k úspoře času analytika a neovlivňuje výrazně kvalitu zpravodajského produktu.

3.5.4. Šíření

Ve fázi šíření autorka opět v současnosti nevidí velký potenciál pro využívání umělé inteligence.

Výjimkou by mohlo být již zmíněné využití AI v **kryptografii**. V případě, kdy je potřeba předat zprávu velkého významu konečnému adresátovi a není zprávu možno předat ve fyzické podobě, musí k jejímu předání dojít přes informační systémy. Aby ale bylo možné zajistit utajení obsahu zprávy, je třeba ji zabezpečit proti neoprávněnému využití nepovolanou osobou.

K tomu účelu slouží šifrování. Není třeba zde zabíhat do detailů fungování šifrovacích algoritmů, v současnosti ale již existují šifrovací metody na takové úrovni, že jejich prolomení – tzn. schopnost rozklíčovat obsah zašifrované zprávy bez vlastnictví příslušného klíče – je při současné výpočetní kapacitě počítačů takřka nemožné (resp. odhadovaná doba prolomení je v řádu desítek až stovek let).

To se ale do budoucna může změnit. Očekává se, že převratným objevem pro kryptografii bude především rozvoj kvantových počítačů skrze jejich výrazně vyšší výpočetní kapacitu. Jak bylo ale již zmíněno v jedné z předchozích kapitol[81], zdá se, že zásadní roli v šifrování bude mít i umělá inteligence. Její potenciální využití je nejen v prolamování existujících šifrování, ale i ve vytváření nových šifrovacích způsobů – a to jak vylepšením šifrovacích algoritmů, tak vytvářením silnějších kryptografických klíčů.[82]

[81] Viz 3.4.2.3 – SIGINT.

[82] AI Cryptography: Enhancing Security and Privacy in the Digital Age. *Medium* [online]. 7.10.2023 [cit. 9.3.2024]. Dostupné z: https://medium.com/@singularitynetambassadors/ai-cryptography-enhancing-security-and-privacy-in-the-digital-age-db5c1bbf5fdb

3.6. Kvantitativní vyjádření využití umělé inteligence při zabezpečování informací

V této části autorka využila nástroje, popsané v metodice empirické části – odhad možného dopadu technologie a stupeň připravenosti technologie – na popis identifikovaných možných aplikací umělé inteligence na zabezpečování informací zpravodajskými službami.

Tabulka 3: Možné aplikace umělé inteligence při zabezpečování informací

Zpravodajský cyklus	**Využití AI**	**Dopad**	**TLR**
Řízení	-	-	-
Shromažďování – OSINT	Vyhledávací stroje – aktivní vyhledávání	revoluční	9
	Vyhledávací stroje – monitoring	revoluční	9
	Analýza sentimentu	vysoký	9
	Shrnování textového obsahu	vysoký	9
	Rozpoznávání vzorců	revoluční	9
Shromažďování – HUMINT	Simulace konverzace s lidskými uživateli	nízký	9
Shromažďování – SIGINT	Detekce, izolace a klasifikace signálu	vysoký	9
	Zpracování metadat	revoluční	8-9
	Dešifrování	revoluční	5
Shromažďování – IMINT	Rozpoznávání objektů	revoluční	8-9
	Rozpoznávání obličejů	revoluční	8-9
	Zlepšení kvality fotografií a videí	nízký	9
Zpracování	Prediktivní analýza	revoluční	9
	Hodnocení informací	nízký	8
	Vizualizace dat	nízký	9
Šíření	Šifrování	vysoký	6-7

Zdroj: vlastní

3.7. Závěr empirické části

Cílem empirické části bylo prozkoumat možný vliv umělé inteligence na činnost zpravodajských služeb. Autorka proto identifikovala úkoly zpravodajských služeb ČR, zvážila možný vliv legislativy a dalších faktorů na samotný akt využívání umělé inteligence zpravodajskými službami v ČR, a poté se již zabývala analýzou konkrétních možných aplikací umělé inteligence v jednotlivých částech zpravodajského cyklu – řízení, shromažďování, zpracování a šíření. Možný vliv těchto konkrétních aplikací vyjádřila nejen kvalitativně během analýzy, ale také kvantitativně za pomoci dvou nástrojů, běžně používaných pro vyjadřování vlivu technologie na určitost oblast – odhad možného dopadu technologie a stupeň připravenosti technologie.

Z provedené analýzy vyplývá, že největší možný vliv může mít umělá inteligence v oblasti shromažďování informací. To je pravděpodobně zapříčiněno velkým nárůstem v množství dat, ke kterým mají v dnešní době zpravodajské služby přístup, a ze kterých musí být ve fázi shromažďování vybrány ty informace, které jsou relevantní pro vytvoření zpravodajského produktu odpovídajícímu zadání.

Obecně pak z analýzy vychází, že pro používání umělé inteligence ve fázi shromažďování platí – čím větší je množství dat, které je nutné projít při hledání informací o zkoumaném jevu, a čím menší je důležitost každé jednotlivé informace, která může být z dat získána, tím roste míra příležitostí vyplývající z možného použití umělé inteligence.

Zpravodajským oborem s největším potenciálem pro využívání umělé inteligence je OSINT. Shromažďování informací z otevřených zdrojů totiž využívá silné stránky algoritmů využívajících umělou inteligenci – jako je schopnost zpracování velkého množství dat, zpracování přirozeného jazyka použitelného na analýzu sentimentu, shrnování obsahu nebo psaní reportů, nebo schopnost nacházet vzorce a vztahy ve zkoumaných datech.

Velký vliv může mít umělá inteligence i na technické obory jako je SIGINT nebo IMINT. Zde hraje velkou roli automatizace některých jednoduchých procesů – jako je automatická detekce signálu nebo rozpoznávání objektu na

obrázku – které umožňují zpracovávání výrazně větších množství dat a dávají pracovníkům zpravodajských služeb v těchto oborech více prostoru věnovat se jiným úkolům, pro které umělá inteligence není v současnosti tak vhodná – třeba těm využívajícím kontextuální chápání a vysvětlování.

Menší potenciál pak má umělá inteligence ve fázi vyhodnocování. Některé nástroje využívající umělou inteligenci sice mohou být v práci analytikům nápomocné, lidskou schopnost kreativity, zkušeností nebo vnímání kontextu ale umělá inteligence není v současnosti schopna replikovat. Jako jedinou aplikaci převratnou pro vyhodnocování informací autorka identifikovala prediktivní analýzu využívající umělou inteligenci, ve které naopak AI dosahuje lepších výsledků než člověk.

Malý či žádný vliv pak autorka vidí ve fázích řízení, šíření a v HUMINTu. Důvodem je především povaha samotných úkolů v těchto částech zpravodajství, pro které je klíčová především lidská komunikace – tedy něco, co umělá inteligence ani přes pokročilé zpracování přirozeného jazyka není schopna nahradit např. z důvodů absence emocionální inteligence. Taktéž se jedná o úkoly, které nevyužívají žádnou ze silných stránek umělé inteligence, a pro menší množství úkonů, které v jejich rámci musí být vykonány, není účelné zabývat se otázkou jejich automatizace.

4. ZÁVĚR

V závěru práce autorka shrne obsah své práce, představí dosažené výsledky, a formuluje vlastní závěry.

4.1. Souhrn obsahu práce

Na úvod autorka představila důvody výběru tématu a cíle a strukturu práce.

V teoretické části autorka položila teoretický základ pro pochopení následující empirické části. Nejprve objasnila pojem umělá inteligence a pojmy s ním související, dále vysvětlila dělení a v současnosti dosažený vývoj umělé inteligence, a shrnula současný právní rámec umělé inteligence v Evropské unii i s připravovaným Zákonem o umělé inteligenci. V druhé podkapitole se autorka zabývala zpravodajstvím. Kromě definice a základních pojmů se soustředila především na vysvětlení jednotlivých fází zpravodajského cyklu a představení zpravodajských oborů, na což později navázala v empirické části. Poslední podkapitola teoretické části se již zabývala zpravodajskými službami České republiky. Tam autorka stručně obecně shrnula definice a klasifikace zpravodajských služeb, a poté již konkrétně představila zpravodajské služby, působící v České republice – Bezpečnostní informační službu, Úřad pro zahraniční styky a informace, a Vojenské zpravodajství.

Empirická část práce měla za cíl objasnit možný vliv umělé inteligence na plnění úkolů zpravodajských služeb v ČR. Po stanovení cíle, omezení, struktury a metod empirické části autorka tyto úkoly identifikovala a obecně shrnula některé omezující faktory využívání umělé inteligence zpravodajskými službami jako je legislativa, cena nebo dostupnost. Poté již autorka přešla k samotné analýze, kde na základě fází zpravodajského cyklu a zpravodajských oborů navrhla konkrétní možné aplikace umělé inteligence při plnění úkolů. Pro kvantitativní vyjádření možného vlivu těchto aplikací pak autorka použila odhad možného dopadu technologií a určení stupně připravenosti technologie. V závěru empirické části identifikovala na základě analýzy oblasti v rámci plnění

úkolů zpravodajských služeb, na které má umělá inteligence potenciál mít největší vliv, a poskytla zdůvodnění.

V závěru práce autorka shrnula obsah práce a představila výsledky dosažené v průběhu psaní práce včetně formulace vlastních závěrů.

4.2. Dosažené výsledky

Teoretická část práce nejprve poskytla čtenáři stručný netechnický úvod do problematiky umělé inteligence, který mimo jiné poskytl náhled do současného stavu vývoje AI a připravované legislativy EU. Poté v krátkosti přiblížila čtenáři fenomén zpravodajství založený na přístupu ke zpravodajství jako k vědnímu oboru, který má své pojmy, cíle, metody a provázanost s jinými vědami. Na závěr autorka představila zpravodajské služby jako instituce nezbytné pro zajišťování bezpečnosti státu zřizované na základě zákona. Ačkoliv autorka v této části nepřinesla nové skutečnosti, text mimo úvodu do tématu, umožňující pochopení empirické části práce, může sloužit i jako průřezové shrnutí současných poznatků ve zkoumaných oblastech.

Těžištěm práce je její empirická část. V té autorka na základě analýzy konkrétních možných využití umělé inteligence v jednotlivých fázích zpravodajského cyklu identifikovala oblasti s největším potenciálem pro využití umělé inteligence.

Tou je především fáze shromažďování informací, kde skrze stále vzrůstající množství dat nadále není možné je vyhodnocovat pouze lidskými silami bez použití automatizace. Největší vliv tak může hrát využívání umělé inteligence především v OSINTu pro automatické vyhledávání dat, vyhodnocování jejich obsahů nebo vyhledávání vzorců a vztahů mezi daty. Velký potenciál má umělá inteligence ale i v automatizaci základních úkonů v technických oborech jako je SIGINT nebo IMINT, které umožní rychlejší zpracování a pokrytí mnohem většího objemu dat.

Menší význam má AI ve fázi shromažďování, kde osobní kvality a schopnosti analytiků stále převyšují kapacity umělé inteligence. Výjimkou je prediktivní analýza, ve které výpočetní schopnosti programu a množství možných dat uvažovaných najednou značně překonává lidské schopnosti.

Nízký či žádný vliv pak autorka v současnosti vidí ve fázích řízení, šíření a ve shromažďování informací z lidských zdrojů. Může za to především povaha úkolů v těchto fázích, které nevyužívají silných stránek umělé inteligence.

4.3. Formulace závěrů

Závěrem z práce vyplývá, že **umělá inteligence má velký, až revoluční potenciál k tomu, ovlivnit a proměnit činnost zpravodajských služeb.**

Každá taková obrovská změna ale přichází s řadou překážek. Kromě potenciálních budoucích legislativních omezení a faktických omezení jako cena programů i hardwaru s dostatečnou výpočetní kapacitou, jejich dostupnost a schopnost naplnit požadavky zpravodajských služeb, výběr dodavatele s důrazem na bezpečnost dodavatelského řetězce, kybernetické zabezpečení programů, správná volba výchozích dat aj., autorka v rámci zpracování práce narazila na jedno dilema – jak zajistit, že umělá inteligence skutečně zlepší kvalitu výsledků zpravodajské činnosti.

Umělá inteligence je, nejen při využívání v rámci zpravodajské činnosti, jako oheň – dobrý sluha, ale zlý pán. Na jednu stranu může nepředstavitelně rozšířit možnosti pracovníků zpravodajských služeb při shromažďování a vyhodnocování dat. Převzetím jednoduchých, opakujících se úkolů může AI šetřit lidské kapacity zpravodajské služby na plnění složitějších zadání, ve kterých nemusí mít umělá inteligence tak velkou úspěšnost. Umělá inteligence taktéž (nadneseně) představuje ideálního pracovníka – může své úkoly plnit ve dne, v noci, není ovlivněna nedostatkem odpočinku, hladem, mezilidskými vztahy na pracovišti nebo osobním životem mimo práci, nebere žádný plat.

To vše činí její využívání velmi lákavým – což může být do budoucna kamenem úrazu. Jednou z hybných sil lidstva bylo vždy dosáhnout co nejvíc s co nejmenší námahou a co nejvíce si usnadnit život. Snadno se tedy může stát, že umělé inteligenci bude časem předáváno více a více různých úkolů, které do té doby byly vykonávány lidmi – úkoly, ve kterých nebude dosahovat tak dobrých výsledků. To může ve finále znamenat zhoršení kvality zpravodajských výstupů.

Jak bylo v práci demonstrováno, **umělá inteligence v současnosti nemá schopnosti vykonávat některé činnosti v rámci zpravodajského procesu na**

takové úrovni jako člověk. Ačkoliv do budoucna schopnosti AI určitě porostou, není pravděpodobné, že bude schopna replikovat všechny lidské kvality. U velkého množství současných systémů využívajících umělou inteligenci navíc lze narazit na problém s určením míry úspěšnosti systémů, tzn. kvality výstupů (např. při používání stejně zkreslených dat při trénování jako při testování). Zároveň ale není v lidských silách při praktickém používání umělé inteligence kontrolovat správnost každého výstupu, neboť se tím ztrácí pointa automatizace.

Podle autorky je tedy na místě již v počátcích využívání umělé inteligence ve zpravodajských službách nakreslit pomyslnou čáru a rozhodnout se, **které úkoly budou svěřeny umělé inteligenci** (např. vyhledávání a automatický monitoring u OSINTu, automatické rozpoznávání objektů u IMINTu nebo automatická detekce a izolace signálu u SIGINTu) a **jak nad nimi bude vykonávána kontrola**, a které úkoly zůstanou pevně v rukou lidských pracovníků.

Obecně může mít využití umělé inteligence ve zpravodajské činnosti podle autorky dvě podoby.

V první řadě je to použití AI na úkoly, které jsou vykonatelné člověkem se stejnými nebo lepšími výsledky, než kterých při nich dosahuje AI – která je ale schopna je vykonat mnohem rychleji a tím pádem v mnohem větším objemu, než lidský pracovník (např. automatický monitoring, analýza sentimentu). Použití umělé inteligence na plnění takových úkolů je tedy účelné, pokud je objem zkoumaných dat natolik veliký, že by nemohl být zpracován dostupnou lidskou silou.

Druhým typem úkolů jsou ty, u kterých umělá inteligence obecně dosahuje lepších výsledků než člověk (např. prediktivní analýza). V případě těchto úkolů je na místě jejich plnění přenechat umělé inteligenci a soustředit se na cílené provádění kontroly jejích výsledků.

SEZNAM POUŽITÉ LITERATURY

Monografie

- HITZ, Frederick. P. *Why Spy? Espionage in an Age of Uncertainty.* Thomas Dunne Books, 2009. ISBN 978-03-1256-173-4.
- HORÁK, Oldřich, a KUTĚJ, Libor. *Základy zpravodajství.* Brno, 2016. ISBN 978-80-7231-457-7.
- MICHÁLEK, Luděk, POKORNÝ, Ladislav, STIERANKA, Jozef, MARKO, Michal, VAŠKO, Adrián. *Zpravodajské služby a zpravodajská činnost.* Praha: Wolters Kluwer ČR, 2021. ISBN 978-80-7598-726-6.
- SHULSKY, Abram. N. a SCHMITT, Gary. J. *Silent Warfare: Understanding the World of Intelligence.* Washington, D. C.: Brassey's, Inc., 2002. ISBN 978-15-7488-345-9.
- ZEMAN, Petr. České zpravodajské služby po roce 1989. In BALABÁN, M., STEJSKAL, L. a kol. *Kapitoly o bezpečnosti.* Praha: Karolinum, 2010. ISBN 978-80-246-1440-3.

Časopisecké články

- ANDRESEN, S.L. John McCarthy: Father of AI. *Intelligent Systems*. IEEE, 2002, 17(5):84 – 85. DOI: 10.1109/MIS.2002.1039837.
- KHARE, Smith K., BLANES-VIDAL, Victoria, NADIMI, Esmaeil S., a ACHARYA, U. Rajendra. Emotion recognition and artificial intelligence: A systematic review (2014–2023) and research recommendations. *Information Fusion*. Volume 102, 2024, 102019. ISSN 1566-2535.
- RAIKOV, A. N. Weak Vs. Strong Artificial Intelligence. *Informatization and Communication*. 3/2020. DOI: 10.34219/2078-8320-2020-11-1-81-88.
- ZEMAN, Petr. Zpravodajský cyklus – ; klišé nebo nosný koncept? *Obrana a strategie.* Brno: Univerzita obrany, 2010, 10(1), str. 45-64. ISSN 1802-7199.

Zákonná úprava a doktríny

- Ústavní zákon č. 1/1993 Sb., Ústava České republiky.
- Usnesení č. 2/1993 Sb., Listina základních práv a svobod.
- Zákon č. 153/1994 Sb., o zpravodajských službách České republiky.

- Zákon č. 154/1994 Sb., o Bezpečnostní informační službě.
- Zákon č. 289/2005 Sb., o Vojenském zpravodajství.

Doktríny a jiné dokumenty

- AJP-2. *Spojenecká společná doktrína zpravodajství, kontrazpravodajství a bezpečnosti, Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security* (Edition B, Version 1, vydání 2020).
- APP-6. *Terminologický slovník pojmů a definic NATO*. Praha, 2002.
- Joint Publication 2-01. *Joint and National Intelligence Support to Military Operations*. 2017.

Webové stránky a elektronické zdroje

- 12a. *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS* [online, cit. 22.2.2024]. Dostupné z: https://artificialintelligenceact.eu/wp-content/uploads/2024/01/AI-Act-FullText.pdf
- AI Act Overview. *Artificial Intelligence Act* [online]. 24.1.2024 [cit. 13.2.2024]. Dostupné z: https://artificialintelligenceact.eu/wp-content/uploads/2024/01/AI-Act-Overview_24-01-2024.pdf
- AI and Cybersecurity: A New Era. *Morgan Stanley* [online]. 15.9.2023 [cit. 8.2.2024]. Dostupné z: https://www.morganstanley.com/articles/ai-cybersecurity-new-era
- AI Cryptography: Enhancing Security and Privacy in the Digital Age. *Medium* [online]. 7.10.2023 [cit. 9.3.2024]. Dostupné z: https://medium.com/@singularitynetambassadors/ai-cryptography-enhancing-security-and-privacy-in-the-digital-age-db5c1bbf5fdb
- AHERNE, Nathan. Cost of training AI models. *LinkedIn* [online]. 7.11.2023 [cit. 2.3.2024]. Dostupné z: https://www.linkedin.com/pulse/cost-training-ai-models-nathan-aherne-8ojtc

- ALLEN, John. The Implications of NIS2 on Cyber Security and AI. *DarkTrace* [online]. 5.12.2023 [cit. 12.2.2024]. Dostupné z: https://darktrace.com/blog/the-implications-of-nis2-on-cyber-security-and-ai
- BIELSKYTE, Severija. How Tinder Became a Weapon In The Russia-Ukraine War. *Huck* [online]. 21.3.2022 [cit. 3.3.2024]. Dostupné z: https://www.huckmag.com/article/how-tinder-became-a-weapon-in-the-russia-ukraine-war
- BOESCH, Gaudenz. Image Recognition. *Viso.ai* [online]. 2024 [cit. 6.3.2024]. Dostupné z: https://viso.ai/computer-vision/image-recognition/
- Charted: There are more mobile phones than people in the world. *World Economic Forum* [online]. 11.4.2023 [cit. 7.3.2024]. Dostupné z: https://www.weforum.org/agenda/2023/04/charted-there-are-more-phones-than-people-in-the-world/
- DAVENPORT, Thomas H. a MITTAL, Nittin. *How Generative AI Is Changing Creative Work*. Harvard Business Review [online]. 14.11.2022 [cit. 8.2.2024]. Dostupné z: https://hbr.org/2022/11/how-generative-ai-is-changing-creative-work
- Deep Blue. *IBM* [online, cit. 9.2.2024]. Dostupné z: https://www.ibm.com/history/deep-blue
- Developments. *EU Artificial Intelligence Act* [online, cit. 12.2.2024]. Dostupné z: https://artificialintelligenceact.eu/developments/
- European Parliament Research Service. The impact of the General Data Protection Regulation (GDPR) on artificial intelligence. *European Parliament* [online]. Červen 2020 [cit. 12.2.2024]. Dostupné z: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf
- Geneva Centre for the Democratic Control of Armed Forces. Intelligence Services. *SSR Backgrounder* [online]. Geneva: DCAF, 2017 [cit. 23.2.2024]. Dostupné z: https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_12_Intelligence%20Services.pdf
- GUPTA, Shanshank. Sentiment Analysis: Concept, Analysis and Applications. *Towards Data Science* [online]. 7.1.2018 [cit. 4.3.2024]. Dostupné z:

https://towardsdatascience.com/sentiment-analysis-concept-analysis-and-applications-6c94d6f58c17

- KANADE, Vijay. What Is Super Artificial Intelligence (AI)? Definition, Threats, and Trends. *SpiceWorks* [online]. 11.3.2022 [cit. 9.2.2024]. Dostupné z: https://www.spiceworks.com/tech/artificial-intelligence/articles/super-artificial-intelligence/
- KNOWLES, Graham. AI is better than humans at seeing patterns. *LinkedIn* [online]. 1.6.2023 [cit. 4.3.2024]. Dostupné z: https://www.linkedin.com/pulse/ai-better-than-humans-seeing-patterns-use-ld-graham-knowles#:~:text=AI's%20superior%20pattern%20recognition%20capabilities,the%20biases%20we%20inherently%20hold.
- KWINT, Jemma. Artificial intelligence: 10 promising interventions for healthcare. *National Institute for Care and Health Research Evidence* [online]. Červenec 2023 [cit. 8.2.2024]. Dostupné z: https://evidence.nihr.ac.uk/collection/artificial-intelligence-10-promising-interventions-for-healthcare/
- LAUCHBURY, John. A DARPA Perspective on Artificial Intelligence. *Defense Advanced Research Projects Agency* [online, cit. 10.2.2024]. Dostupné z: https://www.darpa.mil/attachments/AIFull.pdf
- LIU, Bin. "Weak AI" is Likely to Never Become "Strong AI", So What is its Greatest Value for us?. *ArXiv: Artificial Intelligence* [online]. 29.3.2021 [cit. 9.2.2024]. Dostupné z: https://doi.org/10.48550/arXiv.2103.15294
- MALLINDER, Jamie. Decoding the Future: OpenAI's Q* Algorithm and Ethical AI Innovation. *LinkedIn* [online]. 29.11.2023 [cit. 7.3.2024]. Dostupné z: https://www.linkedin.com/pulse/decoding-future-openais-q-algorithm-ethical-ai-jamie-mallinder--cfatc
- MAHARAJ, Sahir. How can you use AI for predictive analytics? *LinkedIn* [online]. 22.1.2024 [9.3.2024]. Dostupné z: https://www.linkedin.com/advice/0/how-can-you-use-ai-predictive-analytics.
- MANNING, Catherine G. Technology Readiness Levels. *NASA* [online]. 27.9.2023 [cit. 29.2.2024]. Dostupné z: https://www.nasa.gov/directorates/somd/space-communications-navigation-program/technology-readiness-levels/

- MANNING, Christopher. *Artificial Intelligence Definitions* [online]. Stanford University, 2020. Dostupné z: https://hai.stanford.edu/sites/default/files/2020-09/AI-Definitions-HAI.pdf
- MERCADO, S. C. *Reexamining the Distinction Between Open Information and Secret* [online, cit. 21.2.2024]. Dostupné z: https://www.cia.gov/static/5d8a8df615f1bb014e49bb1452991991/Difference-Open-Info-Secrets.pdf
- National Security Council Intelligence Directive No. 6. *Signals Intelligence* [online]. 26.4.2010 [cit. 21.2.2024]. Dostupné z: https://www.cia.gov/readingroom/docs/CIA-RDP05T00644R000100110006-6.pdf
- NUNN, Jeremy. How AI And Machine Learning Help Detect And Prevent Fraud. *Forbes* [online]. 1.11.2023 [cit. 8.2.2024]. Dostupné z: https://www.forbes.com/sites/forbestechcouncil/2023/11/01/how-ai-and-machine-learning-help-detect-and-prevent-fraud/
- O'HANLON, M. *Forecasting change in military technology, 2020-2040* [online]. Tech. Rep., Foreign Policy at Brookings Institution, Washington, D.C. 2018 [cit. 28.2.2024]. Dostupné z: https://www.brookings.edu/wp-content/uploads/2018/09/FP_20181218_defense_advances_pt2.pdf.
- RAMIREZ, David. SignalEye: Machine Learning Automation for SIGINT. *General Dynamics Mission Systems* [online]. Květen 2019 [cit. 7.3.2024]. Dostupné z: https://gdmissionsystems.com/-/media/General-Dynamics/Cyber-and-Electronic-Warfare-Systems/PDF/Brochures/SignalEye-Machine-Learning-ML-Automation-for-SIGINT-Whitepaper.ashx?la=en&hash=9BE22EBA836C06B65F577F39BDB732B89058CF20
- READING, D. F., a EATON, J. Science & Technology Trends 2020-2040 [online]. Brusel: NATO Science & Technology Organization, 2020 [cit. 11.3.2024]. Dostupné z: https://securitydelta.nl/media/com_hsd/report/406/document/190422-ST-Tech-Trends-Report-2020-2040.pdf

- STANLEY-LOCKMAN, Zoe, a CHRISTIE, Edward Hunter. An Artificial Intelligence Strategy for NATO. *NATO Review* [online]. 25.10.2021 [cit. 29.2.2024]. Dostupné z: https://www.nato.int/docu/review/articles/2021/10/25/an-artificial-intelligence-strategy-for-nato/index.html
- The Data Analyst's Guide to AI. *Pecan.ai* [online]. 15.11.2023 [cit. 9.3.2024]. Dostupné z: https://www.pecan.ai/blog/ai-for-data-analysts-guide/
- UNDERWOOD, Kimberly. The Secret Life of Metadata on the Battlefield. *AFCEA* [online]. 1.11.2018 [cit. 7.3.2024]. Dostupné z: https://www.afcea.org/signal-media/secret-life-metadata-battlefield
- WAHL, Thomas. Commission: White Paper on AI. *Eucrim* [online]. 1.4.2020 [cit. 12.2.2024]. Dostupné z: https://eucrim.eu/news/commission-white-paper-ai/
- White Paper on Artificial Intelligence: a European approach to excellence and trust. *European Commission* [online]. 19.2.2020 [cit. 12.2.2024]. Dostupné z: https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en
- ZARAKI, Abolfazl. An excellent talk from DARPA on the three waves of Artificial Intelligence (AI) – The Contextual Adaptation is the right direction to go: Explainable AI. *Cardiff University Blogs* [online]. 18.7.2020 [cit. 10.2.2024]. Dostupné z: https://blogs.cardiff.ac.uk/ai-robotics/an-excellent-talk-on-the-three-waves-of-artificial-intelligence-ai-the-contextual-adaptation-is-a-way-to-go-explainable-ai/
- ZEMAN, P. *Co je zpravodajství* [online]. Květen 2008 [cit. 14.2.2024]. Dostupné z: http://www.absd.sk/co_je_ zpravodajstvi