

GULYÁS ATTILA*

NYELVI MODELLEK ALKALMAZÁSA A KIBERVÉDELEMBEN

I. RÉSZ

Összefoglalás: A nagy nyelvi modellek jelentős elterjedése, azok mindennapos használata a világhálón egyre inkább rámutat ezen innovációk lehetséges kibernetikai védelmi aspektusainak a fejlesztésére mind a saját belső intraneten, mind vállalkozásaink és a védelmi (hon- és rendvédelmi) informatikai hálózatokon. A nyelvi modellek kibervédelmi alkalmazása támogatja informatikai hálózataink magasabb szintű védelmét. E tudományos közlemény a szerző egyetemi szakdolgozatának kivonata, amelyet a Torinói Tudományegyetem (UniTo) Masters di II Livello in Strategia Globale e Sicurezza szakon nyújtott be és védett eredményesen a 2024/2025. tanévben.

Kulcsszavak: nagy nyelvi modellek, kibervédelem, hálózatalapú hadviselés, természetes nyelvfeldolgozás, természetes nyelvek megértése

Abstract: The significant spread of large language models (LLMs) and their casual use on the World Wide Web increasingly points to the development of the possible cyber defense aspects of this innovation, both in our own internal and in our enterprises and in the defense (homeland and law enforcement) IT networks. The cyber defense application of large language models supports a higher level of protection of our IT networks. This scientific paper is an excerpt from the author's university thesis, submitted to the University of Turin (UniTo) for the Masters di II Livello in Strategia Globale e Sicurezza in the 2024-2025 academic year.

Keywords: large language models, cyber defense, Network Centric Warfare, Natural Language Processing, Natural Language Understanding

BEVEZETÉS

Az Európai Unió (EU) belüli [1] rendvédelmi együttműködés legfontosabb intézménye, az EUROPOL [2] a közelmúltban figyelmeztetést [3] adott ki, amely alapján a mesterséges intelligencián (MI) alapuló rendszerek rosszindulatú tevékenységekre is felhasználhatóak. [4] A kiberbűnözői csoportok a ChatGPT (Generative Pre-trained Transformer) támogatásával chatbotokat használhatnak *social engineering* (pszichológiai manipuláció) jellegű támadásaikhoz, dezinformációs kampányokhoz, kiberbűnözői tevékenységeikhez. [5] Az állásfoglalás szerint az MI-alapú programok egyre nagyobb fenyegetettséget jelentenek a kibertérben, ezért a megfelelő és arányos védelem rendkívüli fontosságú. [6] Ugyanakkor a jelentésben kiemelik, hogy a gépi tanulási modellek újabb verziói, kiemelten a GPT-4 [7] már sokkal hatékonyabb támogatást nyújtanak a kiberbűnözés elleni védekezés támogatására. [8] A jelentésben ez szerepel: „Az újabb modell jobban megérti a kód kontextusát, valamint a hibáüzeneteket, továbbá a programozási hibák javítására is alkalmasabb lett. A csekély műszaki ismerettel rendelkező, potenciális bűnöző számára ez felbecsülhetetlen értékű erőforrás. (...) Egy fejlettebb technikai képességekkel rendelkező felhasználó pedig arra használhatja ki ezeket a jobb képességeket, hogy tovább finomítsa vagy akár automatizálja a kifinomult kiberbűnözői modi operandi-t.” [9]

Felmerül tehát a kérdés: ha a fejlett verziójú gépi tanulási modellek könnyebben felhasználhatóak az emberek megtévesztésére, milyen lépéseket lehetséges, sőt kötelező tennünk a kibertérben elkövetett káros cselekmények korlátozására. Úgy vélem, az első lépés, hogy széles, széle-

* Ezredes, csoportfőnök,
Híradó, Informatikai és
Információvédelmi
Csoportfőnökség,
Honvéd Vezérkar,
Magyar Honvédség.
ORCID:
0000-0001-5774-5757

sebb körű tájékoztatást, oktatást kell biztosítanunk a gépi tanulási eljárások megértése érdekében. Tudatosítani kell az egyéni felhasználókkal és vállalkozásokkal, hogy a 2025-ös évben a nagy nyelvi modellek (Large Language Models – LLMs) olyan fejlettségi szintet értek el, amellyel könnyen lehet manipulálni az adott személyt/személyeket döntéseikben, felhasználva a megtévesztés különböző módjait (pl. phishing mailek, hang- és kép manipulálása, ransomware-t [zsarolóprogramot], deep fake videót stb. [10]) Azt is fel kell ismernünk, hogy a magas fokú automatizálás eredményeképpen a rosszindulatú felhasználók (támadók) részéről egyre kisebb informatikai tudásra lesz szükség a kibertérben elkövetett káros cselekményeikhez.

Mindezen tényeket áttekintve és értelmezve, véleményem szerint szükség van a gépi tanulási modellek általános bemutatását tartalmazó összefoglaló anyag összeállítására, melyben kiemelendő ezen gépi tanulási modellek alkalmazhatósága a digitális hálózataink kiberműveleteiben, kiemelt tekintettel a védelmi (katonai és rendvédelmi) digitális információs hálózatok védelmére. Ezért választottam jelen témának az MI-alapú, a gépi tanulási eljárások alkalmazhatóságának vizsgálatát a kibertevékenységekben, elsődlegesen a kibervédelemben. [11]

E tudományos közleményben nagy léptékben bemutatom az LLM történelmi fejlődését és az elért eredményeket, majd azt vizsgálom, hogy a világ vezető MI-fejlesztő országai és vállalkozásai milyen szabályzó környezetet hoztak vagy törekednek létrehozni az LLM robbanásszerű fejlődésének szabályozására. [12] A továbbiakban azt is vizsgálom, hogy a gépi tanulási modellek újdonságai hogyan, mi módon alkalmazhatóak a kiberműveletekben, elsősorban a kibervédelmi eljárások automatizálásában az emberi kibervédelmi tevékenységek támogatására. Belátható, hogy a gépi modellek adatgyűjtő/rendszerző és mintafelismerő képessége messze felülmúlja az emberi lehetőségeket. Úgy vélem, a biztonságtudatosság fogalmának frissítésével, új értelmezésével „megnyerhető” a küzdelem a digitális hálózatunkba behatolni kívánó kibertámadó (hacker) ellen, a hálózat védelmére felelős mérnöki állomány javára.

Ugyanakkor látható, hogy az egyes államok és tökére erős vállalkozások által támogatott számítástechnikai ipari szakterületek, az ezek támogatása mögött meghúzódó célirányos és igen határozott befektetői szándékok, a jelentős támogatáscsomagok megjelenése [13] (források allokációja) lesz a döntő, amikor helyzeti előnybe kívánják hozni egy adott országban tevékenykedő polgári vállalkozás MI-fejlesztését [14] (pl. az USA-ban, EU-tagországokban, [15] Kínában) annak érdekében, hogy a gépi tanulás jelenleg még óriási erőforrásigényét (processzorteljesítmény és memóriaigények) fedezni lehessen.

Azonban e területen is dinamikus a fejlődés: hónapról hónapra jönnek hírek a mind kevesebb erőforrást felhasználó, de képességeiben a jelenlegi (GPT-4 [16]) applikáció abszolút értelemben vett tudásához felnövő vagy azt meghaladó, újabb és újabb gépi tanulási modellek, algoritmusok megjelenéséről. A fejlődés üteme és léptéke szinte robbanásszerű, és úgy vélem, lehetetlen megjósolni, hogy kis- és középtávon (2-6 év) merre halad előre a gépi megértés és beszéd, az adatfeldolgozás szintje.

Szilárd meggyőződésem, hogy a polgári és a katonai kutatóknak egyaránt figyelemmel kell kísérniük ezen műszaki változásokat annak érdekében, hogy a védelmi (katonai- és rendvédelmi) digitális hálózatok kibervédelmében minél nagyobb arányban használják a gépi tanulási modellek újdonságait, a katonai vezetési és irányítási rendszerek folyamatainak automatizálása és átfogó kibervédelme érdekében.

TÖRTÉNELMI KITEKINTÉS

Amikor az 1960-as években az Amerikai Egyesült Államok vezető kutatói sikeresen összeállították az ARPANET névre keresztelt első, a Neumann-elvek [17] alapján tervezett, önálló, digitális alapon működő számítógépekből álló hálózatot, megszületett a csomagkapcsolt átvitelre épülő, önálló, független hálózat első képviselője, amelynek a sikere alapot szolgáltatott a fejlesztések felgyorsítására. Csak a valóban élénk képzelőerővel rendelkező szakértők hittek abban, hogy alig 50 éven belül olyan mély integráltságú, a teljes Földet behálózó integrált hálózat alakul ki, amely lehetővé teszi a széles spektrumban értelmezett adatcserét mind a tudományos, mind a társadalmi és a gazdasági élet területein. Míg az 1980-as években a katonai kutatások és fejlesztések diktálták az ütemet az informatikai hálózatok fejlesztésében, az 1990-es évek második felétől – a közösségi média és a szórakoztatóipari alkalmazások, programok, számítógépes hálózati játékok nagyobb arányú megjelenésével – egyre inkább a polgári vállalkozások és az általuk támogatott kutatások vették át a vezető szerepet a kereslet kiszolgálására. Ezen profitérdekelt vállalkozások napjainkra – mind hardverek, mind szoftverek tekintetében – teljes mértékben átvették a vezető szerepet a világméretű hálózatok összetevői, alkotóelemei fejlesztésében, és a katonai alkalmazások egyre inkább átveszik és továbbfejlesztik, követik ezen polgári fejlesztések eredményeit. Az 1949-ben megalakított, 2025-ben már 32 tag nemzetet számláló politikai-katonai szövetség, a NATO [18] dokumentumaiban is alapvetésként jelenik meg a kölcsönösen összekapcsolt és illesztett digitális hálózatok kialakításának igénye.

Kicsit visszatekintve az időben, a 2002 őszén tartott prágai NATO-csúcsértekezleten a Prágai Képességvállalás szerződése keretében megegyező született a szövetségi képességfejlesztések új irányáról. „A szövetséges államok elkötelezik magukat következő képességeik fejlesztésére: atom-vegyi-biológiai fegyverek elleni védelem; felderítő/hírszerző rendszerek fejlesztése; föld-levegő felderítő és jelentő rendszerek fejlesztése; a vezetési és irányítási rendszerek, valamint az azokat támogató híradó és informatikai rendszerek bővítése; az egységek/alegységek harcérték-növelése a valószínűsített ellenség légvédelmi fenyegetésének elnyomásával és precíziós lőszerek alkalmazásával; a stratégiai légi és tengeri szállítási képesség fejlesztése; a légi utántöltési képesség további fejlesztése, a telepíthető harci támogató és harci kiszolgáló erők fejlesztése.” [19] Az azonosított feladatok rendszere és a képességek fejlesztésének igénye alapvetően eredeztethető az új évezred szinte minden – politikai, társadalmi, szociális, katonai – vetületének összekapcsolt, hálózatos értelmezéséből. Általános értelemben tehát a hálózatalapú hadviselésnek (NCW – Network Centric Warfare) [20]

támogatnia kell a döntés-előkészítő és döntéshozatali folyamatok felgyorsulását és az automatizálási igények kielégítését. Katonai értelemben ez elképzelhetetlen a korszerű távközlési és informatikai szolgáltatások magasabb szintű kihasználását lehetővé tevő, digitális alapú híradó és informatikai rendszerek kialakítása nélkül. [21]

A hálózatszerűen kialakított vezetési rendszerek által biztosítható információs fölény szükségszerűen elvezet a vezetési fölény kialakulásához, amely a modern hadviselés keretei között [22] – ahol a műveleti cél elérése az előerő, a saját csapatok veszteségeinek csökkentésén keresztül valósul meg – a hatékonyságalapú támadásban, összességében a hatásalapú (EBO – Effect Based Operations [23]), hálózatközpontú műveletekben összpontosul. [24] A magyar elméleti kutató, dr. Szternák György megállapítása alapján „a hálózatközpontú katonai művelet lényege, hogy egy (azonos) rendszert alkot a felderítés, a döntés és a cél pusztítása a katonai műveletek végrehajtása teljes időtartamában”. [25] Ez a korszerű megközelítés segíti a modernizált vezetési és irányítási információs rendszereket technikailag támogató híradó és informatikai rendszerek kialakítási igényének a megértését.

A hálózatalapú hadviselés igényli a NATO-hálózat nyújtotta szolgáltatások (NNEC – NATO Network Enabled Capability [26]) áttekintését és igényalapú fejlesztését. A hálózati szolgáltatások keretében integrált információs hálózatok elemei bármikor, bármilyen szintről hozzáférhetőek, a műveletek sikerét biztosító információk elérhetők. [27] A legálább a műveleti hadszíntér szintjén összekapcsolt és illesztett hálózatos vezetési rendszerekben alapkövetelmény a rendszer elemeinek együttműködési képessége (interoperabilitása) a magas szintű hálózati illesztettség állapotának elérése érdekében, ami egyaránt kötelező érvényű az információs hadviselés fizikai, információs és kognitív szegmensére. A legeredményesebb műveleti koherencia azonban csakis a műveleti hadszíntér, a döntéseket előkészítő, a döntéshozó és a feladatokat végrehajtó szervek teljes körű együttműködésével valósulhat meg. E műveleti interoperabilitás elérése érdekében – a washingtoni NATO-csúcsértekezleten meghatározott képességek fejlesztésének igényével – a NATO tagállamai felgyorsították a had-erőátalakítási folyamatokat.

A katonai információs infrastruktúrák fejlesztése tehát interdiszciplináris feladat, amely alapvetően támaszkodik a polgári kutatás-fejlesztési novumok folyamatos vizsgálatára, áttekinté-

sére és rendszerezésére annak érdekében, hogy a leginkább a katonai felhasználásra alkalmas, a katonai értelemben a megfelelő funkciókat ellátni képes applikációkat vegyék át. A polgári információs technológiák fejlődése, a fejlesztések iránya tehát nagyban befolyásolja a katonai információs rendszereink fejlesztését is. Ezen folyamatokhoz szorosan kapcsolódnak a 21. századi innovációkban a vezető elemeket képviselő közösségimédia-platformok megjelenése (mint *driver*ek), illetve a felhasználói számítógépes programok robbanásszerű fejlődése. Ezen platformok futtatása megköveteli a szélessávú adatátviteli hálózatok rendelkezésre állását, melyek lehetnek rez- vagy optikai összekapcsolású (hagyományos stacioner) hálózatok, amely mellett napjainkban egyre nagyobb teret nyernek a rádiófrekvenciás (mobil) adatátviteli hálózatokra épülő adatkapcsolati rendszerek. Utóbbiak az EU által szabványosított 4G/LTE, illetve egyre inkább az 5G mobilhálózati kapcsolatokat [28] használják ki a nagy mennyiségű adatátvitel igényével fellépő social platformok információtovábbítására. Kijelenthető, hogy a már Európában is jelen lévő, rendelkezésre álló és egyre nagyobb arányban globális szinten kiépülő úrtávközlés adja a 21. századi fejlett adatátvitel irányát. Ugyanakkor az úrtávközlés igényének mértéke és a kapcsolódó műszaki fejlesztések iránya jelenleg nehezen prognosztizálható. Nem zárhatjuk ki, hogy az úrtávközlésben a 2000-es évek mobilkommunikációjához hasonló, robbanásszerű fejlődés alakul ki.

Bill Clinton első elnöki periódusa folyamán (2003) fogadták el a *The National Information Infrastructure: Agenda for Action NNI* dokumentumot, amely a következőképpen fogalmaz a digitális hálózatokról, illetve az azok fejlesztéséhez kötődő nagyhatalmi törekvésekről, amelyek egyaránt értelmezhetőek a polgári és katonai törekvések oldaláról: „A fejlett információs infrastruktúra lehetővé teszi az amerikai vállalkozások számára, hogy versenyezzenek és győzedelmeskedjenek a globális gazdaságban. (...) Az információ a nemzet egyik legkritikusabb gazdasági erőforrása, a szolgáltatóipar, a feldolgozóipar, a gazdaság és a nemzetbiztonság szempontjából egyaránt. (...) A globális piacok és a globális verseny korában az információ létrehozására, manipulálására, kezelésére és felhasználására szolgáló technológiák stratégiai jelentőségűek az Amerikai Egyesült Államok számára.” [29] Nem felejtethetjük el, hogy az USA Földünk több szempontból is vezető nemzete és a NATO alapító tagországa, messze a legnagyobb gazdasági és katonai potenciállal bíró ország.

Az információs infrastruktúrák jelentőségének korai felismerése, a vezető technológiák kidolgozásának igénye és az informatikai iparágban a vezető szerep fenntartása



2. ÁBRA.
(Illusztráció: Shutterstock)

tehát alapvető amerikai stratégiai érdek, amelyhez való csatlakozás, a kutatás-fejlesztési eredmények figyelemmel követése, azok átvétele, még inkább ezen fejlesztésekben való európai részvétel (EU tagállami vállalkozások részéről) egyben az EU tagállamainak stratégiai érdekei is.

Vizsgáljuk hát meg, e globális technológiai verseny mely szegmensét tekinti az EU jelentősnek, érdemesnek a jelen és a közeljövő fejlesztéseire. Az Európai Parlament és Tanács egy határozatában szereplő gondolatsorát érdemes bemutatni. A *Digitális évtizedhez vezető út* elnevezésű, 2030-ig előre tekintő szakpolitikai programban az alábbiakat határozzák meg mint közvetlen fejlesztési irányokat: informatikai hálózatok fejlesztésének területén az európai közösség tagállamaiban, az egyéntől a vállalkozáson át, a közszolgáltatások területét is ide értve cél az ún. „gigabites” optikai hálózat európai szintű (lefedettségű) kialakítása; minden lakott településen az 5G mobilhálózati lefedettség kialakítása; nagy informatikai biztonsággal üzemelő informatikai ún. peremcsomópontok kiépítése és üzemeltetése; az uniós vállalkozások legalább 75%-ának bevonása a felhőalapú szolgáltatások használói körébe; a nagy adathalmazok (big data) használata; valamint az MI fejlesztése és szolgáltatásalapú használata, illetve további rendszerkialakítása. [30] Ezek együttes fejlesztése, folyamatos használata, majd a levont tapasztalatok alapján történő továbbfejlesztése növeli az EU digitális versenyképességét, és az előrelépés iránya(i) egyértelműen mutatják, hogy a kutatás-fejlesztés tendenciái, e forradalmi változások egyre inkább áttolódnak a kibertérbe, kiaknázva az ezen doménben rejlő nyilvános és rejtett képességeket is; a geopolitikai küzdelmek új terepe a kibertér (is) lett. [31]

A kibertér nagyarányú felhasználását leginkább az úgynevezett negyedik ipari forradalom (Ipar 4.0) digitalizált elemei, fejlett applikációinak alkalmazásai mutatják be. A 21. század a digitalizáció és az automatizáció (robotizáció) kora, ahol a fizikai hálózati környezet és a kibertér összekapcsolódása útján egyetlen, még nem teljesen önálló, de kimagaslóan intelligens információs környezet alakul ki. [32] Az Európai Parlament egy 2016-ban megfogalmazott állásfoglalása szerint: „Az Ipar 4.0 a termelési folyamatok szervezését írja le, mely keretében az alkotórészek, az eszközök önállóan kommunikálnak egymással, azonos értéklánc mentén. A jövőben ún. „okos” gyárat hozhatnak létre, ahol a számítógép-vezérelt rendszerek nyomon követik a fizikai folyamatokat (is), létrehozzák a fizikai valóság virtuális lenyomatát, majd önszervező mechanizmusaik alapján decentralizált döntéseket hoznak.” [33] Ilyen technológiák lesznek/ lehetnek az additív gyártás, a mesterséges intelligenciára épülő döntéshozatali rendszerek térnyerése, a bloklánc, a nagyméretű adatok kezelése, a felhőszolgáltatások, a dolgok ipari internete stb.

Úgy vélem, hogy a 21. századi digitális hálózati és az ezen hálózatokon végrehajtott polgári és katonai műveletek sikerét alapvetően határozzák meg az MI fejlesztései. [34] Ezen fejlesztések olyannyira felgyorsultak, hogy sokkal pragmatikusabb, technológiai oldalról jobban értelmezhetőbb, kézzelfoghatóbb a mesterséges intelligencia-rendszer (MI-rendszer) kifejezés, amit egyébként az EU jogalkotói is alkalmaznak. Ezen rendszerek alkotóelemei-



nek vizsgálata, összetevőinek rövid áttekintése és azok fejlesztési irányainak összefoglalása, valamint az MI-rendszerek katonai alkalmazásainak kérdései képezik alapelemeit ezen tudományos értekezésnek, amelyben alapvetően arra a kérdésre keresem a választ, hogyan támogathatják ezen MI-rendszerek a kiberbiztonság feladatrendszerét.

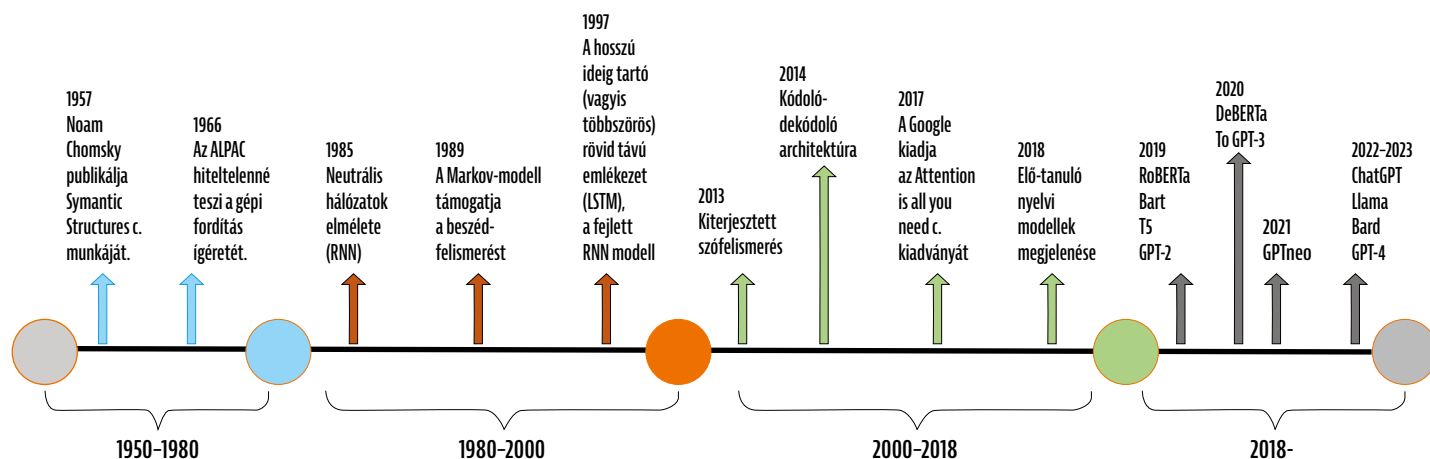
BEVEZETÉS A NAGY NYELVI MODELLEKBE (LLM)

Az MI-rendszer olyan szoftverek összessége, amelyek az ember által meghatározott célkitűzések közül, azok adott csoportja tekintetében olyan kimeneteket képesek generálni, amelyek tartalmakat, előjelzéseket, ajánlásokat és döntéseket biztosítanak. Ezek befolyásolják a környezetüket, amellyel kölcsönhatásba is lépnek. Ezen folyamatokban nagy szerepe van az ún. neurális hálózatokon [35] alapuló szoftverrendszereknek. Ez olyan technológia, amely alkalmazását a közelmúlt számítógépes forradalma gyorsított fel, ahol a nagy teljesítményű mikroszámítógépekkel, a nagy adathalmazokat rövid idő alatt feldolgozni képes számítástechnikai erőforrások nagyarányú alkalmazásával érjük el a kívánt hatásokat.

MI AZ LLM ÉS HOGYAN MŰKÖDIK?

A mesterséges neurális hálózatokat matematikai modellként mutatták be, [36] amely modell az emberi agy működését mintázza. Az alapneuron összetevői lehetnek alap bemeneti jelek, különböző műveletilelem-funkciók vagy kimeneti impulzusok. [37] Ezen neuronok hálózatot alkotnak, amelyek letéteményesei a kimeneten megjelenő jelek hasznosulásának. E folyamatot mélytanulásnak (*deep learning*) nevezzük, [38] ami az LLM tekintetében megkerülhetetlen. A mélytanulási folyamatok megértését leginkább az ún. ellenőrzött tanulási folyamatok rendszere támogatja. [39] A gépi tanulásban az algoritmusok alkalmazásával azonosítunk mintákat a vizsgálandó adathalmazokban, és ezen minták felhasználásával létrehozunk egy, az előjelzésekre alkalmas adatmodellt. A gépi feldolgozás, a gépi tanulási modellek fejlesztésével, nagy adathalmazok többszöri feldolgozását ismételve, ezen struktúrált és struktúrátlan adathalmazokban történő mintaazonosítást követően áttekinthetővé / áttekinthetőbbé válik az adatokban rejlő

3. ÁBRA.
(Illusztráció:
Shutterstock)



4. ÁBRA.

Az NLP fejlődése.

(Rövidítések:

ALPAC: Automatic Language Processing Advisory Committee
 RNN: Recurrent Neural Networks
 LSTM: Long Short-Term Memory
 RoBERTa: nyelvi tanulási modellek)
 DeBERTa: Decoding-enhanced BERT
 (Szerkesztette a szerző)

összefüggésrendszer. A folyamatmodellezés érdekében a mintákat úgy állítjuk össze, hogy azok a kimeneten elvárt „viselkedést”, paramétereket adják meg. [40] A nyelvi modell tehát olyan valószínűségi eloszlás a szavak, szósortozatok között, ahol a modell minden szóhoz valószínűségi értéket rendel egy bizonyos szekvenciában.

Más megközelítésben az algoritmusnak a mondatban / sorrendben a következő szót kell előre jeleznie, az előtte már rendszerezett és valószínűségük sorrendisége alapján kikövetkeztetett adathalmazból. [41] A nyelvi modellek fejlődésének mérföldköve volt az ún. „transzformer technológia” [42] megjelenése. Egyes kutatók állásfoglalása alapján ez a technológia szolgál alapul a ma ismert összes nagy nyelvi modell képzéséhez. E technológia alapja és a modern nyelvi modellek közös tulajdonsága, hogy szóbeágyazásokat (tokenek) használnak, [43] a szavakat vagy azok elemeit többdimenziós matematikai vektormennyiségekké alakítják át, és azt vizsgálják, hogy e vektortérben az egymáshoz közel eső szavak jelentése hasonló-e. A tokenizálás folyamán a feldolgozott és szétbontott, a legkisebb adatsomaghöz értékeket, azaz tokeneket rendelünk. [44]

Ezen tokenek szoftveres vizsgálatával, az ún. modelltanítási folyamat során a cél, hogy a szoftver mintegy „megjósolja” a következő, a hiányzó tokenet e szekvenciális hálózatban. [45] Így hoznak létre egy alapmodellt. A programozók felgyorsíthatják a tanulási folyamatokat azzal, hogy meghatározzák, és mintát biztosítanak a kimeneten elvárt követelményekről. Ha ezt elég gyakran elvégzik, a gépi tanulás felgyorsul; ezt felügyelt finomhangolós eljárásnak nevezik. [46] Ugyanakkor nyilvánvaló, hogy a betanítási folyamat e jelen fejlettségi szinten óriási számítógépes memóriát és nagy jel- (adat-) feldolgozási sebességet és processzorteljesítményt igényel. [47] Nem meglepetés tehát, hogy csak a valóban világméretű, az adatkezelésben vezető óriásvállalkozások (pl. Google, AWS, Microsoft, Oracle) mint nagy informatikai iparági képviselők, képesek a gépi tanuláshoz szükséges számítási teljesítményre képes hardverállományt mozgósítani.

NATURAL LANGUAGE PROCESSING (NLP) ÉS NATURAL LANGUAGE UNDERSTANDING (NLU)

A gépi tanulási modellek fejlesztésének nagy lendületet adott, amikor 2019-től a GPT-applikációk megjelentek, és

a több millió mintavételt követően előbb megértették az emberi beszédet, később képessé váltak az emberi hang emulálására és értelmes válaszok megfogalmazására. A 4. ábra bemutatja a gépi tanulás időrendi fejlődését. [48]

Az ábrán pontosan követhető az a történeti fejlődés, amely magán viseli a 20. és a 21. század tudományos életének MI-jellegzetességeit. Már az 1950-es években zajlottak jelentős kutatások az MI alapösszetevőjének számító gépi tanulás tématerületén. Ezt az időszakot a szabályalapú taxonómiák használata és az előre magadott/meghatározott mintaillesztés jellemezte. Ezen időszakban a struktúratlan szövegfeldolgozást, az automatikus tartalomfeldolgozást angol nyelven programozták, lévén amerikai és angol kutatók voltak a tématerület úttörői. Ugyanakkor a 60-as évek végén máris megjelentek a pesszimista hangok, akik úgy ítélték meg, hogy a gépi tanulás sosem ér el arra a szintre, ami a valós felhasználását eredményessé teszi. Aztán az 1980-as években a gépi tanulási algoritmusokra való áttérés és a feladatok feldolgozásának statisztikai megközelítése, a rövid és hosszú távú memóriaegységek programozása megjelent a gyakoriságon alapuló szóbeágyazottság alkalmazásában. Mindezen modelleket azért tervezték, mert ezek adták vissza leginkább az emberi gondolkodás, az emberi beszéd sajátosságait. Ugyanakkor a 2000-es évektől a nyelvprogramozás túllépte az egynyelvi (angol) megkötést, és egyre több ország kutatócsoportjai fordultak a gépi tanulás, a beszéd-felismerés és beszédértés kutatási területe felé. A 2020-as évekre előállt az a helyzet, hogy nemcsak a nagy amerikai és brit egyetemeken, de az EU tagországaiban, valamint ázsiai egyetemeken (Kína, India, Japán) is jelentős tudású kutatócsoportok foglalkoznak a gépi tanulás fejlesztésével.

Ahogy a 4. ábrán látszik, elsősorban 2017-től, a gépi tanulás a természetes nyelvfeldolgozás (NLP) irányába mozdult el, illetve gyorsult fel. Az NLP célja, hogy a számítógép megértse a különböző nyelveket és szöveges információkat, azokat analitikus módon rendszerezze, kezelje, és a magas rendelkezésre állást biztosítsa a keresésben. Ugyanakkor a nagy nyelvi modellek valódi áttörése a természetes nyelvek megértésével kapcsolatos (NLU), ahol a szövegértés és a szemantikai elemzések elvégzése kerül a feladatvégzés fókuszába. [49] Az LLM

részterületei tehát arra irányulnak, hogy magasabb szinten legyünk képesek kommunikálni a számítógépünkkel, a számítógép-hálózatunkkal.

A NYELVI MODELLEK KATEGORIZÁLÁSA

A nyelvi modellek besorolását, kategóriák közé szorítását, osztályozását több kutatótársam is megpróbálta, és több értékes tudományos közlemény született e témakört feldolgozva. Általánosan elfogadott azonban a hármas felosztás, amely alapvetően a gépi modellek cél/funkció alapján történő besorolását tűzi ki célul.

Az első lehetséges kategória az úgynevezett előképzésre alkalmas modellek csoportja, amelyek hangolását a nagy adatbázisok áttekintésére, feldolgozására, elemzésére alakították ki. Ezen modell alapján a gépi tanulás alapvetően igényli a teljes adatbázisokon belüli hozzáférést és a kutatást azokon belül. Ezen feldolgozási folyamat alapján megvalósulhat változatos nyelvi minták, illetve nyelvi szerkezetek feltérképezése. [50] Példaképpen érdemes felsorolni a GPT-3 és GPT 3.5, a T5 és XLN alkalmazásokat. [51]

Újabb osztályt képeznek a már valamilyen dedikált vagy tényleges cél érdekében tervezett gépi tanulási modellek, melyek a már előre szkennelt hatalmas adatmennyiségeken úgynevezett finomhangolást végeznek, azaz a meghatározott keresési cél érdekében többször, újra meg újra szkennelik a rendelkezésre álló gigantikus mennyiségű adatkészleteket, [52] majd a találatok alapján ezen kisebb adatmennyiségekben egyre szűkebb spektrumban kutakodva állítják elő a keresett információkat. Ezen gépi tanulási modellek rendkívül hatékonyak a szövegosztályozásokban, célirányos kérdések megválaszolásában, akár érzelmek elemzéseiben. A BERT (Bi-directional Encoder Representations from Transformers) és változatai, fejlesztett verziói az ALBERT, a RoBERTa modellek a Google fejlesztései, melyek a hardver-evolúció eredményeképpen egyre kisebb feldolgozási (processzor) kapacitásigénnyel [53] és belsőmemóriai szükséglettel lépnek fel. [54]

E kategorizálás alapján a következő változat az úgynevezett multimodális modellek osztálya, ahol a szöveges adatbázisok rendszeréből kilépve képeket, hang- és videófájlokat is felhasználnak annak érdekében, hogy a modell közvetlenül és nagy hatékonysággal értse meg, [55] dolgozza fel a szöveges alapadatok és a képek, videófájlok közötti koherenciát. [56] E modell lehetővé teszi a képek és videófájlok szöveges leírását, és ennek inverzeként, képesek szöveges fájlok leírásaiból képeket vagy videófelvételt előállítani. [57] E nyelvi modell képviselői a CLIP, [58] a DALL-E [59] és az IBM Granite [60] applikációk.

A NAGY NYELVI MODELLEK ÁLTALÁNOS HASZNÁLHATÓSÁGA

Azt gondolom, célszerűbb lenne összegyűjteni azokat – az életünk minden szegmensére kiterjedő – tématerületeket, ahol *nem alkalmazzuk* a mesterséges intelligenciát, a nagy nyelvi modellek által biztosított mozgási szabadságot a fizikai és a szellemi élet minden területén. Egyre nyilvánvalóbb, hogy nincsenek, vagy alig vannak ilyen területek az online világban, a kibertérben. Ezen modellek alkalmazása szinte már önműködő, háttérben futó, észre-

vétlen és – kijelenthetjük – magától értetődő is. A következőkben mégis teszünk egy kísérletet, hogy – a teljesség igénye nélkül – felsoroljam, mely területeken alkalmazzuk a leginkább az MI vívmányait.

A szolgáltatásalapú polgári vállalkozásokban az úgynevezett chatbotok használata manapság már alapvetés. A chatbotok olyan fejlett alkalmazások, amelyek az NLP vívmányait felhasználva az emberihez nagyon hasonló módon képesek beszélgetésre és más interaktív együttműködésre. Az online felületeken egyszerre képesek kiszolgálni nagyszámú kommunikációs csatornát (például egy online vásárlásra szakosodott weboldalon futtatva, vagy egy szolgáltatócég, például villamosművek, vagy multi-kommunikációs [pl. Telekom, One, Yettel] vállalkozás ügyfélközpontú ügyintézését). A chatbotok az ügyfélkommunikáció alapján korlátoosan ugyan, de tanulni képesek. [61] A fejlettebb rendszerek felismerik az emberi szófordulatokat, valamint ezeket alkalmazzák is a kommunikációjuk folyamán. Ezen képességük, hatalmas tudástárak lehetővé teszi, hogy nagy mennyiségű emberi munkát váltsanak ki több adatbázis szimultán, többlépcsős vizsgálatával, az információk széles spektrumban történő kinyerésével. [62]

E tématerülethez szorosan kapcsolódik az online értékesítés folyamatának LLM-általi optimalizálása, felgyorsítása. Az LLM támogatja a célirányos marketinget és a kinyert adatok magasabb szintű osztályozását, értelmezését és feldolgozását. Az összegzett információkat a gépi tanulás támogatásával az emberi ügyintézési idő töredéke alatt lehetséges feldolgozni, rendszerezni és az eredményeket újra felhasználni a következő tranzakciók folyamán. Más megközelítésben, az ügyfél-visszajelzések alapján a nyelvi modell képessé vált tanulni és adaptálódni. [63]

Az LLM tanulási képessége abban is megmutatkozik, hogy az eredetileg kialakított programnyelvtől (elsősorban angol, francia, olasz vagy kínai) eltérő nyelveket is képes az emberi tanulási, emberi ismeretfeldolgozási folyamatokhoz képest töredék-időmennyiség alatt áttekinteni, elsajátítani, e nyelveken feladatokat megoldani. Az LLM különböző algoritmusokkal megérti a nyelvek különféle összefüggéseit, dialektusokat, egy adott tájegységre jellemző szófordulatokat, így nagymértékben és széles körben alkalmazhatóak szövegből a kulcsszavak kinyerésére, összefoglalók készítésére, de akár szöveges alapküldetések részletes elemzésére is. [64]

Ehhez szorosan kapcsolódó terület az LLM-nek a kutatás-fejlesztésben megjelenő, egyre karakteresebb szerepe. A nagy nyelvi modellek széleskörűen képesek jó vagy kiváló minőségű tudományos közlemény, folyóiratcikk, tanulmány, dolgozat, akár évfolyamdolgozat, diplomamunka elkészítésére, előállítására, hiszen a világ legszéleskörűbb adatkapcsolati rendszerében képesek keresést-kutatást, elemzést és összefoglalást végezni. De innen továbblépve, a későbbiekben az LLM akár képes lehet arra is, hogy önállóan, tudományos területen hajtson végre előrelépést, akár azonos stílusban, formázással, tartalmi összefüggések áttekintésével, nagyban utánozva a rendelkezésre álló, illetve a tudományos, akadémiai anyagokat. [65]

Nagy előrelépés az LLM alkalmazása esetén, hogy magas szinten képesek elemzések elkészítésére, statisztikai

megaadatok igen rövid idő alatti áttekintésére, a vonatkozó munkafolyamatok automatizálására. Ez teszi, teheti lehetővé közel valós idejű statisztikai jelentések összeállítását ügyféltrendekről vagy egy adott szakterület, üzleti terület piaci viszonyainak az áttekintéséről. [66]

Úgy vélem, az egyik legintenzívebb fejlődés, előrelépés az MI alkalmazása területén a képzés, az oktatás során valósul meg. Az LLM határozottan támogatja az egyénre szabott tantárgyprogramokat és tanulási stratégiákat. [67] Az egyetlen korlát itt a hálózatelérés biztosítása, ami lehet fizikai/statikus elérés (optikai hálózatelérés) vagy a modern 4/5G cellás lefedettség használata a mobilinternet és a szolgáltatások elérésére. Az oktatásban nemcsak az adatbázisok elérése tud felgyorsulni, hanem virtuális asszisztensek támogatásával egyénre szabott oktatási program valósulhat meg, amely a felhasználó sajátosságaihoz (elfoglaltságok, elérési módok stb.) idomul. [68] Fontosnak tartom megjegyezni, hogy a számítógépes, a mesterséges intelligenciát alkalmazó képzések, felkészülések folyamán az egyénre szabott tanulás folyamán a gépi tanulás (NLP és NLU) is fejlődik, felgyorsul. [69]

Katonai vonatkozásban a legígéretesebb LLM-alkalmazás a védelmi szoftverek fejlesztésében történő támogatás, ahol a meghatározott védelmi és biztonsági paraméterek alapján a fejlett gépi modellek igen rövid idő alatt képe-

sek előállítani, tesztelni, programozni azokat az alkalmazásokat, amelyek hozzájárulnak az adott nemzet, nemzetek, országok szövetsége, de akár világméretű egyesülések védelmi képességeinek növeléséhez. [70] Ezen védelmi szoftverek erős szoftvervédelmet, kvantálást, kódolást, információvédelmet igényelnek. Az információvédelmi folyamatok automatizálásában, a tesztfolyamatokban és a statisztikai elemzésekben nagy támogatást nyújtanak az LLM elemei. Néhány fejlesztői platform máris alkalmazza a GPT-3 és GPT 3.5 és 4.0 szoftvertervezői képességeit, és e folyamatok irányai jelenleg előre nem láthatóak, de igen kecsegtető lehetőségeket rejtenek a védelmi szektorban is. [71]

A tudományos közlemény második részében összefoglalom az LLM és a kibervédelem lehetséges kapcsolódásait, bemutatom a védelmi szektorban elérhető, megvalósítható eljárásrendeket és megoldásokat.

A 2022-2.1.1-NL-2022-00012 azonosító számú Kooperatív Technológiák Nemzeti Laboratóriuma projekt a Kulturális és Innovációs Minisztérium Nemzeti Kutatási, Fejlesztési és Innovációs Alapból nyújtott támogatásával, a 2022-2.1.1-NL Nemzeti Laboratóriumok Létrehozása, Komplex Fejlesztése pályázati program finanszírozásában valósul meg. ■

(Folytatjuk)

HIVATKOZÁSOK

- [1] Az Európai Unió hivatalos internetes oldala. 2025.02.10. https://european-union.europa.eu/index_it (Letöltve: 2025.01.31.)
- [2] Az EUROPOL hivatalos internetes oldala. 2025.02.01. <https://www.europol.europa.eu/about-europol-it> (Letöltve: 2025.01.31.)
- [3] Az EUROPOL figyelemztetése. 2025.01.31. <https://www.europol.europa.eu/media-press/newsroom/news/criminal-use-of-chatgpt-cautionary-tale-about-large-language-models> <https://doi.org/10.1055/a-2436-4957> (Letöltve: 2025.01.31.)
- [4] A Nemzeti Kibervédelmi Intézet közleménye. 2025.01.31. <https://nki.gov.hu/it-biztonsag/hirek/a-chatgpt-veszelyeire-figyelmeztet-az-europol/> (Letöltve: 2025.01.31.)
- [5] A Szabályozott Tevékenységek Felügyeleti Hatósága hivatalos internetes oldala. 2025.02.11. <https://sztfh.hu/tevekenysegek/kiberbiztonsagi-tanusitas/kiberbiztonsagi-felugyelet/> (Letöltve: 2025.02.11.)
- [6] A SecurityOpenLab hivatalos internetes oldala. 2025.02.10. <https://www.securityopenlab.it/news/4555/ai-e-cybercrime-il-quadro-italiano-le-sfide-per-il-2025.html> (Letöltve: 2025.02.11.)
- [7] Az OpenAI hivatalos internetes oldala. 2023.03.13. <https://openai.com/index/gpt-4/> (Letöltve: 2025.03.14.)
- [8] Cisternino, A.: GPT-4o, ecco la vera svolta della nuova intelligenza artificiale. 2024.05.15. <https://www.agendadigitale.eu/mercati-digitali/gpt-4o-lia-oltre-la-chat-cosa-cambia-e-cosa-si-potra-fare-gratis/> (Letöltve: 2025.05.15.)
- [9] Az EUROPOL hivatalos internetes oldala. 2025.02.01., 8–9. <https://www.europol.europa.eu/cms/sites/default/files/documents/Tech%20Watch%20Flash%20-%20The%20Impact%20of%20Large%20Language%20Models%20on%20Law%20Enforcement.pdf> (Letöltve: 2025.02.12.)
- [10] AI-vezérelt Social Engineering: a kiberbiztonság új kihívásai. 2024.12.06. <https://index.hu/info/2024/12/06/ai-vezerealt-social-engineering-a-kiberbiztonsag-uj-kihivaisai/> (Letöltve: 2025.02.02.)
- [11] A Nemzeti Kibervédelmi Intézet hivatalos internetes oldala. 2025.02.15. <https://nki.gov.hu/it-biztonsag/hirek/veszelyesek-lehetnek-a-harmadik-feltol-szarmazo-chatgpt-pluginok/> (Letöltve: 2025.02.17.)
- [12] Agenzia per la cybersicurezza nazionale hivatalos internetes oldala. 2025.02.14. <https://www.acn.gov.it/portale/strategia-nazionale-di-cybersicurezza> (Letöltve: 2025.02.17.)
- [13] Dematteo, F.: La nuova impresa di Trump da 500 miliardi di dollari nell'IA è un campanello d'allarme per gli investitori'. 2025.01.22. <https://it.investing.com/news/stock-market-news/la-nuova-impresa-di-trump-da-500-miliardi-di-dollari-nellia-e-un-campanello-dallarme-per-gli-investitori--green-di-devere-93CH-2658424> (Letöltve: 2025.02.01.)
- [14] Guerini, R.: In AI funding and research, China and US outperform Europe. Science and Business 2024.05.21. <https://sciencebusiness.net/news/ai-funding-and-research-china-and-us-outperform-europe> (Letöltve: 2025.05.23.)
- [15] Macron urges European action to attract AI projects 2025.02.10. Le Monde https://www.lemonde.fr/en/france/article/2025/02/10/macron-urges-european-action-to-attract-ai-projects_6738003_7.html (Letöltve: 2025.02.11.)
- [16] Az OpenAI hivatalos internetes oldala. 2025.02.15. <https://openai.com/index/gpt-4o-and-more-tools-to-chatgpt-free/> (Letöltve: 2025.02.16.)
- [17] Aglio, L.: Neumann, John, Enciclopedia dei ragazzi 2006, [https://www.treccani.it/enciclopedia/john-von-neumann_\(Enciclopedia-dei-ragazzi\)/](https://www.treccani.it/enciclopedia/john-von-neumann_(Enciclopedia-dei-ragazzi)/) (Letöltve: 2025.02.11.)
- [18] NATO – North Atlantic Treaty Organization. https://www.nato.int/nato-welcome/index_hu.html (Letöltve: 2025.02.19.)
- [19] The Prague Summit Declaration. http://www.nato.int/cps/en/SID-3D8E1C2E-E5B0BC8E/natolive/official_texts_19552.htm?selectedLocale=en (Letöltve: 2025.02.18.)
- [20] Bertolotti, C.: Sfide e minacce non convenzionali. Osservatorio Strategico, 2021/6, 2. https://www.difesa.it/assets/allegati/38334/07_bertolotti_os_6_2021_ita_web.pdf (Letöltve: 2025.02.18.)
- [21] Cebrowski, A. K. – Garstka, J. H.: Network-Centric Warfare: Its Origin and Future, Chapter: How can the military not change. Proceeding magazine. January 2008. US Naval Institute. <http://www.usni.org/magazines/proceedings/1998-01/network-centric-warfare-its-origin-and-future> (Letöltve: 2025.02.01.)
- [22] Kovács, L.: Információs háborúk: célpontok, eszközök stratégiák. Előadás, ZMNE Információs Műveletek és Elektronikai Hadviselés Tanszék. https://www.hte.hu/documents/10180/4737479/P1_3_Prof_Dr_Kovacs_Laszlo_Kibervedelmi_feladatok_a_honvedelemben.pdf (Letöltve: 2025.02.01.)
- [23] Viglietta, R.: The Italian Army And Effects-Based Operations: A New Concept For An Army Of Use. School of Advanced Military Studies United States Army Command and General Staff College, Fort Leavenworth, Kansas, 2006, 33–53. <https://apps.dtic.mil/sti/tr/pdf/ADA450638.pdf> (Letöltve: 2025.02.15.)
- [24] Haig, Zs.: Kritikus infrastruktúrák és kritikus információs infrastruktúrák. Nemzeti Közszolgálati Egyetem, tanulmány 2012, 105–119. https://www.uni-nke.hu/document/uni-nke-hu/kritikus_infrastrukturak.pdf (Letöltve: 2025.02.16.)

- [25] Szternák, Gy.: Gondolatok a hatásalapú- és hálózatközpontú katonai műveletekről. *Hadtudományi Szemle* 2008/3, 1–7. https://real-j.mtak.hu/16787/7/hadtudomanyi_szemle_2008_03.pdf (Letöltve: 2025.03.12.)
- [26] Puligheddu, A.: FORZA NEC: al via la conferenza internazionale. *Network Enabled Capability Technology* 2017.02.02. <https://www.difesaonline.it/evidenza/eventi/forza-nec-al-la-conferenza-internazionale-network-enabled-capability-technology> (Letöltve: 2025.03.15.)
- [27] Kassai, K.: A Magyar Honvédség információvédelmének – mint a biztonság részének – feladatrendszere. Doktori (PhD) értekezés, Budapest 2007, 24–27. <https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/12088/ertekezés.pdf;jsessionid=C9D4EEF4B756ECC4B485F26D5274D93?sequence=1> (Letöltve: 2025.03.11.)
- [28] Servidio, G.: Quando arriverà il 6G, come sarà e che differenza c'è rispetto al 5G? 2025.02.15. <https://www.geopop.it/6g-cose-quando-arriva-e-differenza-con-5g/#> (Letöltve: 2025.03.12.)
- [29] Brown, R. H.: The national information infrastructure: agenda for action. Executive Office of the President, Information Infrastructure Task Force, 2003, 2.
- [30] Európai Bizottság: Javaslat az Európai Parlament és Tanács határozatára: „A digitális évtizedhez vezető út” szakpolitikai program. COM/2021/574 final, 2021.09.15.
- [31] Tálas, P.: A varsói NATO-csúcs legfontosabb döntéseiről. *Nemzet és Biztonság* 2016/2, 98–100. <https://doi.org/10.32576/nb.2024.2.3> (Letöltve: 2025.04.14.)
- [32] Ináncsi, M. – Dub, M.: Dezinformáció az Ipar 4.0 rendszerek elleni támadásokban. *Hadmérnök* 2024/3, 138–142. <https://doi.org/10.32567/hm.2024.3.10> (Letöltve: 2025.04.21.)
- [33] Industry 4.0 – Policy Department Economic and Scientific Policy, 2016. 22–23. [https://www.europarl.europa.eu/RegData/etudes/STUD/2016/570007/IPOL_STU\(2016\)570007_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2016/570007/IPOL_STU(2016)570007_EN.pdf) (Letöltve: 2025.03.12.)
- [34] Dalenogare L. S. et al.: The expected contribution of Industry 4.0 technologies for industrial performance. *International Journal of Product Economics*, 2018/204, 383–394. <https://doi.org/10.1016/j.ijpe.2018.08.019> (Letöltve: 2025.04.14.)
- [35] Coldewey, D.: Age of AI: Everything you need to know about artificial intelligence, 2023.07.11. <https://techcrunch.com/2023/07/11/age-of-ai-everything-you-need-to-know-about-artificial-intelligence/> (Letöltve: 2025.03.01.)
- [36] Bajjaoui, A.: A mathematical introductions of neural networks Advanced Mathematics. Master Program of the Universitat de Barcelona Barcelona, 2020.01.12. 10–31. https://diposit.ub.edu/dspace/bitstream/2445/180441/2/tfm_lichtner_bajjaoui_aisha.pdf (Letöltve: 2025.03.25.)
- [37] Guilhoto, L. F.: An Overview Of Artificial Neural Networks for Mathematicians. University of Chicago Department of Mathematics, 3–8. <https://math.uchicago.edu/~may/REU2018/REUPapers/Guilhoto.pdf> (Letöltve: 2025.03.26.)
- [38] LeCun Y. et al.: Deep learning. *Nature Magazine*, 2015.05.17. 436–444. <https://www.nature.com/articles/nature14539> (Letöltve: 2025.01.31.)
- [39] Goldberg: A primer on neural network models for natural language processing. *JAIR Vol. 57*, 2016.11.20. <https://doi.org/10.1613/jair.4992> (Letöltve: 2025.03.31.)
- [40] Rumelhart, D. E. et al.: Learning representations by back-propagating errors. *Nature Magazine* 1986.01.10, 533–535. <https://www.cs.utoronto.ca/~hinton/absps/naturebp.pdf> (Letöltve: 2025.01.12.)
- [41] Jurafsky D. – Martin J.H.: *Speech and Language Processing* (3rd ed. draft) 2023. <https://web.stanford.edu/~jurafsky/slp3/3.pdf> (Letöltve: 2025.01.15.)
- [42] Vaswani, A.: Attention Is All You Need. *Advances in Neural Information Processing Systems* 2017, 5998–6008.
- [43] Mikolov, T.: Efficient Estimation of Word Representations in Vector Space, 2013. <https://arxiv.org/pdf/1301.3781> (Letöltve: 2025.04.14.)
- [44] Wei, J. et al.: Emergent abilities of large language models, 2023. máj. <https://openreview.net/pdf?id=yzkSU5zdwD> (Letöltve: 2025.04.14.)
- [45] Wei J. et al.: Chain-of-Thought Prompting Elicits Reasoning in Large Language Models, *Correl University*, 2022.11.28. <https://arxiv.org/abs/2201.11903> (Letöltve: 2025.01.18.)
- [46] Karsa I. – Négyesi, A.: A nagy nyelvi modellek alkalmazhatóságának áttekintése a katasztrófavédelmi hatósági eljárások során. *Védelem-tudomány* 2024/2, 42–44. <https://doi.org/10.61790/vt.2024.15993>
- [47] Radford A. et al.: Language Models are Unsupervised Multitask Learners. Open AI website 2019. https://cdn.openai.com/better-language-models/language_models_are_unsupervised_multitask_learners.pdf (Letöltve: 2025.01.14.)
- [48] Mohana, N.: Natural Language Processing – presentazione. Avinashilingam University 2024, slide 05. <https://doi.org/10.13140/RG.2.2.13534.04169>
- [49] Chorowski, J.: Attention-based models for speech recognition, *Neural Information Processing Systems* 2015. Cornell University, 2015, 577–585. https://proceedings.neurips.cc/paper_files/paper/2015/file/1068c6e4c8051cfd4e9ea8072e3189e2-Paper.pdf (Letöltve: 2025.01.24.)
- [50] Mohamadi, S. et al.: ChatGPT in the Age of Generative AI and Large Language Models: A Concise Survey. 2023.07.09. <https://doi.org/10.48550/arXiv.2307.04251>
- [51] Ofosu-Ampong, K. et al.: Acceptance of Artificial Intelligence (ChatGPT) in Education: Trust, Innovativeness and Psychological Need of Students, *Information and Knowledge Management*, 2023/4, 37–47. https://www.researchgate.net/publication/372787378_Acceptance_of_Artificial_Intelligence_ChatGPT_in_Education_Trust_Innovativeness_and_Psychological_Need_of_Students (Letöltve: 2025.04.13.)
- [52] Hadi, M. U. et al.: A Survey on Large Language Models: Applications, Challenges, Limitations, and Practical Usage. *TechRxiv*, Aug 2024, https://www.researchgate.net/publication/383058502_Large_Language_Models_A_Comprehensive_Survey_of_its_Applications_Challenges_Limitations_and_Future_Prospects (Letöltve: 2025.04.11.)
- [53] Keya, A. J. et al.: Recurrent ALBERT for recommendation: A hybrid architecture for accurate and lightweight restaurant recommendations November 2023, *IET Wiley* https://www.researchgate.net/publication/375230162_Recurrent_ALBERT_for_recommendation_A_hybrid_architecture_for_accurate_and_lightweight_restaurant_recommendations (Letöltve: 2025.04.14.)
- [54] Bottyán, S.: A nagy nyelvi modellek működése és képzése, valamint alkalmazásuk stratégiai elemzése, 1. rész. *Nemzetbiztonsági Szemle* 2025/1, 77–95. DOI: 10.32561/nsz.2025.1.6 (Letöltve: 2025.08.30.)
- [55] What are multimodal language models? Applications, challenges and how they work <https://hu.shaip.com/blog/multimodal-large-language-models-mlms/> (Letöltve: 2025.01.25.)
- [56] UK Government Policy paper: A pro-innovation approach to AI regulation Updated. Part 3 and Part 4. 2023.08.03. <https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach> (Letöltve: 2025.01.15.)
- [57] McFarland, A.: Az 5 legjobb nyelvi modell (LLM) 2025 februárjában. 2024.09.19. <https://www.unite.ai/hu/legjobb-nagy-nyelvi-modellek-llms/> (Letöltve: 2025.01.25.)
- [58] Az OpenAI weboldala: <https://openai.com/index/clip/> (Letöltve: 2025.01.25.)
- [59] Az AI-pro.org weboldala: https://ai-pro.org/start-dall-e-c/?locales=it&keyword=dall-e&adid=725838274279&ppg=05&pmt=paydl&gad_source=1&gclid=CjwKCAiAnpy9BhAkEiwA-P8N4tXlPsl_VVhX6utx3olglQvlpYQW-CaD6taGpQNJ7s6i22QAcxaPxoCXocQAvD_BwE (Letöltve: 2025.01.22.)
- [60] Az IBM weboldala: https://www.ibm.com/it-it/granite?utm_content=SRCWW&p1=Search&p4=43700081258569042&p5=p&p9=58700008825608863&gad_source=1&gclid=CjwKCAiAnpy9BhAkEiwA-P8N4hrm2YDw-PiPuskmlHR3o5FSX6GDI4OgTaEElewhCHRAFir_oNuY8RoC2vQQAvD_BwE&gclid=aw.ds (Letöltve: 2025.01.25.)
- [61] Creativesite vállalkozás. Veszprém, Magyarország 2025. <https://creativesite.hu/webdesign-blog/mi-az-a-chatbot> (Letöltve: 2025.01.25.)
- [62] Tlili, A. et al.: What if the devil is my guardian angel: ChatGPT as a case study of using chatbots in education. *Smart Learning Environments*, 2023/1, 15. <https://slejournal.springeropen.com/articles/10.1186/s40561-023-00237-x> (Letöltve: 2025.03.14.)
- [63] Dwivedi, Y.: So what if ChatGPT wrote it? Multidisciplinary perspectives on opportunities, challenges and implications of generative conversational AI for research, practice and policy. *International Journal of Information Management* 71/2023, 102642. <https://forskning.ruc.dk/en/publications/so-what-if-chatgpt-wrote-it-multidisciplinary-perspectives-on-opp> (Letöltve: 2025.04.19.)
- [64] Wang, J.: On the Robustness of ChatGPT: An Adversarial and Out-of-distribution Perspective 2023. <https://arxiv.org/pdf/2302.12095.pdf> (Letöltve: 2025.01.25.)
- [65] Cotton, D.: Chatting and cheating: Ensuring academic integrity in the era of ChatGPT. *Innovations in Education and Teaching International* 2023, 1–12. <https://doi.org/10.1080/14703297.2023.2190148> (Letöltve: 2025.01.25.)
- [66] Dai, H.: ChatAug: Leveraging ChatGPT for Text Data Augmentation. 2023.02.28, 4–6. <https://it.scribd.com/document/695626214/2302-13007> (Letöltve: 2025.01.25.)
- [67] Pericles, R.: Artificial intelligence in teaching and learning: what questions should we ask of ChatGPT? *Interactive Learning Environments* 2023.02.22. 1–3. <https://it.scribd.com/document/760339411/Artificial-intelligence-in-teaching-and-learning-what-questions-should-we-ask-of-ChatGPT> (Letöltve: 2025.04.12.)
- [68] Duha, A. et al.: ChatGPT in Teaching and Learning: A Systematic Review. *Education Sciences* 2024/6, 18. <https://doi.org/10.3390/educsci14060643>
- [69] Adiguzel, T. et al.: Revolutionizing education with AI: Exploring the transformative potential of ChatGPT. 2023.03.28. *Contemporary Educational Technology*, 2023/3, 429. <https://www.cedtech.net/download/revolutionizing-education-with-ai-exploring-the-transformative-potential-of-chatgpt-13152.pdf> (Letöltve: 2025.04.12.)
- [70] Ray, P.: ChatGPT: A comprehensive review on background, applications, key challenges, bias, ethics, limitations and future scope. *Internet of Things and Cyber-Physical Systems* 2023/4, 121–154. https://www.researchgate.net/publication/370036739_ChatGPT_A_comprehensive_review_on_background_applications_key_challenges_bias_ethics_limitations_and_future_scope (Letöltve: 2025.04.13.)
- [71] Caballero, W. – Jenkins, P.: On LLM in national security applications. 2024.07.03. <https://arxiv.org/html/2407.03453v1> (Letöltve: 2025.04.14.)