

UPRAVLJANJE KRITIČNE INFRASTRUKTURE IN UMETNA INTELIGENCA

BOJANA VASIĆ, IZTOK PODBREGAR, MARINA DEŽMAN

Univerza v Mariboru, Fakulteta za organizacijske vede, Kranj, Slovenija
bojana.vasic1@um.si, iztok.podbregar@um.si, marina.dezman@um.si

Kritična infrastruktura je sistem, ki je vzpostavljen za nemoteno in stabilno delovanje držav in družbe. Pri tem je nesporno potrebno, da so grožnje in ranljivost sistema področje, ki ga je potrebno na nivoju države še posebej celovito in zadostno upravljati. Kritična infrastruktura vključuje številne medsebojno povezane in odvisne vitalne sektorje, in če pride do delnega ali popolnega izpada le enega sektorja, lahko to povzroči velike družbene in gospodarske posledice ter različne vrste kriz. Zato so zaščita, zagotavljanje in upravljanje kritične infrastrukture za vsako državo izrednega pomena. V prispevku želimo povezati vlogo kritične infrastrukture v družbi z elementi oz. trendi sprememb. Eden izmed njih je brez dvoma umetna inteligenca, pri čemer je kritična infrastruktura tudi izpostavljena omenjenemu trendu. Tako kot pretekla tveganja, ki so izhajala iz bodisi demografskih, gospodarskih, tehnoloških ali družbenih sprememb, so tudi tveganja, povezana z umetno inteligenco, prisotna v sistemih kritične infrastrukture. Gre za tveganja kibernetске varnosti, vprašanja, povezana z etiko in moralo in elementi, na katere bomo poskušali v prispevku čim bolj celovito odgovoriti.

DOI

[https://doi.org/
10.18690/um.fov.7.2025.5](https://doi.org/10.18690/um.fov.7.2025.5)

ISBN

978-961-299-059-6

Ključne besede:

kritična infrastruktura,
umetna inteligenca,
upravljanje,
tveganje,
sektor



Univerzitetna založba
Univerze v Mariboru

DOI
[https://doi.org/
10.18690/um.fov.7.2025.5](https://doi.org/10.18690/um.fov.7.2025.5)

ISBN
978-961-299-059-6

Keywords:

critical infrastructure,
artificial intelligence,
management,
risk,
sector

CRITICAL INFRASTRUCTURE MANAGEMENT AND ARTIFICIAL INTELLIGENCE

BOJANA VASIĆ, IZTOK PODBREGAR, MARINA DEŽMAN

University of Maribor, Faculty of Organizational Sciences, Kranj, Slovenia
bojana.vasic1@um.si, iztok.podbregar@um.si, marina.dezman@um.si

Critical infrastructure is the system that is in place for the smooth and stable functioning of countries and societies. It is indisputable that threats and vulnerabilities to the system are an area that needs to be managed, particularly at the national level, comprehensively and sufficiently. Critical infrastructure comprises many interconnected and interdependent vital sectors, and the partial or total failure of just one sector can lead to major social and economic consequences, as well as crises of various kinds. Therefore, the protection, provision, and management of critical infrastructure are of paramount importance for every country. In this paper, we aim to link the role of critical infrastructure in society to elements or trends of change, one of which is undoubtedly artificial intelligence, and critical infrastructure is also exposed to this trend. Like the risks of the past, which stemmed from demographic, economic, technological, or social changes, the risks associated with artificial intelligence are also present in critical infrastructure systems. These are cyber-security risks, issues related to ethics and morality, and elements that we will try to address as comprehensively as possible in this paper.



University of Maribor Press

1 Uvod

Koncept kritične infrastrukture in njenega pomena za ljudi se je sčasoma močno razvil, kar je odraz sprememb v družbi, tehnologiji in upravljanju. Ljudje so se vedno zavedali pomena osnovne infrastrukture, najprej v svojih prvih domovih, nato pa s cestami, mostovi in vodnimi sistemi, ki so omogočali trgovino, prevoz in komunikacijo. Ta zgodnji razvoj infrastrukture je postavil temelje za družbeni in gospodarski razvoj.

Industrijska revolucija je pomenila pomemben premik v razvoju infrastrukture, saj so se pojavile tovarne, železnice, telegrafi in drugi sistemi, ki so spodbudili hitro industrializacijo zahodnih družb. Infrastruktura je postajala vse bolj povezana in zapletena ter je podpirala urbanizacijo in množično proizvodnjo.

V 20. stoletju je bila prepoznana ključna vloga infrastrukture v nacionalni varnosti in obrambi. Med obema svetovnima vojnama je strateška infrastruktura, kot so železnice, пристanišča in komunikacijska omrežja, postala tarča vojaških napadov, kar je poudarilo njen pomen za vojaško logistiko in strateške operacije. Obdobje hladne vojne je poudarilo potrebo po odporni infrastrukturi, ki bo kos morebitnim grožnjam, vključno z jedrskimi napadi in sabotажami. Vlade so veliko vlagale v izgradnjo robustnih sistemov za energijo, telekomunikacije, promet in odzivanje na izredne razmere, da bi zagotovile neprekinjeno delovanje osnovnih storitev v primeru krize.

Digitalna doba je prinesla nove izzive in priložnosti za kritično infrastrukturo. Ker je družba postala vse bolj odvisna od medsebojno povezanih računalniških sistemov in omrežij, se je kibernetska varnost pojavila kot pereč problem. Sektorji kritične infrastrukture, kot so energetika, finance, zdravstvo in promet, so postali ranljivi za kibernetske napade, kar je poudarilo potrebo po zanesljivih ukrepih kibernetske varnosti za zaščito pred grožnjami.

Globalizacija je konec 20. in v začetku 21. stoletja povzročila večjo medsebojno povezanost in soodvisnost med državami in njihovimi infrastrukturnimi sistemi. Dobavne verige, prometna omrežja in finančni sistemi so postali vse bolj globalizirani, kar je ustvarilo nove priložnosti za trgovino in gospodarsko rast, hkrati pa povečalo potencialni vpliv motenj na svetovni ravni. Vse pogostejše in hujše

naravne nesreče ter učinki podnebnih sprememb so poudarili pomen odporne infrastrukture. Orkani, poplave, potresi in druge naravne nesreče lahko povzročijo obsežno škodo na kritični infrastrukturi, kar ovira bistvene storitve in predstavlja velik izziv pri prizadevanjih za obnovo in rekonstrukcijo.

Pandemija covid-19 je poudarila ključno vlogo infrastrukture pri podpori javnega zdravja in prizadevanj za odzivanje na izredne razmere. Sistemi zdravstvenega varstva, telekomunikacijska omrežja, dobavne verige in digitalna infrastruktura so imeli ključno vlogo pri obvladovanju krize, omogočanju dela na daljavo, zagotavljanju zdravstvenega varstva in razdeljevanju cepiva.

Ker se družba še naprej razvija in sooča z novimi izzivi, je zagotavljanje odpornosti in varnosti kritične infrastrukture še vedno glavna prednostna naloga vlad, podjetij in skupnosti po vsem svetu. Zaščita kritične infrastrukture je bistvenega pomena za nacionalno varnost in odpornost. Da bi zmanjšali tveganja in zagotovili neprekinjeno delovanje bistvenih storitev, je treba nenehno vlagati v ukrepe, kot so kibernetška varnost, redundanca, pripravljenost na izredne razmere in vzdrževanje kritične infrastrukture.

Po drugi strani je umetna inteligenca eden od najpomembnejših dosežkov, ki sooblikujejo človeštvo v 21. stoletju. V dobi digitalizacije postajajo prednosti in slabosti umetne inteligence vse bolj očitne, saj vplivajo na različne vidike našega življenja. Transformacijske zmožnosti umetne inteligence prispevajo k znatnemu napredku na različnih področjih življenja, bogatijo človekove izkušnje in rešujejo zapletene izzive na različnih področjih. Pojav umetne inteligence pri upravljanju in vzdrževanju kritične infrastrukture pomeni pomemben premik v načinu spremljanja, upravljanja in vzdrževanja teh bistvenih sistemov. Umetna inteligenca omogoča napovedno vzdrževanje kritične infrastrukture, kot so elektrarne, prometna omrežja in naprave za čiščenje vode. Z analizo podatkov iz senzorjev, naprav interneta stvari in preteklih zapisov o vzdrževanju lahko algoritmi umetne inteligence predvidijo okvare opreme, še preden do njih pride, kar omogoča pravočasne posege za preprečevanje dragih izpadov in motenj.

V nadaljevanju bomo na kratko predstavili opredelitev kritične infrastrukture ter umetne inteligence. Opredelili bomo uporabnost umetne inteligence v sektorjih kritične infrastrukture. Nazadnje pa bomo opisali nekatere prednosti in slabosti, ki jih je umetna inteligenca prinesla v sektorje kritične infrastrukture.

2 Kritična infrastruktura

Od nastanka prvih stavb je infrastruktura osnova za preživetje in razvoj civilizacije (Marković, 2017). Poleg gradnje se je moral človek, da bi jo čim bolj učinkovito uporabljal, naučiti tudi, kako jo zaščititi. V osemdesetih letih prejšnjega stoletja je izraz infrastruktura predstavljal referenčno točko za ustvarjalce javne politike in varnosti (Jakovljević & Gačić, 2012).

Pojav pojma kretniška infrastruktura (v nadaljevanju KI) je sledil naraščajočemu zaznavanju ogroženosti in soodvisnosti različnih infrastrukturnih elementov, ki skupaj naredijo državo in s tem družbo izjemno ranljivo za različne vrste napadov. Danes vprašanje zaščite KI predstavlja enega najpomembnejših varnostnih izzivov države, z vidika groženj KI pa velja za vprašanje, ki je za nacionalno varnost najpomembnejše.

Eno prvih poročil o kritični infrastrukturi je izšlo v Ameriki leta 1997 pod imenom *Critical Foundations: Critical Foundations: Protecting America's Infrastructures*, ki je po besedah Kathai Ann Brown (2006) omogočilo novo razumevanje moči in šibkosti same države. Veliko večja pozornost dojemanju ključnih informacij se pojavi po terorističnih napadih, najprej v New Yorku 11. septembra 2001, nato pa še po vrsti napadov v Evropi – v Parizu, Madridu, Moskvi, Londonu, Berlinu in Barceloni –, kar je potrdilo potrebo po novem dojemanju kritične infrastrukture in predvsem njene zaščite same.

Glavni cilj zaščite KI je zmanjšati njeno ranljivost, preprečiti teroristične in kibernetске napade, sabotaze ter preprečiti in ustaviti negativne posledice, ki bi se v večji ali manjši meri odrazile na večjem številu sektorjev in bi lahko privedle do delne ali popolne prekinitve normalnega delovanja infrastrukture. Zato je mogoče sklepati, da je ključna informacijska infrastruktura bistvenega pomena za normalno delovanje družbe.

Zaradi vse večje odvisnosti predvsem od informacijskih tehnologij se povečuje odvisnost med različnimi infrastrukturnimi sektorji in podsektorji. Na koncu se ta odvisnost ne konča z mejami ene države, temveč se kaže v mednarodni soodvisnosti različnih sektorjev v različnih državah, kar hkrati še dodatno otežuje že tako zapleten nadzor in zaščito kritičnega sektorja.

2.1 Opredelitev kritične infrastrukture

Do danes ni enotne, splošno sprejete opredelitve KI. Obstajajo različne opredelitve in razlage KI, ki so odvisne od konteksta in perspektive zainteresiranih strani. Tako po mnenju OECD (The Organization for Economic Co-operation and Development) kritična infrastruktura predstavlja »hrbtenico sodobnih, medsebojno povezanih gospodarstev«³. V okviru Evropske unije ključna infrastruktura vključuje elektroenergetska in prometna omrežja ter informacijske in komunikacijske sisteme⁴. Po mnenju vlade ZDA so kritična infrastruktura tista sredstva, sistemi in omrežja, ki zagotavljajo funkcije, potrebne za njihov način življenja⁵. V Republiki Sloveniji KI opredeljujejo zmogljivosti, ki so ključnega pomena za državo, in bi v primeru prekinitve njihovega delovanja nastale pomembne posledice za nacionalno varnost in gospodarstvo ter zdravje, varnost, zaščito in blaginjo prebivalstva⁶. Ob upoštevanju različnih opredelitev ključnih informacij je mogoče sklepati, da je opredelitev ključnih informacij in njihovih sektorjev stvar vsake države posebej.⁷

2.1.1 Razvrstitev sektorjev kritične infrastrukture

Opredelitev ključne infrastrukture je prvi potreben korak pri oblikovanju politike varnosti in zaščite ključne infrastrukture. KI vključuje širok nabor bistvenih sektorjev (predstavljeno v tabeli 1), ki so temeljnega pomena za normalno delovanje družbe in gospodarstva. Delna ali popolna odpoved katerega koli sektorja KI ima lahko daljnosežne posledice, vključno z ogrožanjem nacionalne varnosti, družbe, lahko pa privede tudi do nastanka različnih kriz v državi.

³<https://www.oecd.org/gov/risk/good-governance-for-critical-infrastructure-resilience-02f0e5a0-en.htm>

⁴https://joint-research-centre.ec.europa.eu/scientific-activities-z/critical-infrastructure-protection_en

⁵ <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience>

⁶<https://www.gov.si/assets/ministrstva/MO/Publikacije/Kriticna-infrastruktura-v-Republiki-Sloveniji.pdf>

Tabela 1: Sektorji, podsektorji in podsistemi kritične infrastrukture

Sektor/Sistem KI		Podsektor/Podsistem KI	
Sektor energetike		Naftna industrija	Naftna podjetja, rafinerije nafte, prevoz goriva in končni uporabniki
		Plinska industrija	Pridobivanje zemeljskega plina, proizvodnja plina, distribucija in prodaja plina
		Električna industrija	Proizvodnja električne energije, njena distribucija in prodaja
		Rudarska industrija	Premogovniki
		Industrija jedrske energije	
		Industrija obnovljivih virov energije	Vključuje podjetja, ki se ukvarjajo z alternativnimi viri energije in trajnostnimi viri energije, vključno s podjetji, ki se ukvarjajo s proizvodnjo hidroelektrične energije, proizvodnjo vetrne in sončne energije, ter podjetja, ki se ukvarjajo s proizvodnjo in distribucijo alternativnih goriv
		Tradicionalna energetika, ki temelji na zbiranju in distribuciji drv (še vedno prisotna in celo zelo pomemben podsektor energetike, zlasti v revnih državah)	
	Telekomunikacije	Kompleksen sklop sistemov, ki vključuje veliko število tehnologij in storitev	Vključuje žične, brezžične, kabelske in radiodifuzne tehnologije, osrednja omrežja, ki temeljijo na internetnem protokolu, ter notranje informacijske sisteme
Sektor prometa		Zračni	Infrastruktura Vozila Ceste
		Železniški	
		Po cesti	
		Vodni	
		Po cevovodu	
		Vesolje	
	Voda	Oskrba z vodo	Nadzor nad količino in kvaliteto vode
	Hrana	Kanalizacija	
Zdravstveno varstvo		Bolnišnice	Infrastruktura
		Zdravstveni centri	Medicinski pripomočki
		Službe nujne pomoči	Vozila

	Sektor/Sistem KI	Podsektor/Podsistem KI	
	Finance	Depozitne institucije, ponudniki naložbenih produktov, zavarovalnice, druge kreditne in finančne organizacije ter ponudniki kritičnih finančnih storitev in storitev, ki podpirajo te funkcije	
	Varstvo okolja		
	Civilna uprava	Vladni objekti in funkcije, vojska, civilne upravne službe, službe za ukrepanje ob nesrečah, poštne in kurirske storitve	

Vir: Lasten

Številni sektorji kritične infrastrukture so med seboj povezani, kar pomeni, da ima lahko motnja v enem sektorju močne učinke na druge. Na primer, kibernetški napad na finančno institucijo bi lahko vplival na prometne sisteme, saj bi bila motena obdelava plačil, kar poudarja potrebo po celostnem pristopu k zaščiti kritične infrastrukture. Soodvisnost sektorjev ni enotna in se nanaša tako na geografske kot funkcionalne posebnosti. Funkcionalna odvisnost vključuje logične, kibernetške in fizične soodvisnosti. Po Marković (2017) se soodvisnost pomembnih infrastruktur določi na podlagi naslednje lestvice:

- 0 – ni soodvisnosti med infrastrukturami (0–1 %),
- 1 – soodvisnost med infrastrukturami je majhna (2–33 %),
- 2 – med infrastrukturami obstaja zmerna soodvisnost (34 %–66 %),
- 3 – medsebojna odvisnost infrastruktur je visoka (67–98 %),
- 4 – med infrastrukturami obstaja popolna soodvisnost, tj. so popolnoma odvisne druga od druge (99–100 %).

Hiter tehnološki napredek prinaša nove ranljivosti in grožnje KI, kot so kibernetške grožnje informacijskim sistemom ali podnebne spremembe, ki vplivajo na proizvodnjo in distribucijo energije. Prepoznavanje in zmanjševanje teh novih groženj zahteva stalno spremljanje in prilagajanje zaščitnih ukrepov, kar je deloma mogoče doseči z ustreznim določanjem stopnje soodvisnosti med sektorji KI.

2.2 Zaščita kritične infrastrukture

Natančni in posodobljeni podatki o KI, ranljivostih in soodvisnostih so bistveni za učinkovito oceno tveganja in določitev prednostnih nalog. Vendar se lahko razpoložljivost in kakovost podatkov razlikujeta po sektorjih in regijah, kar predstavlja izziv za celovito analizo in sprejemanje odločitev.

Zaščita kritične infrastrukture pogosto vključuje sodelovanje med vladnimi agencijami, subjekti zasebnega sektorja in drugimi zainteresiranimi stranmi. Vzpostavitev učinkovitih partnerstev in mehanizmov za izmenjavo informacij je lahko izziv zaradi različnih prednostnih nalog, pomislekov glede lastniških informacij in regulativnih okvirov.

Za reševanje teh skupnih težav države uporabljajo različne metodološke in politične pristope, prilagojene njihovim posebnim okoliščinam in potrebam. Ti pristopi lahko vključujejo metodologije ocenjevanja tveganja, sektorske predpise in standarde, javno-zasebna partnerstva, mehanizme mednarodnega sodelovanja in pobude za krepitev odpornosti. Na splošno je za obvladovanje kompleksnosti zaščite kritične infrastrukture potreben multidisciplinaren pristop z več deležniki, ki poudarja sodelovanje, izmenjavo informacij, obvladovanje tveganj ter stalno prilagajanje na spreminjajoče se grožnje in izzive.

Medsektorski pristop se je zaradi soodvisnosti med sektorji in samimi sektorji, ki se ne konča znotraj meja ene države, izkazal za enega boljših pristopov k varstvu KI. Medsektorski pristop k opredelitvi ključnih infrastrukturnih sektorjev temelji na temeljiti preučitvi ključnih meril za učinkovito določanje prednostnih nalog in zaščito ključne infrastrukture. Z analizo teh meril je mogoče razviti celovito razumevanje pomembnosti in soodvisnosti različnih sektorjev. Nekatera merila lahko opredelimo na naslednji način:

- določanje stopnje nevarnosti, ranljivosti in tveganja za določen sektor;
- predvidena škoda za družbo, ki bi nastala zaradi odpovedi infrastrukturnega sektorja;
- čas, ki preteče od trenutka odpovedi infrastrukture do izbruha krize;

- čezmejne posledice (določitev čezmejnih posledic v primeru odpovedi ali prenehanja delovanja določene infrastrukture, kar hkrati omogoča reševanje skupne ranljivosti in povečanje zaščite pred nadnacionalnimi grožnjami);
- opredelitev stopnje soodvisnosti infrastrukturnih sektorjev;
- natančna opredelitev kritičnih objektov in geografskega območja, na katerem se nahajajo;
- stopnja odgovornosti, ki izhaja iz položaja upravljavca, upravljavca infrastrukture in lastnika;
- lastniška struktura infrastrukturnega objekta, ki zagotavlja informacije za sprejemanje odločitev glede upravljanja, regulacije in naložb v ukrepe zaščite in odpornosti;
- pravna podlaga;
- jasno načrtovani in izvedeni varnostni ukrepi za vsako KI.

S sistematičnim ocenjevanjem teh meril v različnih sektorjih lahko oblikovalci politik razvijejo ciljno usmerjene strategije in učinkovito razporedijo sredstva za izboljšanje odpornosti in varnosti kritične infrastrukture proti številnim grožnjam in ranljivostim. Ob upoštevanju zapletene soodvisnosti sektorja KI je v zadnjih letih za številne vlade postalo zelo nujno, da zgradijo odporne sisteme KI, ki bodo zagotovili nadaljnje delovanje nacionalnega gospodarstva (Osei-Kyei, Tam, Ma & Mashiri, 2021).

Razumevanje, da ranljivosti kritične infrastrukture ni mogoče popolnoma odpraviti, poudarja pomen učinkovitih strategij blaženja in ukrepov pripravljenosti. Med zunanjimi grožnjami se teroristične grožnje pogosto štejejo za posebej resne, saj lahko povzročijo obsežne motnje in škodo.

3 Umetna inteligenca

Umetno inteligenco (v nadaljevanju UI) razumemo kot pojem, kjer naprave skušajo posnemati človeško inteligenco. Enotne definicije, kaj je to UI, ni, saj gre za pojem, ki se nenehno razvija. K razvoju UI pripomore razvoj tehnologije, ki napravam omogoča, da posnemajo vedenje ljudi. Zaradi nenehnega razvoja se postavlja veliko mejnikov UI, s tem pa se prilagaja tudi sama definicija (Petersson, 2023).

Izraz umetna inteligenca se je sprva začel kot preprosta teorija o človeški inteligenci, ki jo kažejo stroji. Leta 1979 je Jerrold S. Maxmen napovedal, da bo UI v enaindvajsetem stoletju prinesla 'postzdravniško dobo'. V današnji dobi hitrega tehnološkega napredka in eksponentnega povečanja izjemno velikih podatkovnih nizov je UI prešla iz teorije v oprijemljivo uporabo v obsegu brez primere. Od ocenjevanja izredno velikih podatkovnih nizov v skoraj realnem času, avtonomnih avtomobilov in priporočil za gledanje videoposnetkov, ki so pod vlivom zgodovine pretakanja, do spletnih nakupovalnih priporočil, oglasov in odkrivanja goljufij je UI postala temeljno zakoreninjena v mnogih vidikih družbe in pogosto deluje nevidno v ozadju naših osebnih elektronskih naprav (Helm, Swiergosz, Haeberle, Karnuta, Schaffer, Krebs, Spitzer & Ramkumar, 2020).

Umetna inteligenca se je začela pojavljati v petdesetih letih prejšnjega stoletja. Takrat je pojem UI predstavljal trud ljudi, da razvijejo naprave, ki bi bile sposobne izzvati človeka kot obliko življenja na planetu oz. njegovo inteligenco. Toda prišli smo do spoznanja, da je definicijo inteligence težko opredeliti, ker se tisto, kar dojemamo za inteligentno, nenehno spreminja (Petersson, 2023).

Ramesh, Kambhampati, Monson in Drew (2004) pravijo, da je UI področje znanosti in tehnike, ki se ukvarja z računalniškim razumevanjem tega, kar običajno imenujemo inteligentno vedenje, in z ustvarjanjem artefaktov, ki izkazujejo tako vedenje. Programi, ki računalnikom omogočajo, da delujejo tako, da se ljudem zdijo inteligentni, se imenujejo umetni inteligentni sistemi. Britanski matematik Alan Turing (1950 v Ramesh et al., 2004) je bil eden od utemeljiteljev sodobnega računalništva in umetne inteligence. Inteligentno vedenje v računalniku je definiriral kot zmožnost doseči zmogljivost na človeški ravni pri kognitivnih nalogah, kar je pozneje postalo znano kot Turingov test⁸.

Da pa lahko določimo, kaj je to umetna inteligenca, moramo najprej razjasniti pojem inteligenca. Ne obstaja enotna definicija inteligence, obstaja pa veliko različic, ki jih bomo predstavili v tabeli 2. Definicije bomo razdelili na tri področja:

⁸ Turingov test je bila pogosta metoda, ki se uporablja za ugotavljanje ali je bila dosežena človeška inteligenca. V testu se oseba pogovarja z neznano stvarjo na drugi strani, bodisi sistemom UI ali dejansko osebo. Če oseba, ki se pogovarja s strojem misli da gre za resnično osebo, potem naj bi stroj izkazoval vsaj nekaj inteligence (Rex, 2019).

- skupne definicije – definicije, ki so bile predlagane s strani organizacij in združenj,
- definicije psihologov,
- definicije raziskovalcev umetne inteligence.

Tabela 2: Definicije inteligence

	DEFINICIJA
SKUPNE DEFINICIJE	– Zmožnost uporabe spomina, razumevanja, domišljije, izkušenj, sklepanja in kritičnosti z namenom reševanja problemov in prilagajanja v situacijah (AllWords Dictionary, 2006); – Sposobnost učenja, razumevanja in odločanja oziroma imeti opcije, ki temeljijo na razumu (Cambridge Advance Learner's Dictionary, 2006); – Inteligenca je zelo splošna mentalna sposobnost, ki vključno s še drugimi stvarmi zajema sposobnost planiranja, abstraktnega mišljenja, sklepanja, učenja iz izkušenj, reševanja problemov, hitrega učenja in razumevanja kompleksnih idej (Skupna izjava, podpisana s strani 52 strokovnjakov); – Sposobnost učenja in sprejemanja dejstev ter veščin, še posebej, ko imamo te sposobnosti res dobro razvite (Encarta World English Dictionary, 2006); – Sposobnost uspešnega prilagajanja okolju, ali s spreminjanjem samega sebe, s spreminjanjem okolja ali iskanja novega okolja ... inteligenca ni le en mentalni proces, ampak kombinacija več procesov, ki so usmerjeni k učinkovitemu prilagajanju okolju (Encyclopedia Britannica, 2006).
DEFINICIJE PSIHOLOGOV	– Inteligenca ni ena enotna sposobnost, ampak je sestavljena iz več funkcij. Izraz označuje tisto kombinacijo sposobnosti, ki je potrebna za preživetje in napredovanje v določeni kulturi (A. Anastasi); – Tista stran uma, ki je osnova naše sposobnosti razmišljanja, reševanja novih problemov, sklepanja in poznavanja sveta (M. Anderson); – Pojem inteligenca bomo uporabili kot sposobnost organizma, da rešuje nove probleme (W. V. Bingham); – Človeka opredeljujemo kot inteligentnega, v kolikor se je sposoben prilagoditi okolju ali pa se je sposoben tega naučiti (S. S. Colvin, 2000);

	– Inteligenca je, kar je merjeno s testom inteligence (E. Boring).
DEFINICIJE RAZISKOVALCEV UI	– Sposobnost sistema, da ustrezno ukrepa v določenem okolju, kjer je ustrezna reakcija sistema tista, ki poveča verjetnost uspeha. Uspeh je doseganje vedenjskih podciljev, ki podpirajo končni cilj sistema (J. S. Albus, 1991); – Katerikoli sistem, ki se s pomočjo prilagodljivega vedenja približuje ciljem v različnih okoljih, lahko označimo za inteligenten sistem (D. Fogel, 1995); – Inteligenca je doseganje kompleksnih ciljev v kompleksnih okoljih (B. Goertzel, 2006); – Inteligenčna zmogljivost je uspešna (tj. ciljno dosegljiva) zmogljivost sistema v zapletenem okolju (J. A. Horst); – Inteligenca meri sposobnost agenta za doseganje ciljev v najrazličnejših okoljih (S. Legg in M. Hutter).

Vir: Povzeto po Legg & Hutter (2007)

Natančna definicija in pomen umetne inteligence je predmet številnih razprav in povzroča veliko zmede. Tako kot definicije inteligence ne moremo točno določiti, tudi definicije UI ni možno strniti v eno samo pravo definicijo. Na primer, en sam slovar podaja različne definicije UI (Cambridge Dictionary, 2024):

- uporaba ali preučevanje računalniških sistemov ali strojev, ki imajo nekatere lastnosti, ki jih imajo človeški možgani, kot je sposobnost interpretacije in ustvarjanja jezika na način, ki se zdi človeški, prepoznavanje ali ustvarjanje slik in reševanje problemov;
- uporaba računalniških programov, ki imajo nekatere lastnosti človeškega uma, kot je sposobnost razumevanja jezika, prepoznavanja slik in učenja iz izkušenj;
- študija o tem, kako izdelati računalnike, ki imajo nekatere lastnosti človeškega uma, kot je sposobnost razumevanja jezika, prepoznavanja slik, reševanja problemov in učenja;
- računalniška tehnologija, ki omogoča, da se nekaj naredi na način, ki je podoben načinu, kot bi to naredil človek.

Zaradi hitrega razvoja so se skozi čas spreminjale tudi definicije. Novejše definicije govorijo o posnemanju inteligentnega človeškega vedenja, kar je že veliko trdnejša definicija (Kok, Boers, Kusters, Putten & Poel, 2002). Nekako lahko vse definicije UI, ki obstajajo, razvrstimo v štiri kategorije:

- sistemi, ki razmišljajo kot ljudje,
- sistemi, ki delujejo kot ljudje,
- sistemi, ki razmišljajo racionalno,
- sistemi, ki delujejo racionalno.

3.1 Uporaba umetne inteligence

Evropska unija (v nadaljevanju EU) je prva, ki je izdala *Akt EU o umetni inteligenci*. Gre za prvi zakon o UI oz. regulativni okvir, katerega cilj je zagotoviti, da so sistemi UI varni in da spoštujejo pravo ter temeljne pravice in vrednote EU⁹.

UI ni nova tehnologija, saj nekatere tehnologije UI obstajajo že vrsto let. Napredek na področju računalniške zmogljivosti, razpoložljivosti velikih količin podatkov in nova programska oprema so v kratkem času privedli do velikih prebojev. Tako UI uporabljamo v mnogih vidikih vsakdanjega življenja za:

- virtualno pomoč,
- diagnoze v medicini,
- samodejno prevajanje,
- navigacijska orodja,
- nadzor kakovosti v proizvodnji,
- napovedovanje naravnih nesreč.

V nadaljevanju navajamo nekaj primerov uporabe UI v vsakdanjem življenju, za katere se mogoče niti ne zavedamo, da delujejo z njeno pomočjo¹⁰:

⁹ <https://www.consilium.europa.eu/sl/policies/artificial-intelligence/>

¹⁰ <https://www.europarl.europa.eu/topics/sl/article/20200827STO85804/kaj-je-umetna-inteligenca-in-kako-se-uporablja-v-praksi>

- spletno nakupovanje in oglaševanje – UI se uporablja za priporočila, prilagojena posamezniku, pri čemer analizira njegova pretekla iskanja in nakupe;
- iskanje na spletu – iskalniki so zmožni se učiti iz ogromnih količin podatkov, ki jih vnašamo uporabniki;
- digitalni osebni asistenti – pametni telefoni uporabljajo UI, da lahko zagotovijo relativen in posamezniku prilagojen izdelek; virtualni asistenti pa nudijo predloge na različnih področjih in nam pomagajo organizirati dan;
- strojni prevodi – programska oprema za prevajanje se zanaša na UI;
- pametni domovi, mesta in infrastruktura – pametni termostati se učijo našega vedenja, da prihranijo energijo (zmanjšajo ogrevanje, ko nas ni doma), snovalci pametnih mest pa upajo, da jim bo UI v pomoč pri urejanju prometa;
- avtomobili – samovozeča vozila še niso v uporabi, a avtomobili uporabljajo varnostne funkcije na podlagi UI; tudi navigacija temelji na UI;
- kibernetika varnost – sistemi UI pomagajo prepoznavati kibernetike napade in grožnje ter se borijo proti njim;
- UI proti covidu-19 – uporabljena je bila za termalne slike na letališčih in pridobivanje podatkov o širjenju bolezni;
- boj proti dezinformacijam – prepozna lahko lažne novice, tako da med podatki na družbenih omrežjih išče senzacionalistične vsebine ter prepozna, kateri viri so verodostojni.

Strnemo lahko, da UI prispeva k inovativnemu, učinkovitemu, trajnostnemu in konkurenčnemu gospodarstvu, hkrati pa se izboljša varnost, izobraževanje in zdravstveno varstvo prebivalstva. Podpira tudi boj proti podnebnim spremembam.

4 Umetna inteligenca v kritični infrastrukturi

Uporaba UI se razlikuje med posameznimi sektorji kritične infrastrukture. V nadaljevanju podajamo opredelitev, kako se metode UI uporabljajo v vsakem sektorju. Zavedamo se, da vseh vidikov uporabe UI ne moramo zajeti v našem pregledu, zato smo skušali navesti tiste vidike uporabe UI, ki se najpogosteje uporabljajo oz. so najbolj vidne navzven.

Sektor energetike

V energetskega sektorja se orodja UI uporabljajo za napovedovanje povpraševanja, zlasti na ravni stanovanj in zgradb (McMillan & Varga, 2022). Nadaljnje aplikacije vključujejo napovedovanje cen in upravljanja povpraševanja. Velik del se osredotoča tudi na proizvodne sisteme, kjer se številne najbolj razvite aplikacije nanašajo na infrastrukturo obnovljive energije. Robotika kaže velik potencial kot pomoč v naftnem, plinskem in jedrskem sektorju, vendar so do sedaj uporabljeni stroji še vedno omejeni v svoji avtonomiji. V sistemih obnovljivih virov energije se UI uporablja za napovedovanje oskrbe (meteorološko napovedovanje in sledenje soncu). UI pomaga naftni in plinski industriji povečati učinkovitost proizvodnih virov, demokratizirati strokovno znanje in povečati vrednosti, hkrati pa zmanjšati posledice za okolje.

Sektor preskrbe s pitno vodo

Metode UI so bile uporabljene v vseh vodovodnih omrežjih, od začetne obdelave vode do distribucije in izzivov, povezanih s potrošniki. Metode strojnega učenja pa so bile uporabljene pri razsoljevanju, kjer lahko vplivajo na načrtovanje obrata. Najbolj pa se UI uporablja za napovedovanje povpraševanja po vodi in napovedovanja cen na različnih geografskih lestvicah.

Sektor prometa

Prometni sektor je mogoče najbolj izpostavljen uporabi UI. Vrsta metod strojnega učenja je bila uporabljena za napovedovanje prometa in nesreč ter za navigacijska orodja. Podobna orodja so bila uporabljena pri napovedovanju povpraševanja in predvidevanja destinacij za taksi službe. Senzorji v vozilih in ob cestah lahko zagotovijo več podatkov o cestnih omrežjih kot kadarkoli prej, metode globokega učenja pa bodo verjetno igrale pomembno vlogo pri razvoju inteligentnega prometnega omrežja (McMillan & Varga, 2022). Robotika (zračna vozila brez posadke) izkazuje velik potencial pri spremljanju železniškega prometa, vendar pa je še vedno zelo odvisna od človeške interakcije. Orodja za globoko učenje so se izkazala za učinkovita pri diagnosticiranju napak v železniškem prometu visokih hitrosti. Pri avtobusnem omrežju pa UI pomaga pri vprašanih voznih redov.

Sektor informacijsko-komunikacijskih omrežij in sistemov

Metode strojnega učenja bodo pomembne za uspeh naslednje generacije brezžičnih omrežij – programsko definirana omrežja, optična omrežja in oblaki. Ocenjevanje uporabniške izkušnje in kakovosti omrežja, ki je lahko odvisno od dejavnikov, vključno z zakasnitvijo, tresenjem, stopnjo izgube in slikovno ali video definicijo, sta aktivni področji raziskav, ki uporabljajo vrsto klasifikatorjev strojnega učenja. Tudi tukaj se UI uporablja za napovedovanje prometa in povpraševanja. Varnost je kritična skrb vsakega brezžičnega omrežja, zato se UI uporablja za identificiranje zavrnitve storitve, vdorov in izbiri ustreznega odgovora.

Sektor zdravstva

Umetna inteligenca je prisotna tudi v zdravstvenem sektorju. UI pomaga pri reševanju trenutno problematičnih operativnih procesov zdravstvenega varstva, ki bi lahko vodili do zapletenih izzivov na točki oskrbe bolnikov. V pomoč je zdravnikom pri natančnosti in točnosti kirurških posegov. Medicinskim sestram pomaga neprenehoma nadzorovati pacientovo stanje (Park et al., 2020). UI pomaga pri napovedovanju in analiziranju vzorcev na podlagi podatkov, ki vplivajo na rezultate zdravljenja. Zmanjšuje negotovosti pri odločanju o zdravljenju z obdelavo velikih količin diagnostičnih medicinskih slik s samoučenjem. Zelo hitro tudi zna obdelati velike količine medicinskih slik, uporaba teh podatkov pa je v pomoč pri ugotovitvi, za katero bolezen gre, in pri oceni negativnih in pozitivnih rezultatov testov. UI lahko tudi dolge nestrukturirane besedilne podatke, torej zdravstvene kartone, pretvori v enostavno branje in interpretacijo.

Sektor financ

Uporaba UI v sektorju financ prinaša številne izboljšave. Uporablja se za modeliranje ekonomsko-finančnih mehanizmov, torej za modeliranje cen, odnosov, interakcij, trgovanja, gibanja tržnih mehanizmov, za razne simulacije in interakcije med deležniki. Nadalje se UI uporablja pri analizi in napovedovanju finančnih trgov (gibanje trga, trenda, dinamike itd.) ter pri agentski ekonomiji in financah (modeliranje in simuliranje trgov, ponudbe in povpraševanja, vedenje udeležencev, strategije itd.). UI je v veliko pomoč pri vzpostavljanju inteligentnega načina upravljanja kreditov, posojil in tveganj ter pri inteligentnih naložbah, optimizaciji in

upravljanju (Cao, 2020). Nenazadnje metode UI uporabljajo za inteligentno trženje, torej za razumevanje in predvidevanje potreb strank.

Sektor varovanja okolja

Umetna inteligenca se uporablja pri problemih okoliškega upravljanja, kot na primer pri uporabi strokovnih sistemov, ki ekipam za ukrepanje ob izrednih dogodkih svetujejo, kako ravnati v primeru industrijskih nesreč, pri uporabi strokovnih sistemov za pomoč pri izdajanju dovoljenj za odlaganje nevarnih odpadkov, pri modeliranju kakovosti vode, napovedi staleža rib in številnih drugih aplikacijah okoliškega inženiringa (Cortés et al., 2000).

Sektor prehrane

Trenutno postaja vse bolj pomembna vloga uporabe strojnega učenja v pred proizvodnji, proizvodnji, predelavi in distribuciji (Ben Ayed & Hanana, 2021). V prvi fazi se UI uporablja za napovedovanje pridelka, lastnosti tal in potreb po namakanju. V naslednji fazi proizvodnje faze UI pomaga pri odkrivanju bolezni in napovedovanju vremena. Pri predelavi gre za oceno načrtovanja proizvodnje za doseganje visoke in varne kakovosti izdelka. Pri zadnji fazi pa se strojno učenje uporablja zlasti pri analizi skladiščenja, transporta in potrošnikov. Vse skupaj pa je povezano z avtomatizacijo kmetijskih strojev, uporabo senzorjev in oddaljenih satelitskih podatkov ter strojnega učenja za izboljšanje spremljanje pridelka in vode za sledljivost kmetijskih živilskih proizvodov.

5 Prednosti in slabosti umetne inteligence v kritični infrastrukturi

V dobi tehnologije in predvsem digitalizacije ima umetna inteligenca eno ključnih vlog. Je močno orodje v rokah tistih, ki jo oblikujejo, poleg tega pa je močno orodje v vseh panogah, kjer jo je mogoče uporabiti. Eno ključnih vprašanj, ki se zastavlja, je, kdo je tisti, ki bo UI povedal, katere so dobre in katere slabe strani programa. Za to je potreben človek, kar na nek način samodejno postavlja pod vprašaj nepristranskost vsega, kar počne UI. Učinkovito izvajanje UI pri upravljanju KI zahteva prispevek različnih virov, vključno s podatkovnimi znanstveniki, področnimi strokovnjaki, inženirji in oblikovalci politik. Ti različni pogledi so bistveni za razvoj zanesljivih rešitev UI, ki zagotavljajo, da so usklajene z

organizacijskimi cilji, izpolnjujejo regulativne zahteve in obravnavajo specifične izzive posameznega okolja.

Upravljanje in vzdrževanje sektorja kritične infrastrukture, kot so energetika, promet, telekomunikacije in oskrba z vodo, s pomočjo UI dejansko predstavlja tako prednosti kot slabosti. Vendar edinstvenost vsakega okolja v sektorju KI pomeni, da pri uvajanju UI ni univerzalne rešitve, ki bi ustrezala vsem. Rešitve UI je treba prilagoditi posebnim potrebam, izzivom in zapletom vsakega okolja v sektorju kritične infrastrukture. Kar se dobro obnese pri upravljanju energetske infrastrukture, morda ne bo neposredno uporabno za prometne sisteme ali sisteme oskrbe z vodo. Prilagajanje vključuje prilagajanje algoritmov, vhodnih in izhodnih podatkov posebnim zahtevam posameznega okolja.

Algoritmi UI lahko analizirajo velike količine podatkov iz senzorjev in drugih virov ter napovedujejo okvare opreme, še preden do njih pride. To omogoča proaktivno vzdrževanje, ki skrajša čas izpada in preprečuje katastrofalne okvare. Hkrati lahko UI poveča učinkovitost z optimizacijo delovanja kritičnih infrastrukturnih sistemov s prilagajanjem parametrov v realnem času glede na spreminjajoče se razmere, kar vodi k večji učinkovitosti in manjši izgubi virov.

Velja, da lahko sistem, ki ga poganja umetna inteligenca, hitreje in natančneje kot človeški operaterji zazna varnostne nevarnosti, kot so puščanje v cevovodih ali okvare v električnih omrežjih, ter tako zmanjša tveganje nesreč in zagotovi varnost delavcev in javnosti. Z avtomatizacijo rutinskih opravil in optimizacijo dodeljevanja virov lahko UI pomaga zmanjšati operativne stroške pri upravljanju in vzdrževanju KI, kar pomeni finančne prihranke za organizacije in vlade.

Vsa infrastruktura za prenos elektrike, podatkov, vode, goriva ter zračnega, kopenskega in vodnega prometa je gonilna sila sodobne centralizirane družbe. UI lahko zagotovi učinkovitost vseh teh prenosov, kar bo zmanjšalo izgubo časa, energije in materiala. Povečala bo tudi zmožnost izogibanja vsaj nekaterim motnjam in zmanjšanja motenj, ki se pojavijo, na primer zaradi orkanov ali ledenih neviht.

Umetna inteligenca lahko izboljša sprejemanje odločitev z analizo kompleksnih podatkovnih nizov in zagotavljanjem vpogledov, ki omogočajo boljše odločanje pri načrtovanju infrastrukture, naložbah in upravljanju tveganj. Vendar pa je pogosto

potrebno človeško posredovanje za zagotavljanje nadzora, sprejemanje kritičnih odločitev in reševanje zapletenih situacij, ki jih UI sama težko obvlada.

Eden največjih izzivov je varnost samega sistema. Nekateri sistemi, v katerih se uporablja UI, vsebujejo zelo občutljive podatke in se nanašajo na sektorje KI, kot so bančništvo, vlada itd. Vnos takšnih podatkov v sistem UI lahko privede do resnih posledic, ki jih povzročijo hekerji, kakšna druga država itd. Infrastrukturni sistemi, ki podpirajo UI, so ranljivi za kibernetске napade, ki lahko motijo delovanje, ogrozijo celovitost podatkov ali celo sabotirajo kritične sisteme, kar predstavlja veliko varnostno tveganje. To pomeni, da morata biti sistem in delo v njem, da bi bila uspešna in da bi se lahko izboljševala, najprej varna.

Kot pri vsaki analizi podatkov so potrebni ustrezni podatki, zato je učinkovitost UI odvisna od kakovosti podatkov in zanesljivosti podatkov, na katerih se usposablja. Netočni ali pristranski podatki lahko privedejo do napačnih napovedi in odločitev, kar lahko ogrozi zanesljivost infrastrukturnih sistemov. Poleg tega sistemi UI delujejo na podlagi algoritmov in programiranja, kar pomeni, da nimajo človeku podobnih kognitivnih sposobnosti, kot so intuicija, ustvarjalnost in sposobnost abstraktnega razmišljanja.

Ena največjih skrbi, povezanih z UI, ki se pojavlja, so etični pomisleki. Upravljanje kritične infrastrukture s pomočjo umetne inteligence sproža etična vprašanja, povezana z zasebnostjo, nadzorom in algoritmično pravičnostjo. Obstajajo pomisleki glede tega, kako bi se lahko sistemi UI uporabljali za kršenje pravic posameznikov ali diskriminacijo določenih skupin. Napake ali motnje v delovanju bi lahko povzročile katastrofalne posledice, vključno z izgubo življenj, okoljsko škodo in gospodarskimi motnjami.

Z novo tehnologijo, ki jo prinaša UI, se lahko ljudje, ki so odgovorni za določene sektorje KI, soočijo s pomanjkanjem znanja in spretnosti. Premostitev vrzeli v znanju in spretnostih ter zagotovitev, da je osebje ustrezno usposobljeno za upravljanje infrastrukturnih sistemov z UI, je lahko izziv.

Sprejetje UI v KI se lahko sooči z regulativnimi ovirami, povezanimi z varnostnimi standardi, predpisi o zasebnosti podatkov in vprašanji odgovornosti. Oblikovalci politik morajo razviti ustrezne predpise in smernice za zagotovitev odgovorne in etične uporabe UI v tem kontekstu.

Na splošno velja, da UI sicer ponuja pomembne potencialne koristi za upravljanje in vzdrževanje KI, vendar je za izkoriščanje njenega polnega potenciala ob hkratnem zmanjšanju negativnih posledic bistvena skrbna preučitev povezanih tveganj in izzivov.

Uspešno izvajanje UI pri upravljanju KI pogosto vključuje sodelovanje med sistemi UI in človeškimi strokovnjaki. Človeški izvajalci prispevajo znanje o domeni, izkušnje in presoje, ki dopolnjujejo zmožnosti umetne inteligence. S sodelovanjem lahko ljudje in UI izkoristijo prednosti drug drugega in dosežejo boljše rezultate, kot bi jih lahko dosegli sami.

Z etičnega vidika se zahteva, da vsak program umetne inteligence kritičnega sistema presega človeško razumevanje. Že od samega začetka je treba postaviti jasne meje in izvajati navzkrižna preverjanja. Vsak sistem je treba navsezadnje omejiti tako v njegovem prostoru kot tudi v okviru samostojnega delovanja, pri čemer je treba zagotoviti človeški nadzor na vsaki meji. Da bi zaščitili sebe in KI, imajo ljudje etično odgovornost, da nobenemu sistemu UI ne dovolijo, da se razvije prek meja razumljivosti.

6 Zaključek

V današnjem vse bolj povezanem svetu je zaščita sistemov kritične infrastrukture najpomembnejša. UI je lahko dragocen zaveznik v tem prizadevanju. Toda njegova zloraba lahko predstavlja tveganje za kritične infrastrukturne sisteme.

Kritično infrastrukturo lahko ohlapno opredelimo kot sisteme, ki so tako pomembni za državo, da bi njihova nezmožnost ali uničenje izčrpavajoče vplivalo na nacionalno varnost, gospodarstvo ali javno zdravje in varnost.

Umetna inteligenca je strateška tehnologija, ki prebivalcem in podjetjem zagotavlja številne koristi, pod pogojem, da je humanocentrična, etična, trajnostna in spoštuje temeljne pravice in vrednote. Poleg tega izboljšuje produktivnost in učinkovitost,

kar okrepi konkurenčnost industrije in izboljša blaginjo prebivalstva. Prispeva tudi k iskanju rešitev za tiste najbolj pereče družbene izzive (boj proti podnebnim spremembam, degradacija okolja, trajnost in demografske spremembe, boj proti kriminalu).

Vključevanje UI v upravljanje in vzdrževanje KI ima ogromen potencial za izboljšanje zanesljivosti, odpornosti in učinkovitosti ob hkratnem zmanjšanju operativnih stroškov in zmanjšanju tveganj. Ker tehnologije umetne inteligence še naprej napredujejo, je pričakovati, da se bo njihova uporaba v sektorjih kritične infrastrukture pospešila, kar bo privedlo do varnejših, bolj trajnostnih in bolj odpornih infrastrukturnih sistemov.

Čeprav umetna inteligenca ponuja ogromen potencial za napredek človeštva, je treba njene prednosti uravnotežiti z njenimi slabostmi. Reševanje izzivov, kot so pristranskost, premestitev delovnih mest in etična vprašanja, zahteva skupna prizadevanja oblikovalcev politik, tehnologov in celotne družbe, da se zagotovi, da bo umetna inteligenca služila skupnemu dobremu in hkrati ublažila njene negativne učinke.

Medtem ko umetna inteligenca ponuja velike možnosti za izboljšanje zaščite in odpornosti kritične infrastrukture, je treba skrbno preučiti povezana tveganja in izzive. Za zaščito kritične infrastrukture v vse bolj digitaliziranem svetu je bistvenega pomena uravnoteženje prednosti zmogljivosti, ki jih poganja umetna inteligenca, z ukrepi za zmanjšanje ranljivosti in zagotavljanje zanesljive kibernetске varnosti. Z razvojem vedenjskih modelov lahko sistemi UI odkrijejo odstopanja in anomalije, ki so lahko znaki kršitev varnosti ali kibernetских napadov.

Rešitve UI napredujejo pospešeno in takšne rešitve naj bi bile bistvene za ustvarjanje pametnih mest in ustvarjanje inteligentnih kritičnih infrastruktur naše prihodnosti. Od energetike in električne energije/oskrbe do proizvodnje in zdravstva UI pomaga narediti naše najbolj ključne sisteme čim bolj učinkovite. UI ima neomejene priložnosti za znaten vpliv v naših najbolj temeljnih panogah. Ko je tehnologije dozorela in se uveljavila z impresivnimi rezultati, sta se njeno sprejemanje in izvajanje vztrajno povečevali.

Umetna inteligenca je že povsod okoli nas, v skoraj vseh delih našega vsakdanjega življenja. Kar zadeva KI, naj bi bila UI temelj naše globalne strategije v zvezi s prizadevanji za digitalno preobrazbo. Izzive pri sprejemanju, izvajanju in zaupanju je mogoče ublažiti tudi z uporabo razpoložljivih rešitev, zdaj in v naši prihodnosti.

Kaj vse nam bo še prinesla UI, je težko predvideti, zagotovo pa se bo še naprej pospešeno razvijala in krojila naša življenja. Nedvomno bo potrebno s sistemi UI ravnati previdno in nikakor ne smemo dopustiti, da UI postane neodvisna od človeške pomoči. Še posebej je to nujen korak v sistemih kritične infrastrukture, kjer se zlorabe lahko zgodijo hitro in imajo uničujoč vpliv na ljudi, podjetja in družbo samo.

V nadaljnjih raziskavah bi lahko še bolj podrobno preučili, kje vse se umetna inteligenca že uporablja v sistemih KI. Razvoj UI pa bo zagotovo prinesel še številne prednosti in slabosti pri uporabi v kritičnih infrastrukturah.

Literatura

- Ben Ayed, R. & Hanana, M. (2021). Artificial Intelligence to Improve the Food and Agriculture Sector. *Journal of Food Quality*, 2021. <https://doi.org/10.1155/2021/5584754>
- Cambridge Dictionary. (2024). *ARTIFICIAL INTELLIGENCE – Cambridge English Dictionary*. <https://dictionary.cambridge.org/dictionary/english/artificial-intelligence>
- Cao, L. (2020). AI in Finance: A Review. *SSRN Electronic Journal*. <https://doi.org/10.2139/SSRN.3647625>
- Cortés, U., Sánchez-Marré, M., Ceccaroni, L., R-Roda, I. & Poch, M. (2000). Artificial intelligence and Environmental Decision Support Systems. *Applied Intelligence*, 13(1), 77–91. <https://doi.org/10.1023/A:1008331413864/METRICS>
- Helm, J. M., Swiergosz, A. M., Haeberle, H. S., Karnuta, J. M., Schaffer, J. L., Krebs, V. E., Spitzer, A. I. & Ramkumar, P. N. (2020). Machine Learning and Artificial Intelligence: Definitions, Applications, and Future Directions. *Current Reviews in Musculoskeletal Medicine*, 13(1), 69–76. <https://doi.org/10.1007/S12178-020-09600-8>
- Jakovljević, V. & Gačić, J. (2012). ZAŠTITA KRITIČNE INFRASTRUKTURE U KRIZNIM SITUACIJAMA. *International Scientific Conference MANAGEMENT 2012*, 280–286. https://meste.org/konf/Arhiva/Man_2012/pdf/RADOVI/Jakovljevic.pdf
- Kok, J. N., Boers, E. J. W., Kusters, W. A., Putten, P. van der & Poel, M. (2002). ARTIFICIAL INTELLIGENCE: DEFINITION, TRENDS, TECHNIQUES, AND CASES. V *Knowledge for sustainable development: an insight into the Encyclopedia of life support systems* (Vol. 1).
- Legg, S. & Hutter, M. (2007). A Collection of Definitions of Intelligence. V *Advances in Artificial General Intelligence: Concepts, Architectures and Algorithms* (str. 17–24). IOS Press.
- Marković, D. (2017). *Ugrožavanje kritične infrastrukture i njena zaštita u republici Srbiji* [Master Thesis, Univerzitet u Beogradu, Terorizam, Organizovani Kriminal i Bezbednost]. <https://fedorabg.bg.ac.rs/fedora/get/o:21332/bdef:Content/get>

- McMillan, L. & Varga, L. (2022). A review of the use of artificial intelligence methods in infrastructure systems. *Engineering Applications of Artificial Intelligence*, 116. <https://doi.org/10.1016/J.ENGAPPAI.2022.105472>
- Osei-Kyei, R., Tam, V., Ma, M. & Mashiri, F. (2021). Critical review of the threats affecting the building of critical infrastructure resilience. *International Journal of Disaster Risk Reduction*, 60. <https://doi.org/10.1016/J.IJDRR.2021.102316>
- Park, C. W., Seo, S. W., Kang, N., Ko, B. S., Choi, B. W., Park, C. M., Chang, D. K., Kim, H., Kim, H., Lee, H., Jang, J., Ye, J. C., Jeon, J. H., Seo, J. B., Kim, K. J., Jung, K. H., Kim, N., Paek, S., Shin, S. Y., ... Yoon, H. J. (2020). Artificial Intelligence in Health Care: Current Applications and Issues. *Journal of Korean Medical Science*, 35(42), 1–11. <https://doi.org/10.3346/JKMS.2020.35.E379>
- Petersson, D. (2023). *AI vs. machine learning vs. deep learning: Key differences*. TechTarget. <https://www.techtarget.com/searchenterpriseai/tip/AI-vs-machine-learning-vs-deep-learning-Key-differences>
- Ramesh, A. N., Kambhampati, C., Monson, J. & Drew, P. J. (2004). Artificial intelligence in medicine. *Ann R Coll Surg Engl*, 86. <https://doi.org/10.1308/147870804290>
- Rex, M. (2019). Artificial Intelligence: Distinguishing between types & definitions. *Nevada Law Journal*, 19(3).