

Prihodnost revidiranja IKT in podajanja zagotovil v digitalnem svetu

33. MEDNARODNA KONFERENCA O REVIDIRANJU IN KONTROLI INFORMACIJSKIH SISTEMOV

15.10.2025 -16.10.2025

Pogled iz leta 2025 v prihodnost

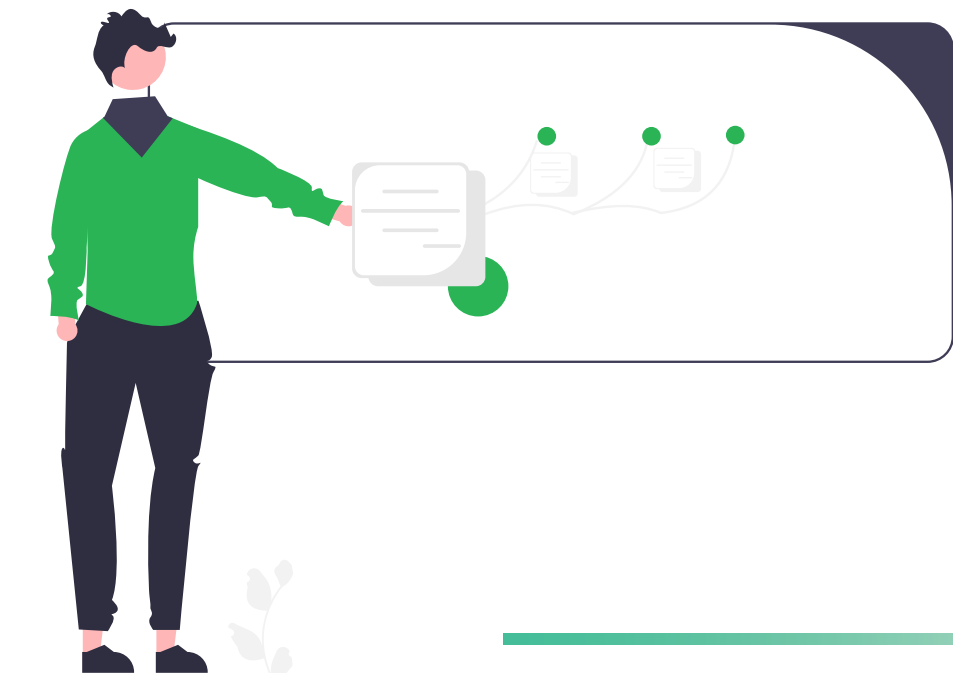
Renato Burazer, CISA, CISM, CRISC, CGEIT, CISSP

Član upravnega odbora ISACA Slovenija

AREM d.o.o., direktor

renato@arem-psn.com

Gradivo je last avtorja (Renato Burazer) v delu, ki ga je avtor pripravil sam in v lasti drugih avtorjev, ki so navedeni kot vir pri vsaki vsebini. Gradivo je namenjeno predstavitvi udeležencem 33. Mednarodne konference o revidiranju in kontroli informacijskih sistemov, ki ga organizira Slovenski inštitut za revizijo. Gradivo je predmet avtorske zaščite in drugih oblik zaščite intelektualne lastnine. Prepovedano je kakršnokoli reproduciranje, razen izključno za osebno uporabo in v nekomercialne namene, pri čemer se morajo ohraniti vsa opozorila o avtorskih ali drugih pravicah, zato se ne smejo prepisovati, razmnoževati ali kako drugače razširjati. Naveden mora biti tudi vir.



Zakaj je tema pomembna?

Digitalizacija = popolna odvisnost od IKT

Geopolitika + regulativa = nova kompleksnost

Zaupanje = Pogoji za ...

Revizor IS = varuh digitalnega zaupanja

- Revizija IKT z nadaljevanjem digitalizacije predstavlja enega od **temeljnih gradnikov zaupanja** v povezanem svetu.
- Vlade največjih svetovnih držav iščejo ravnovesje med svobodo in kontrolo, razvojem in inovacijami, hkrati pa **ščitijo svoje geopolitične in interese** tudi na račun dobrobiti za človeka in planet.
- EU v svojih strateških usmeritvah poudarja kibernetsko varnost in pri tem ni osamljena. Isto počno vsi drugi centri moči. Če je še ob začetku leta 2025 veljalo, da se EU lahko opre na ZDA kot večnega partnerja na vseh področjih, je mogoče ugotoviti, da je odvisnost EU od globalih deležnikov na področju IKT vseprisotna. Nadzor in **zaupanje v IKT** je tako vedno bolj kompleksen in **pomemben v celotnem arhitekturnem stolpu, ki podpira končne odjemalce storitev**.
- Prispevek postavlja revidiranje IKT v kontekst evropskih in svetovnih geopolitičnih in regulatornih silnic ter tehnološkega razvoja.
- Uporabljeni so nekateri izsledki raziskav ISACA in drugih virov. Predstavljen je prototip "Revizorja IS 2.0".
- Prispevek omogča pridobivanje ali osvežitev pogleda na prihodnost podajanja zagotovil v digitalnem svetu iz perspektive leta 2025.
- Pogled je podan na osnovi sinteze navedenih virov in razmišljanja avtorja.
- UI je bila uporabljena samo delno za označeno slikovno gradivo.

Digitalizacija = popolna odvisnost od IKT

FIZIČEN SVET



Vir: Generiral avtor (RB) z orodji UI – MS Copilot

DIGITALNI SVET

Renato Burazer, CISA, CISM, CRISC, CGEIT, CISSP

- **Zaupanje** je temeljni element družbenega kapitala – bistvenega pomena za kohezijo skupnosti, bistvenega pomena za učinkovito sodelovanje in ključnega pomena za gospodarski razvoj.

Our World
in Data

Vir: Our World in Data's mission is to publish the *"research and data to make progress against the world's largest problems."*

- zaúpanje -a s (û)

prepričanje, da je kdo sposoben, voljen narediti, kar se pričakuje: z delom upravičiti zaupanje koga; delavci so izkušeni, zato uživajo zaupanje; poln zaupanja prositi koga za pomoč / imeti zaupanje vase

// prepričanje, da je kdo pošten, iskren: zlorabiti zaupanje koga; ekspr. v slepem zaupanju mu je verjela

// prepričanje, da je kaj dobro in da bo dobro vplivalo na uresničitev določenih pričakovanj: zaupanje lastni moči / zaupanje v razum

- *publ. večina volivcev mu je izrazila zaupanje je glasovala zanj; knjiž. podarjati komu zaupanje zaupati vanj*

Vir: Slovar slovenskega knjižnega jezika, druga, dopolnjena in deloma prenovljena izdaja, www.fran.si, dostop 5. 10. 2025.

KOGNITIVNO ZAUPANJE

Kognitivno zaupanje je zaupanje ali pripravljenost stranke, da se zanaša na **usposobljenost** in **zanesljivost** ponudnika storitev (Moorman et al., 1992; Rempel et al., 1985). Izhaja iz **nakopičenega znanja**, ki nam omogoča, da z določeno stopnjo gotovosti **napovedujemo verjetnost**, da bo osrednji partner izpolnil svoje obveznosti. To je tisto, kar Rempel et al. (1985) imenujejo »predvidljivost«, Johnson-George in Swap (1982) pa »zanesljivost«. Znanje se zbira z opazovanjem vedenja partnerjev v osrednjem odnosu in iz poročanja o ugledu v drugih odnosih. Ko so učinki ugleda močni, so lahko začetne interakcije le priložnost za potrditev predhodnih zaznav, kognitivno zaupanje pa lahko postane dokončno v eni ali več interakcijah.

Vir: Cognitive and affective trust in service relationships, Devon Johnsona*, Kent Grayson

AFEKTIVNO ZAUPANJE

Afektivno zaupanje je zaupanje, ki ga človek položi v partnerja na podlagi občutkov, ki jih ustvarja raven skrbi in zaskrbljenosti, ki jo partner kaže (Johnson-George in Swap, 1982; Rempel et al., 1985). Zanj so značilni občutki varnosti in zaznana moč odnosa. Učinki ugleda vplivajo tudi na afektivno zaupanje, vendar je afektivno zaupanje odločno bolj omejeno na osebne izkušnje z osrednjem partnerjem kot kognitivno zaupanje.

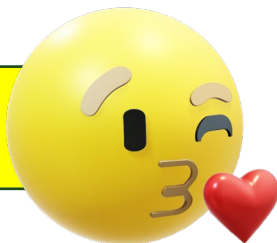
Bistvo afektivnega zaupanja je zanašanje na partnerja, ki temelji na čustvih.

Kaj je dovolj dobro za revizorja IS ?

Upanje

Sprejemanje, ki temelji na čustvih.

AFEKTIVNO
ZAUPANJE



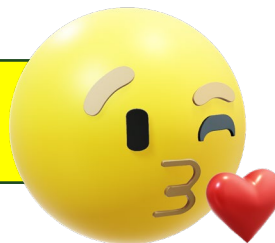
Zaupanje

Temelji na intelektu in čustvih. Temelji na nepopolnih dokazih.

KOGNITIVNO
ZAUPANJE

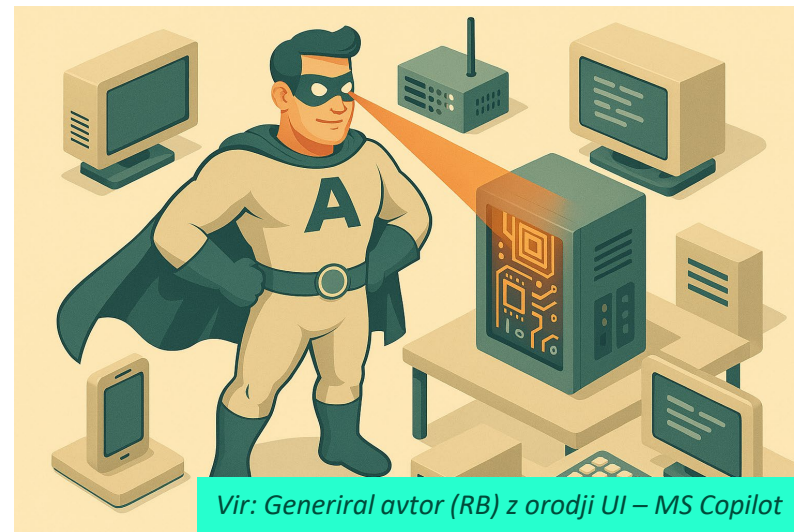


AFEKTIVNO
ZAUPANJE



Gotovost

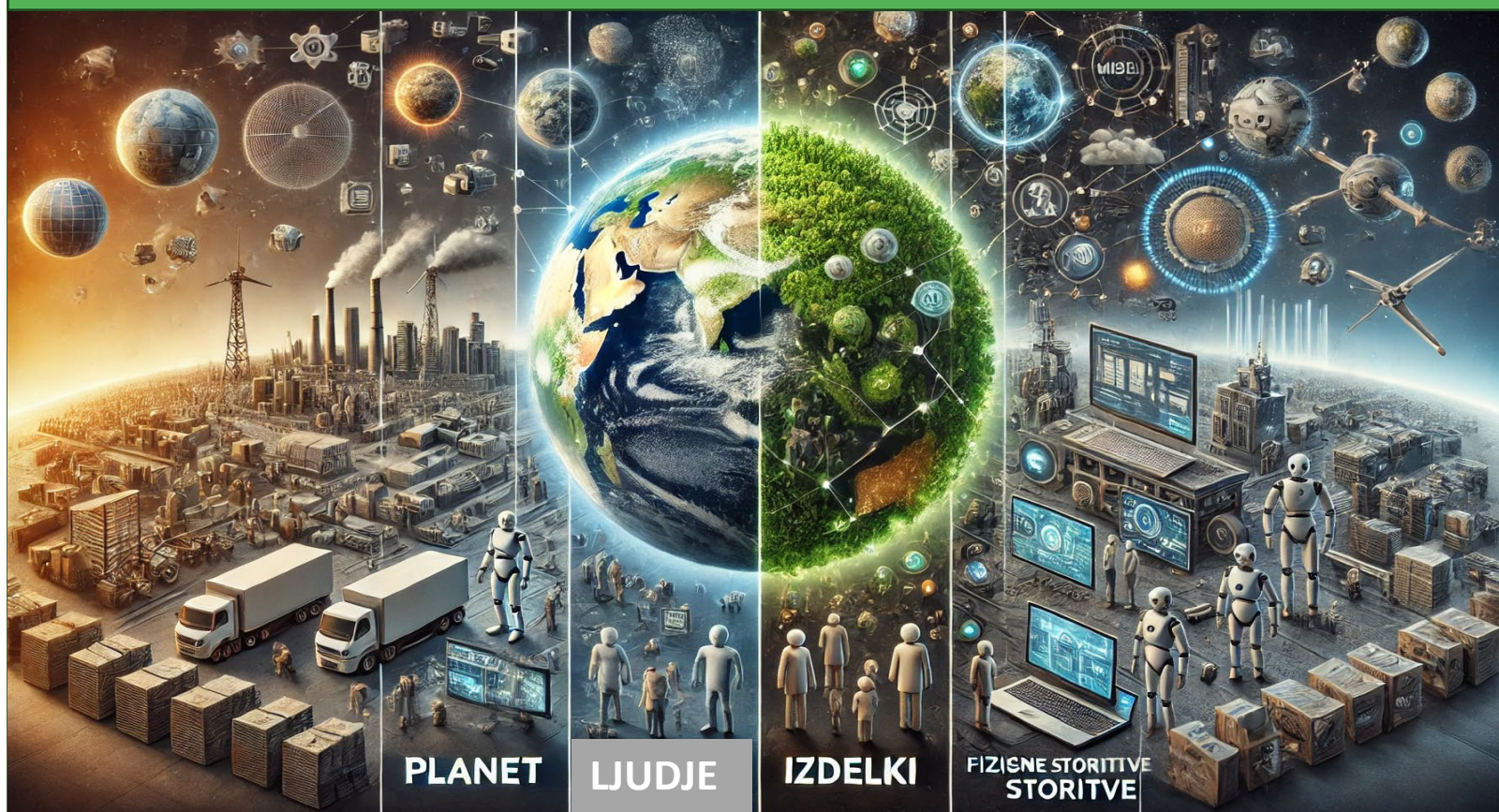
Zagotovilo, ki temelji na **zanesljivih** dokazih.



Vir: Generalni avtor (RB) z orodji UI – MS Copilot

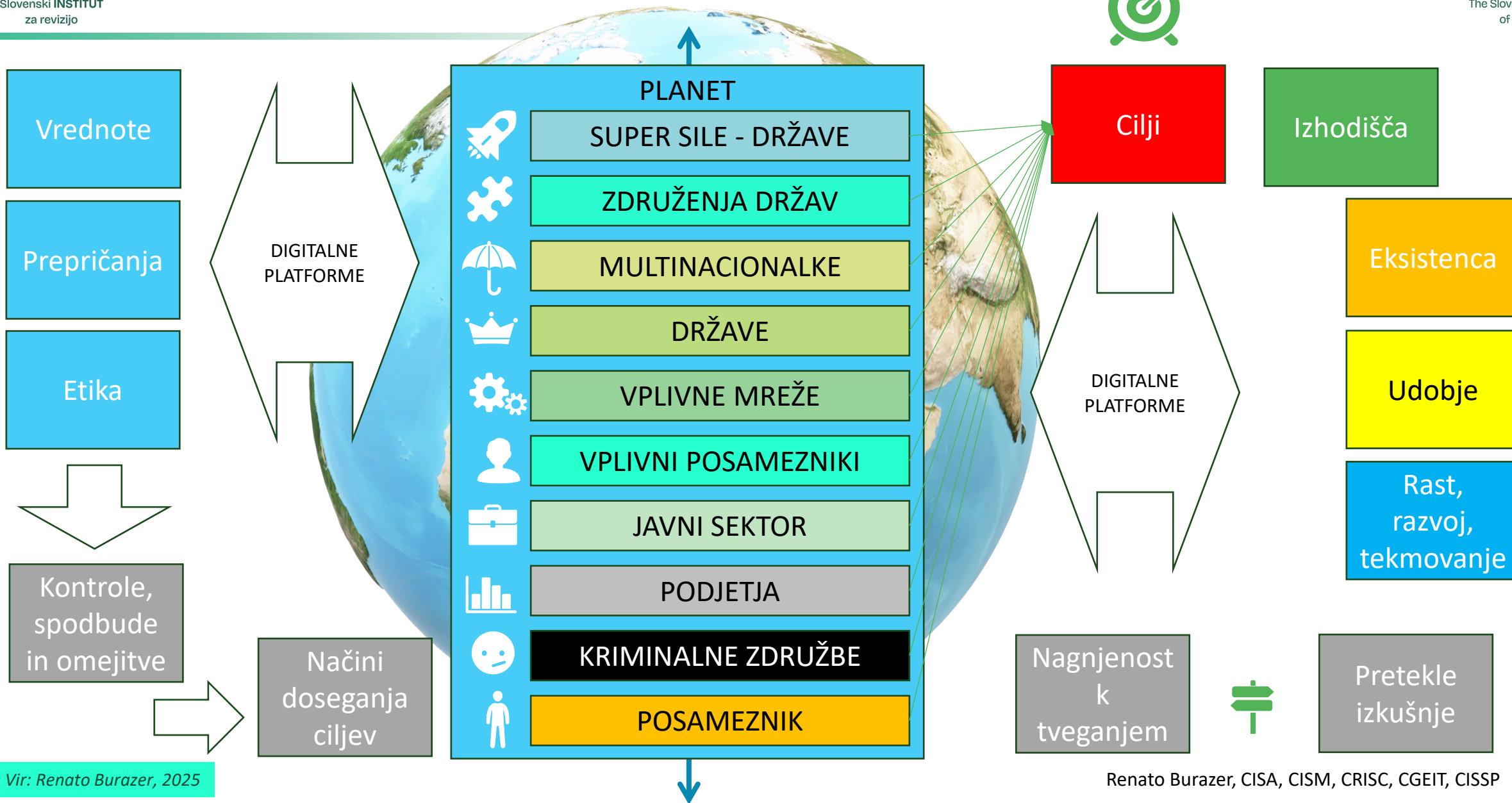
DIGITALNI SVET

FIZIČEN SVET

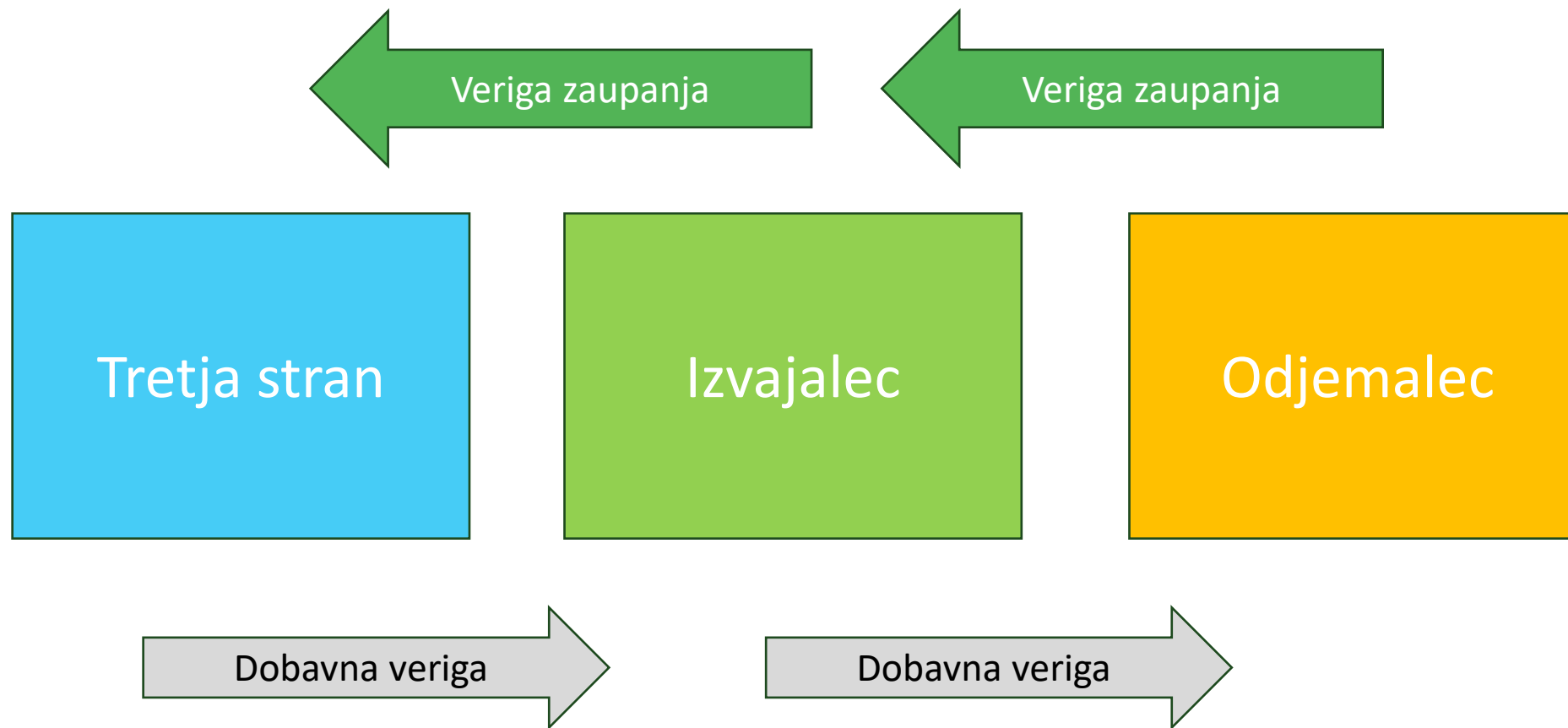


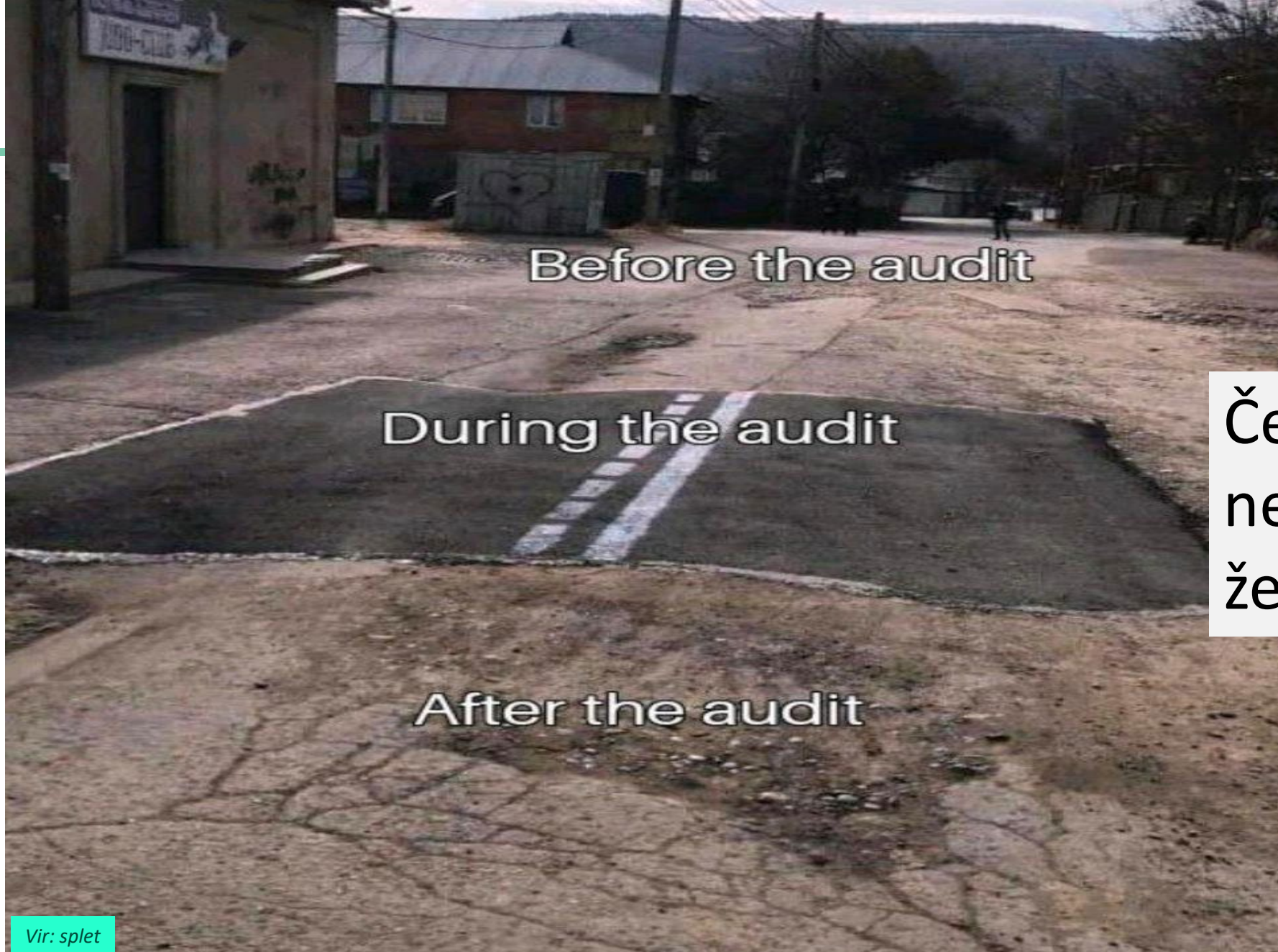
Vir: General avtor (RB) z orodji UI – MS Copilot

Model zaupanja (TM-RB)



Zaupanje iz strateške na operativno raven ...





Česa si
ne
želimo ...

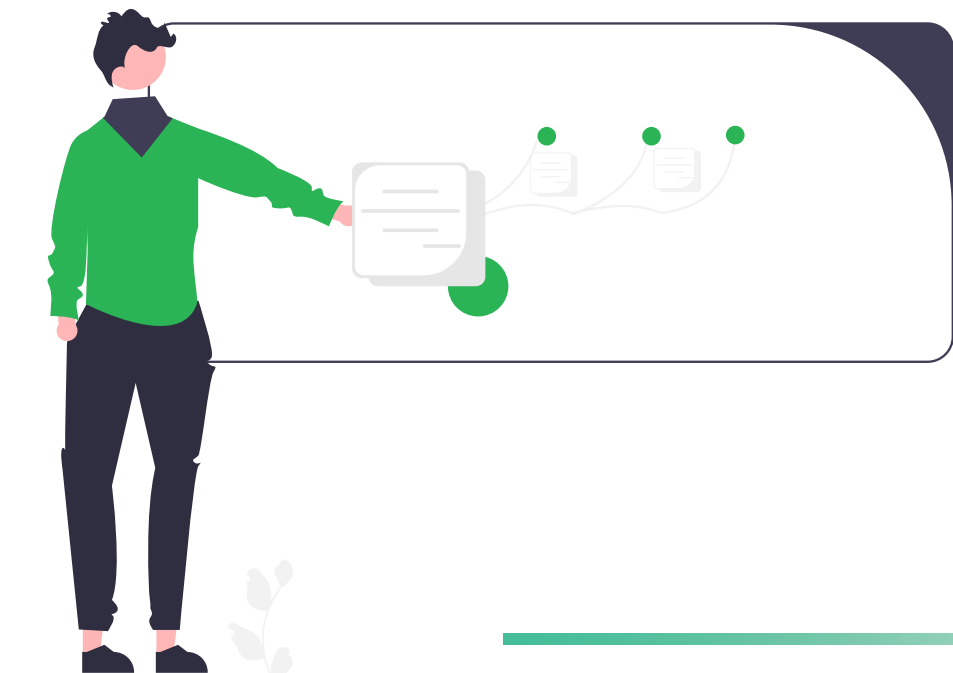
Vir: splet



Vir: splet – avtor neznan

Česa si
ne
želimo ...

Renato Burazer, CISA, CISM,
CGEIT, CRISC, CISSP

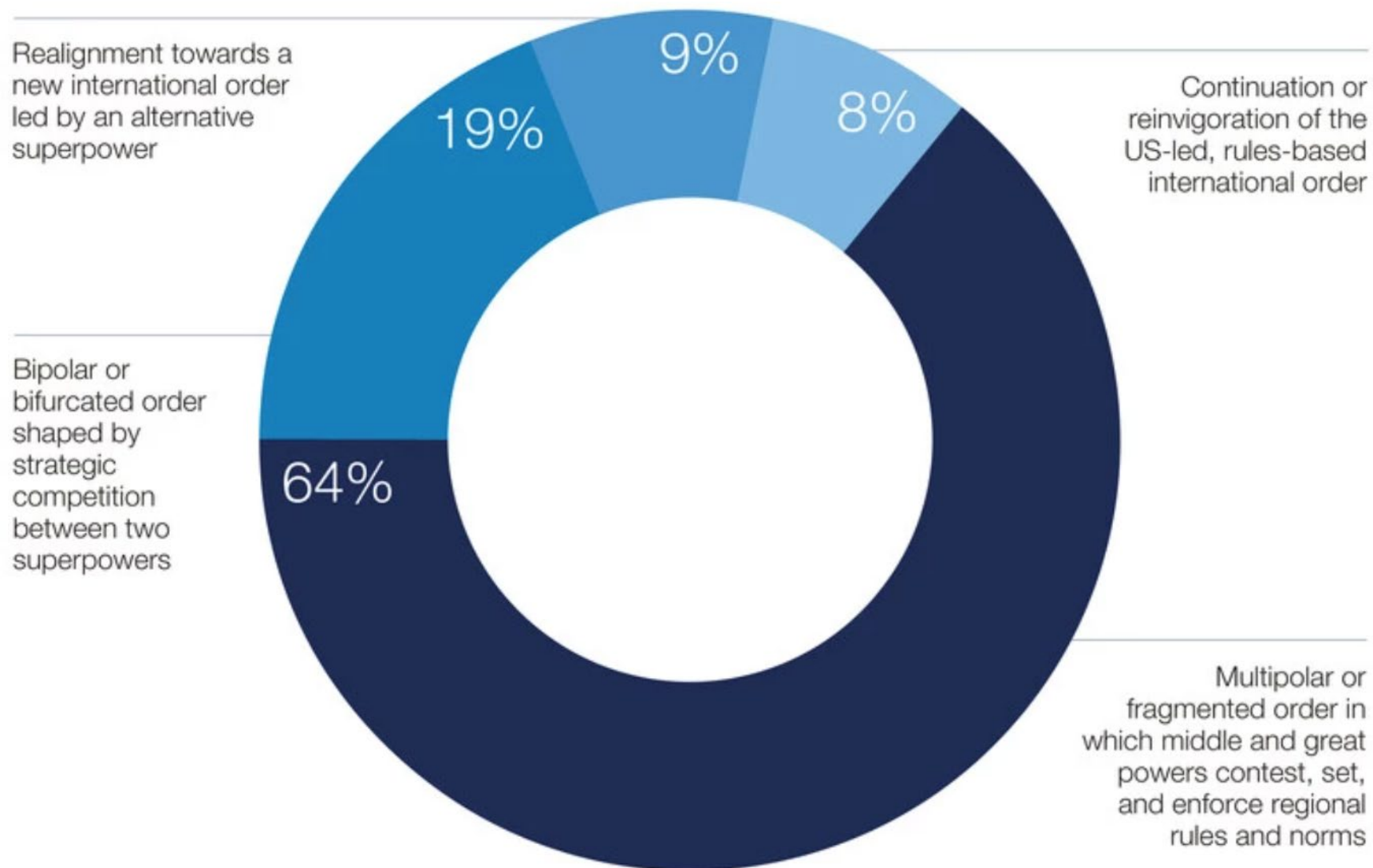


Geopolitični okvir

ZDA ↔ Kitajska ↔ EU ↔ XY

Tehnologija = strateško orožje

Kako se bodo oblikovali centri moči ?



WORLD
ECONOMIC
FORUM

An official website of the United States government [Here's how you know](#) ▼

NIST CSRC MENU

Search CSRC

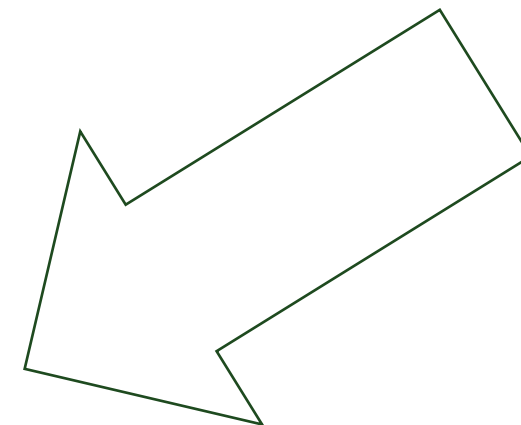
NIST COMPUTER SECURITY
RESOURCE CENTER
CSRC

October 1, 2025: Due to a lapse in federal funding, this website is not being updated. [Learn more.](#)

PROJECTS CYBERSECURITY AND PRIVACY REFERENCE TOOL

Cybersecurity and Privacy Reference Tool CPRT

f X in



- **Zaupanje** je temeljni element družbenega kapitala – bistvenega pomena za **kohezijo skupnosti**, bistvenega pomena za učinkovito sodelovanje in **ključnega pomena za gospodarski razvoj**.

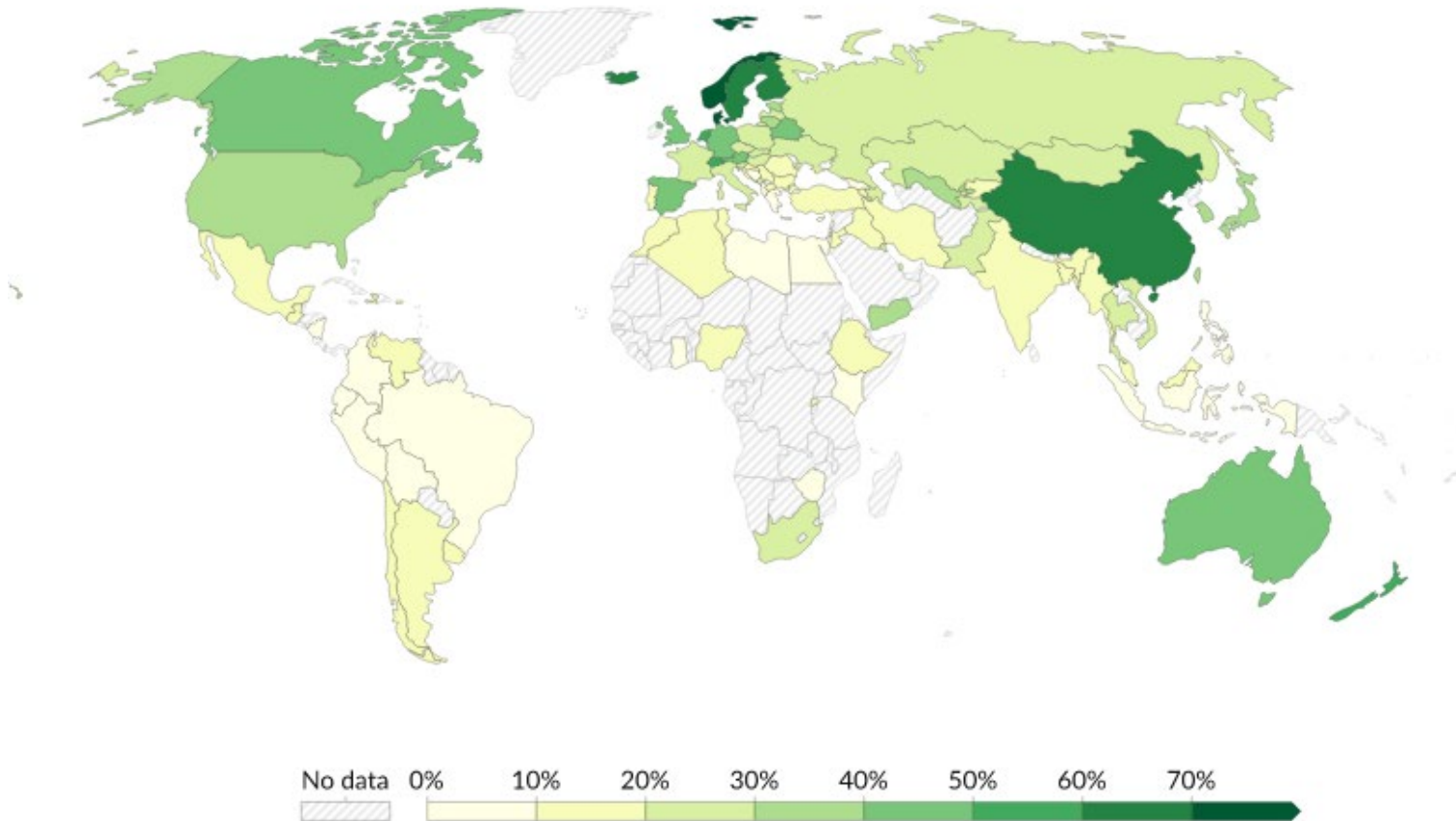
Our World
in Data

Vir: Our World in Data's mission is to publish the *"research and data to make progress against the world's largest problems."*

Raven zaupanja najvišje ocenjena v Aziji

Share of people agreeing with the statement "most people can be trusted", 2022

Our World
in Data



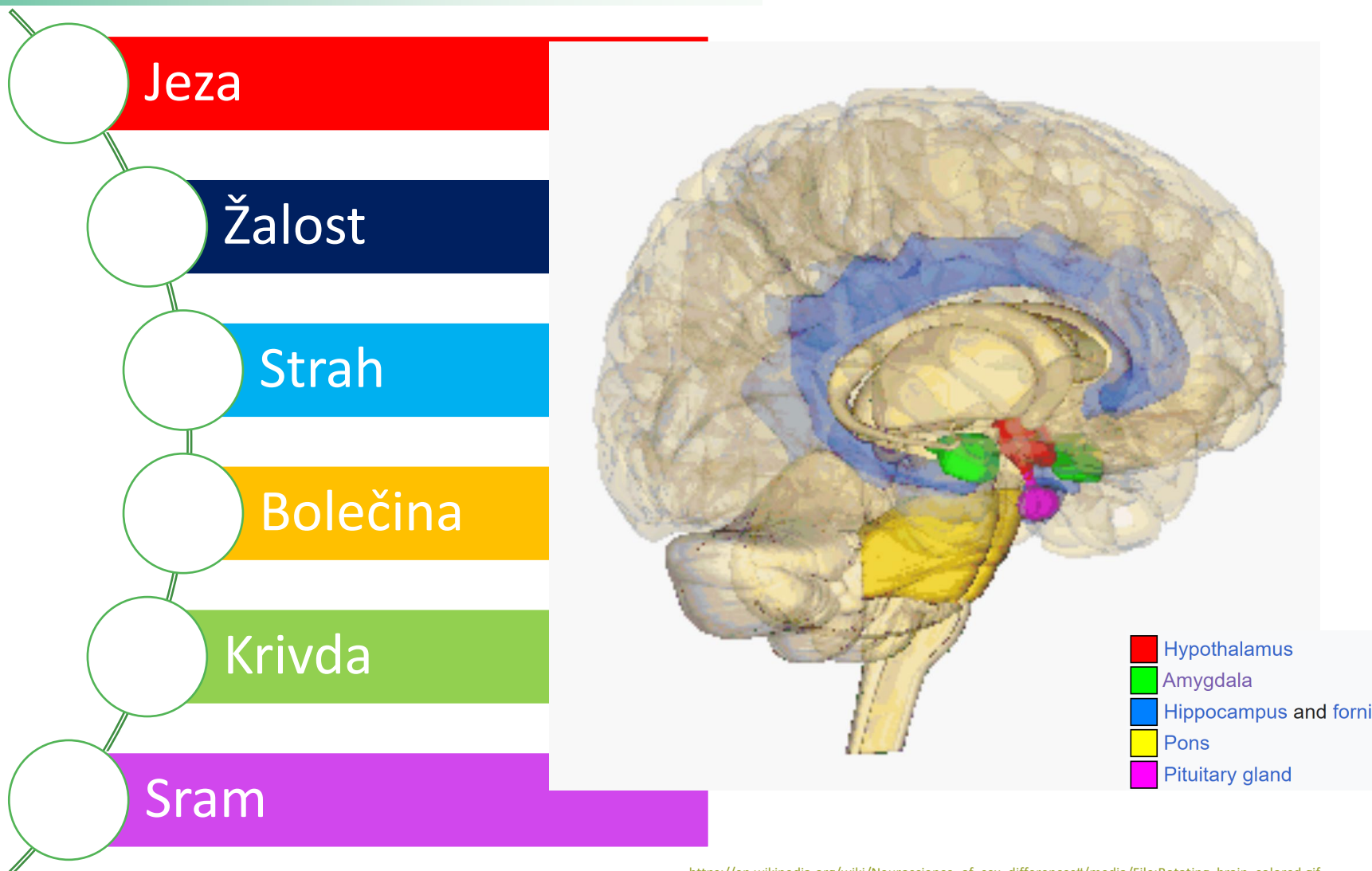
Kako se
visoka raven
zaupanja
odraža ?

Data source: Integrated Values Surveys (2024)

OurWorldinData.org/trust | CC BY

Renato Burazer, CISA, CISM, CRISC, CGEIT, CISSP

Procesiranje čustev je prioritetno = evolucija



https://en.wikipedia.org/wiki/Neuroscience_of_sex_differences#/media/File:Rotating_brain_colored.gif

“ugrabitev amigdale” (amygdala hijack)

- Povečano delovanje amigdale (zlasti ob stresu, strahu ali jezi) ima neposreden vpliv na sposobnost racionalnega razmišljanja, presoje in odločanja, ker začasno prevzame nadzor nad možgansko aktivnostjo.

Ko amigdala zazna nevarnost ali grožnjo (tudi če je ta zgolj zaznana, ne dejanska), sproži **hiperaktivno reakcijo**:

1. Pošlje **alarmni signal** v hipotalamus → sproži **stresne hormone** (adrenalin, kortizol).
2. Aktivira **boj ali beg** (*fight or flight*) odziv.
3. Sočasno **zatre delovanje prefrontalnega korteksa** – dela možganov, ki je odgovoren za:
 1. logično razmišljanje,
 2. analizo posledic,
 3. samokontrolo,
 4. načrtovanje.

AFEKTIVNO ZAUPANJE

Rezultat:

Čustva preglasijo razum.

Človek reagira impulzivno, instinktivno in pogosto **nepremišljeno**.

„ugrabitev amigdale“ = uspešen napad SOC. INŽ.

„Prodajne metode“

=

Metode socialnega
inženiringa

Uporaba
vpliva

Zastraševanje

Konformizem

Ustvarjanje
občutka
pomanjkanja

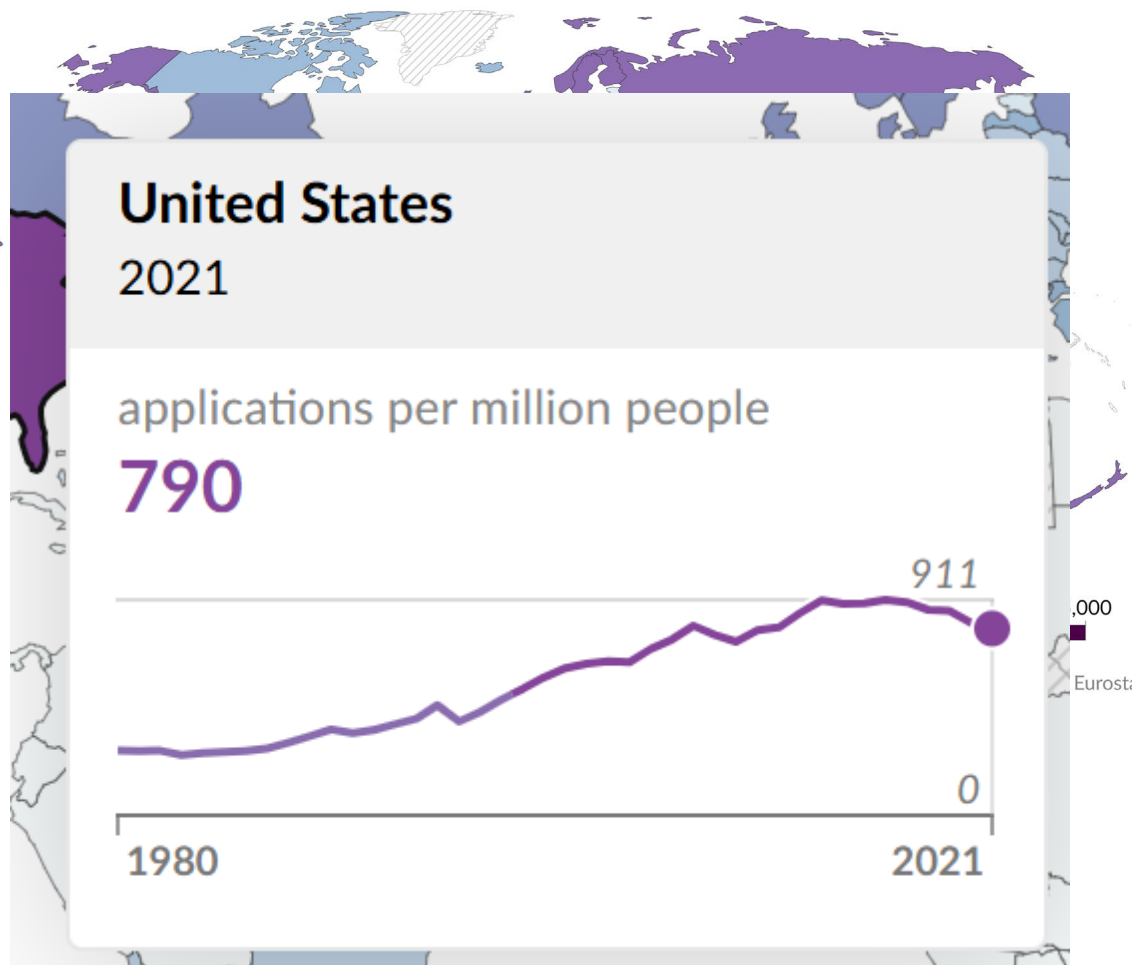
Ustvarjanje
občutka
nujnosti

Priljubljenost

= Metode geopolitičnega obvladovanja ljudi

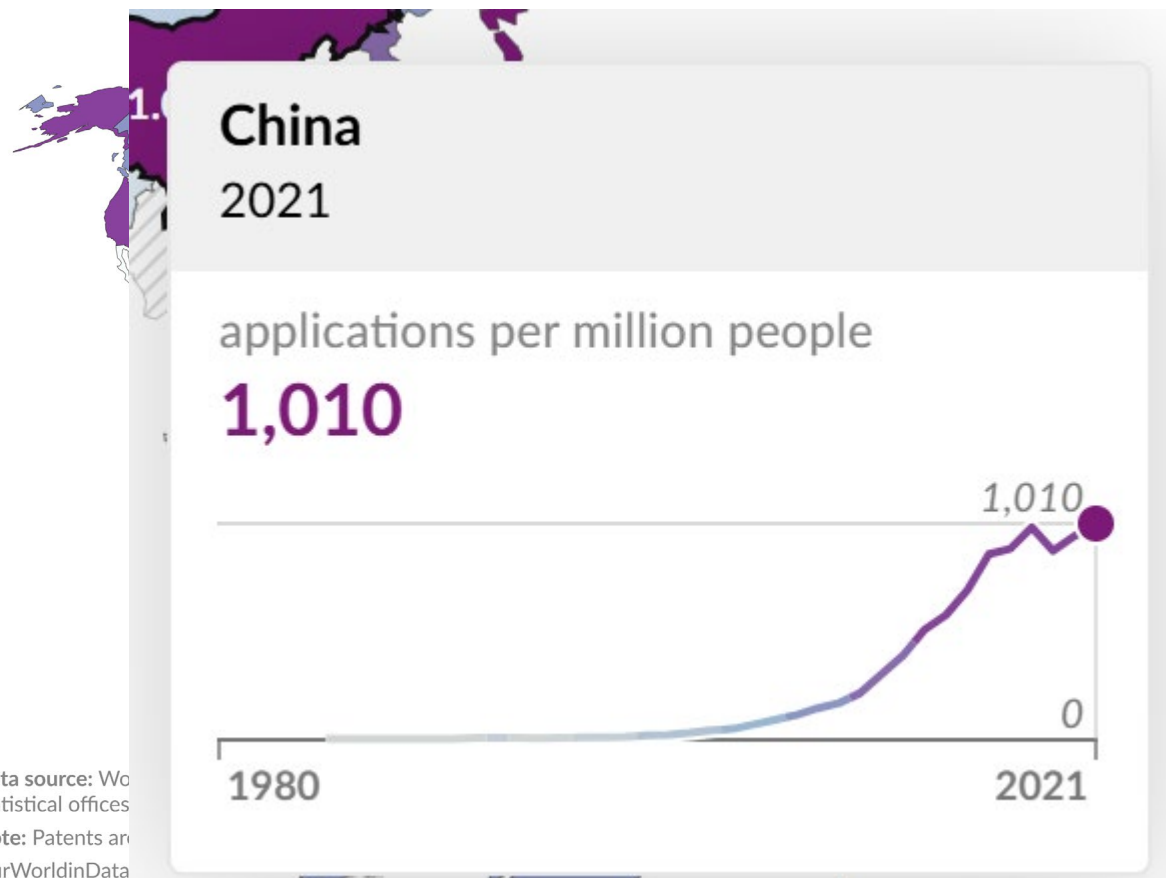
Annual patent applications per million people, 1990

Our World
in Data



Annual patent applications per million people, 2021

Our World
in Data

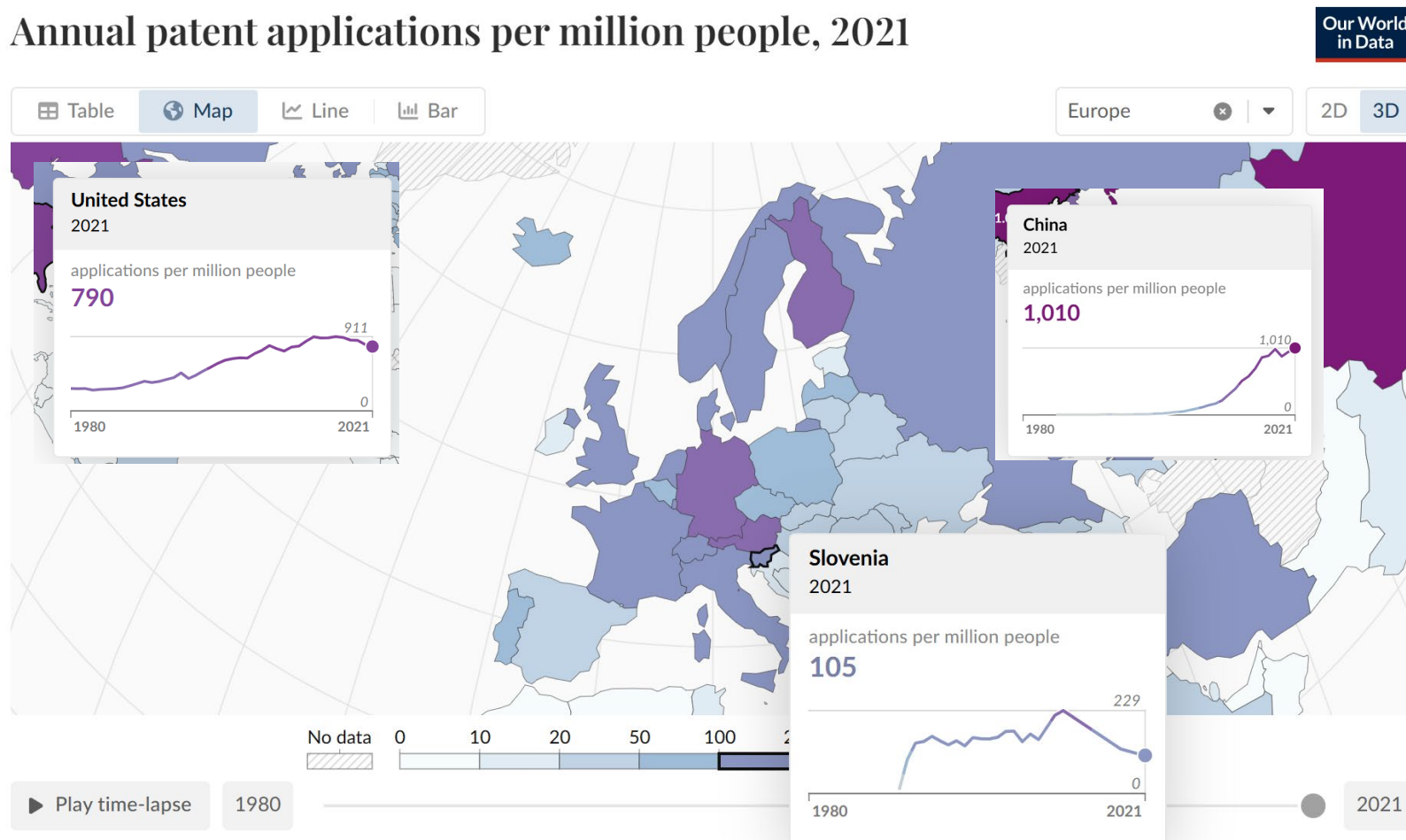


Data source: World
statistical offices
Note: Patents are
OurWorldinData

at, national

<https://ourworldindata.org/grapher/patent-applications-per-million?time=2021>

Annual patent applications per million people, 2021



Data source: World Intellectual Property Organization (WIPO), via World Bank (2025); United Nations Population Division, Eurostat, national statistical offices, and United Nations Statistics Division, via World Bank (2025) – [Learn more about this data](#)

Note: Patents are assigned based on the residence country of the first-named applicant.

OurWorldinData.org/research-and-development | CC BY

Slovenija:

Prebivalstvo: **2,097,893 (2024 ocena)**

Rast števila: **-0.1% (2024 est.)**

ZDA:

Prebivalstvo: **341,963,408 (2024 ocena)**

Rast števila: **0.67% (2024 ocena)**

Kitajska:

Prebivalstvo: **1,416,043,270 (2024 ocena)**

Rast števila: **0.23% (2024 ocena)**

- Združene države imajo "tržno usmerjen" model, ki se osredotoča na "zaščito svobode govora, prostega interneta in spodbud za inovacije".
- Kitajska ima "državni model", katerega cilj je "povečati tehnološko prevlado države ob ohranjanju družbene harmonije in nadzora".
- Medtem EU sledi „pristop, ki temelji na pravicah . . . humancentrični pristop k urejanju digitalnega gospodarstva", ki temelji na zavezah "temeljnim pravicam", kot sta zasebnost in "pojem pravičnega trga".



FEDERAL REGISTER
The Daily Journal of the United States Government



FEDERAL REGISTER
The Daily Journal of the United States Government



PD Presidential Document

Safe, Secure, and Trustworthy Artificial Intelligence

A Presidential Document by the Executive Office of the President

Removing Barriers to American Leadership in Artificial Intelligence

A Presidential Document by the Executive Office of the President on 01/31/2025



PUBLISHED DOCUMENT: 2023-24283 (88 FR 10000)



PDF

Executive Order 14110 of October 1, 2023



Document
Details

Safe, Secure, and Trustworthy Artificial Intelligence



Executive Order
Details

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered:



PDF

PUBLISHED DOCUMENT: 2025-02172 (90 FR 8741)

Executive Order 14179 of January 23, 2025



Document
Details

Removing Barriers to American Leadership in Artificial Intelligence

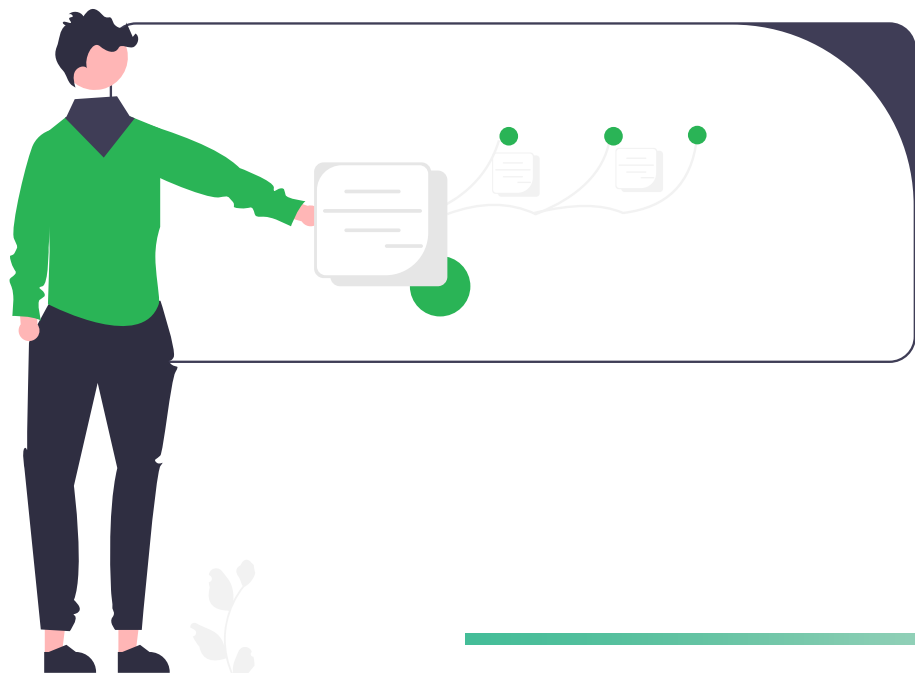


Executive Order
Details

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered:

<https://www.federalregister.gov/documents/2025/01/31/2025-02172/removing-barriers-to-american-leadership-in-artificial-intelligence>

<https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence>



Regulativa EU (2025+)

NIS2 – kibernetška varnost za ključne in bistvene subjekte

DORA – odpornost finančnega sektorja

AI Act – regulacija umetne inteligence

CRA – kibernetška odpornost izdelkov z digitalnimi elementi - Akt o kibernetški odpornosti

Globalna tveganja razvrščena po resnosti

Risk categories



Economic



Environmental



Geopolitical



Societal

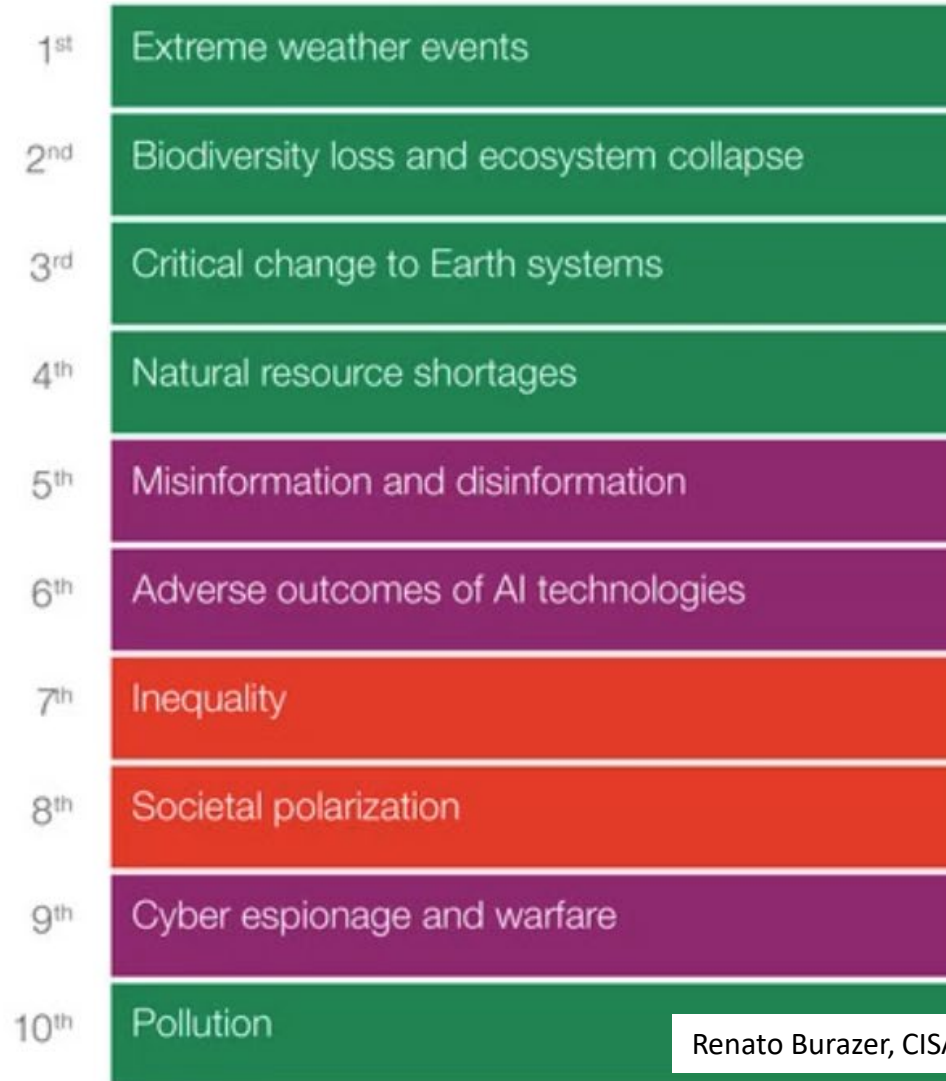


Technological

Short term (2 years)



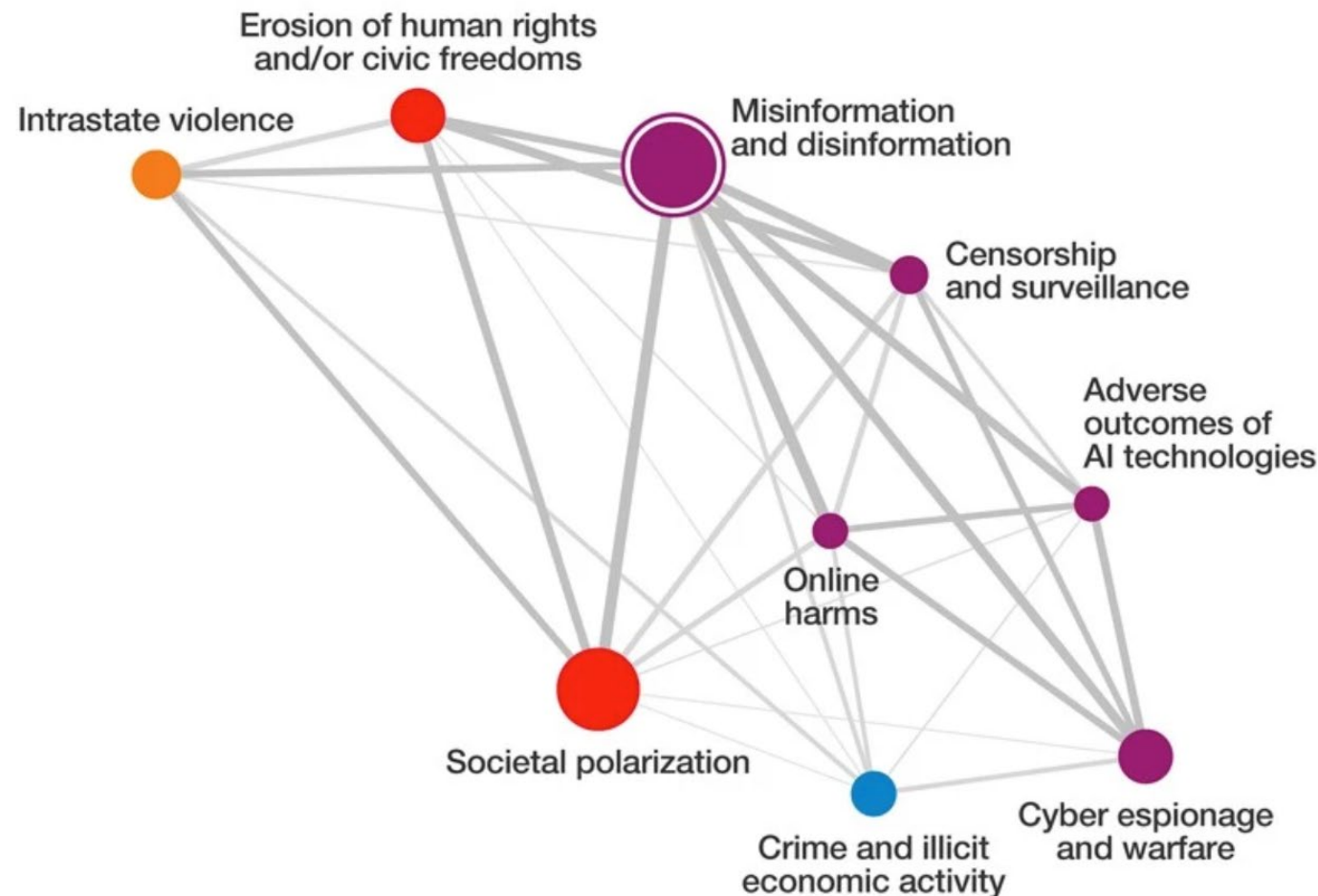
Long term (10 years)



Vir: Global Risks
Report 2025

Medsebojne povezave tveganja: napačne informacije in dezinformacije

Vir: Global Risks Report 2025



Relative influence, Edges — High — Medium — Low

Risk influence, Nodes ○ High ○ Medium ○ Low

Risk categories ● Economic ● Environmental ● Geopolitical ● Societal ● Technological

Digitalni prostori = bojišča za geopolitični vpliv

- TikTok se je iz aplikacije za družabne medije razvil v - v očeh nekaterih oblikovalcev politik v digitalno orožje. Zaradi množičnega globalnega sledenja je postal kulturni „superjunak“.
- Zaradi izjemnega uspeha je postal tudi glavna tarča v stopnjevanju tehnološke vojne med ZDA in Kitajsko.
- Njegov algoritem ni podoben algoritmom drugih družbenih platform, ki se zanašajo na uporabnikov socialni graf (kaj sledite, koga poznate) za povezovanje ljudi, organizacij in krajev.
- Namesto tega TikTok uporablja sistem priporočil v realnem času, ki temelji na mikrointerakcijah: kako dolgo gledate videoposnetek, ali ga začasno zaustavite ali znova predvajate, in celo vzorce pomikov in dotikov zaslona. Rezultat je tok vsebine, ki izjemno zasvoji.
- To daje TikToku skoraj neprimerljivo moč oblikovanja mnenj, bodisi namerno ali ne.



AI-Driven Disinformation Bots Target Czech Elections on TikTok

📅 2025-10-03 📖 [7 articles](#) 📍 Czechia

During the Czech parliamentary elections, hundreds of AI-driven bot accounts on TikTok spread disinformation and extremist propaganda, reaching millions of users. TikTok removed dozens of these accounts following urgent intervention by the European Commission, but experts warn the **AI-enabled campaign already impacted the electoral process.** [AI GENERATED]

AI principles:

Accountability Fairness Transparency & explainability Democracy & human autonomy Robustness & digital security Respect of human rights

Industries:

Media, social platforms, and marketing Government, security, and defence

Affected stakeholders:

General public Government

Harm types:

Public interest

Severity:

AI Incident

► Why's our monitor labelling this an incident or hazard?



According to the Special Eurobarometer survey, most Europeans support greater digitalisation, yet are concerned about the risks posed to information integrity:



More than 90% of respondents consider **protecting children online** to be an urgent concern.



85% of respondents think that **public authorities should support EU companies** in growing to compete globally.



89% of Europeans believe in the importance of **increasing research and innovation** for stronger and more secure digital technologies.



75% of Europeans consider that the **digitalisation of daily services** makes their lives easier.



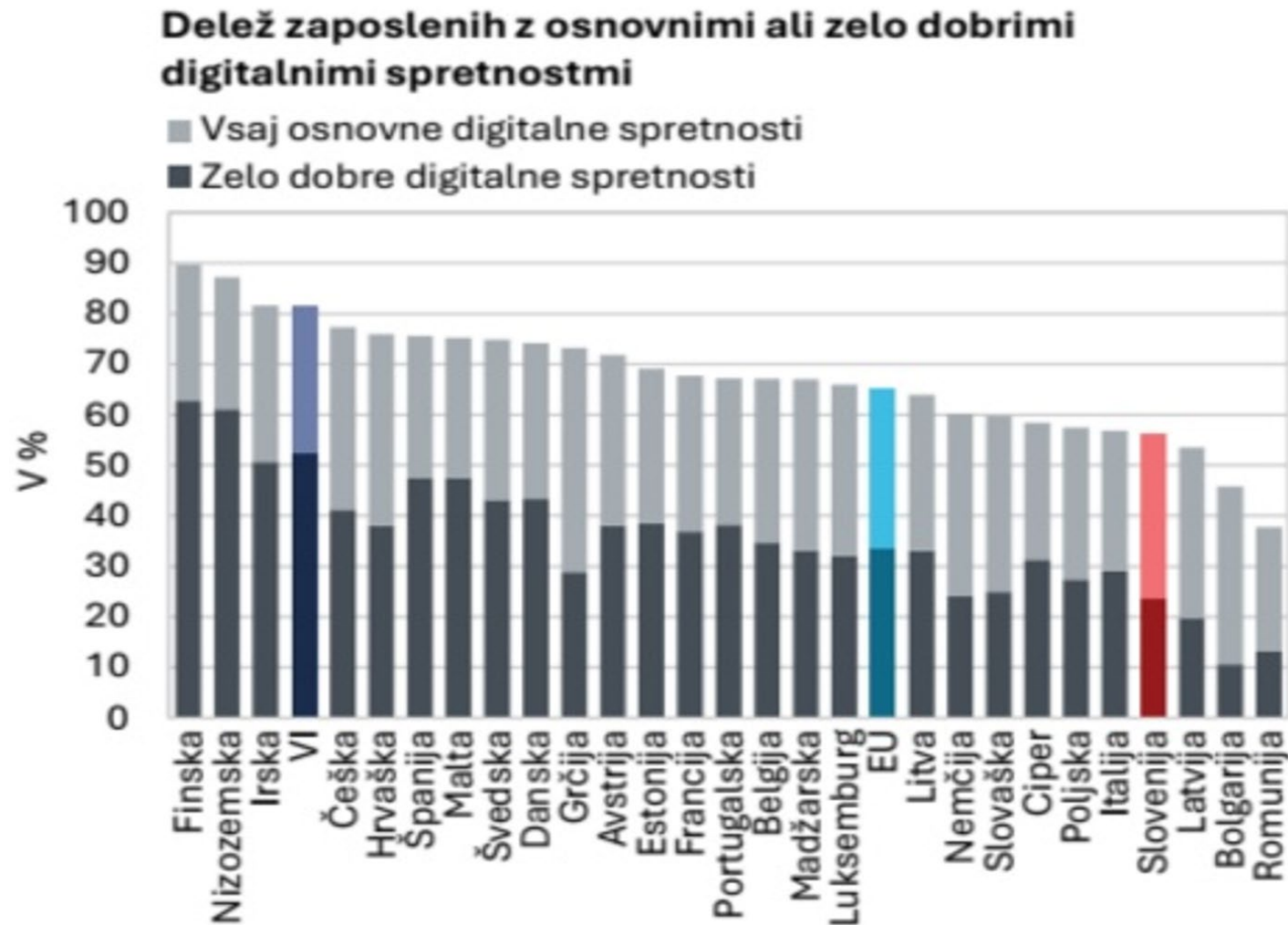
Urad Republike Slovenije
za makroekonomske
analize in razvoj
Gregorčičeva 27
1000 Ljubljana

Kakovost življenja v Sloveniji

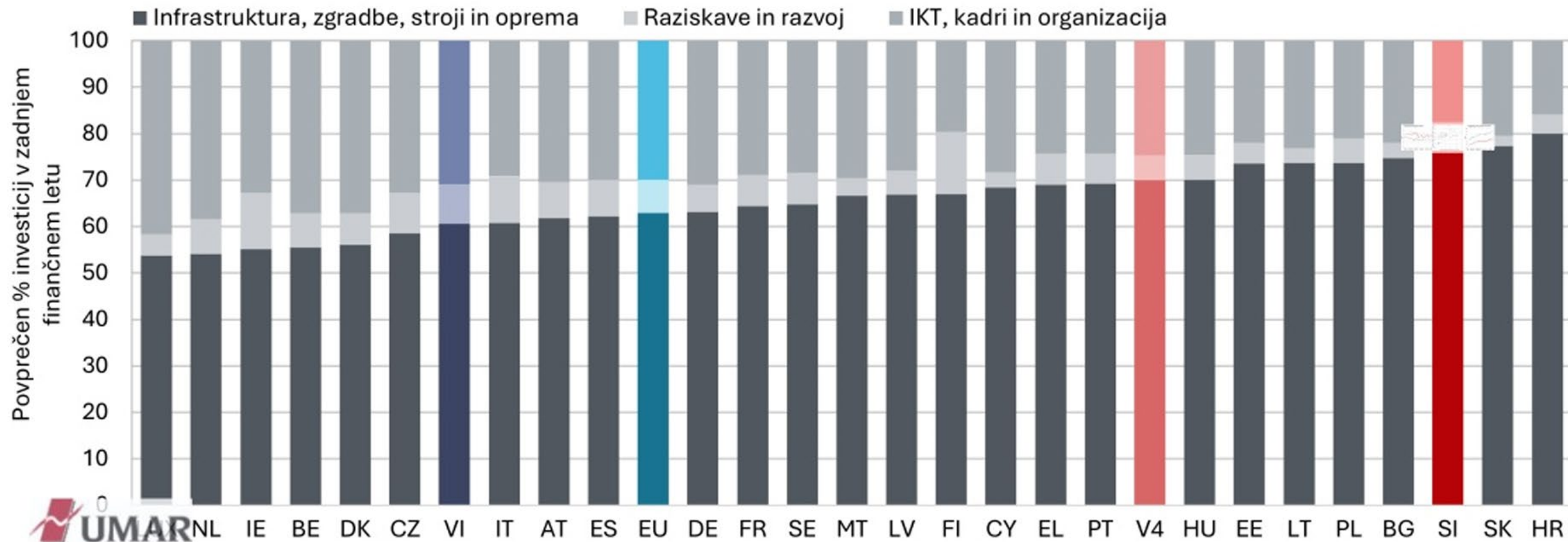
Poročilo o razvoju 2025



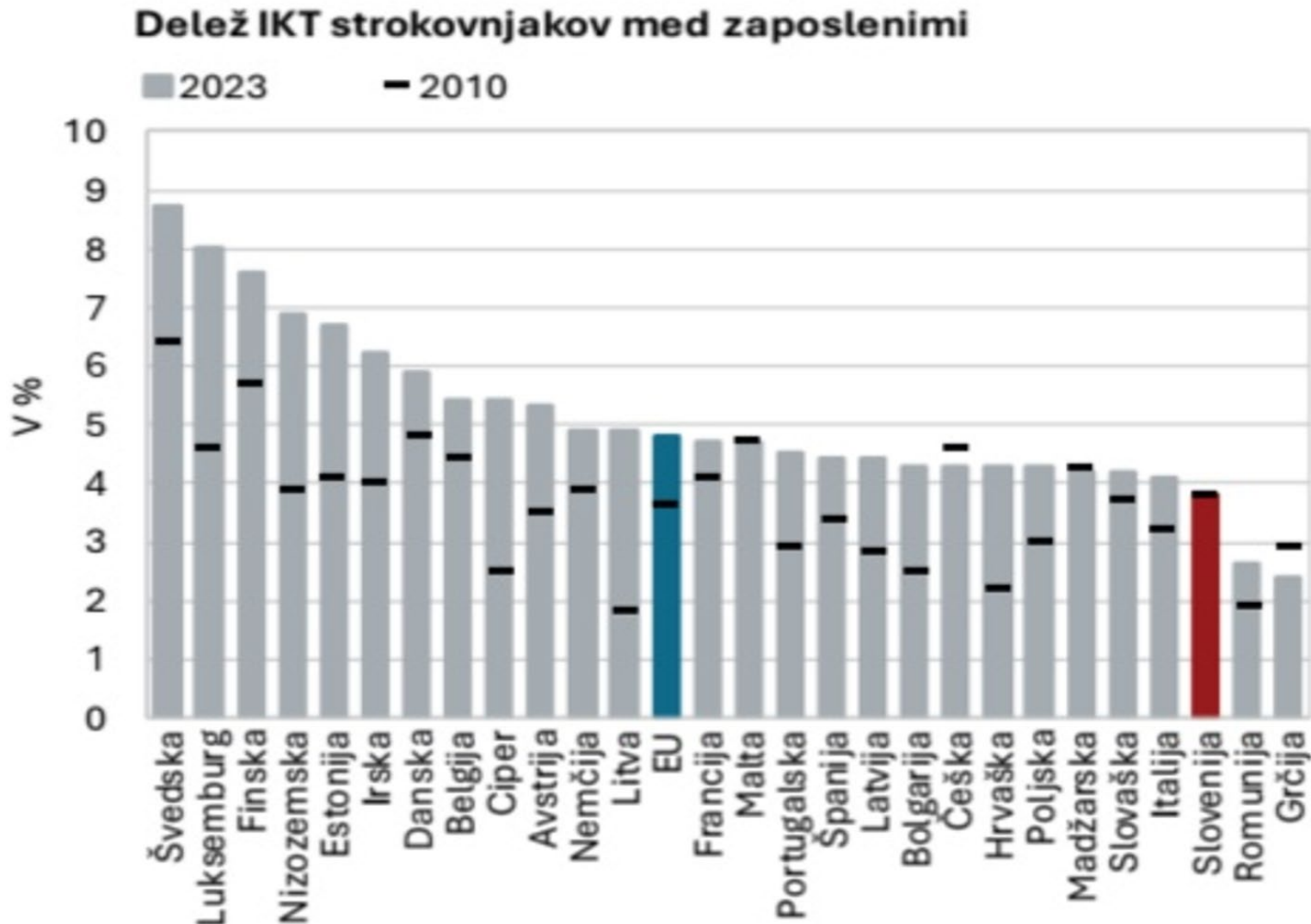
www.umar.gov.si



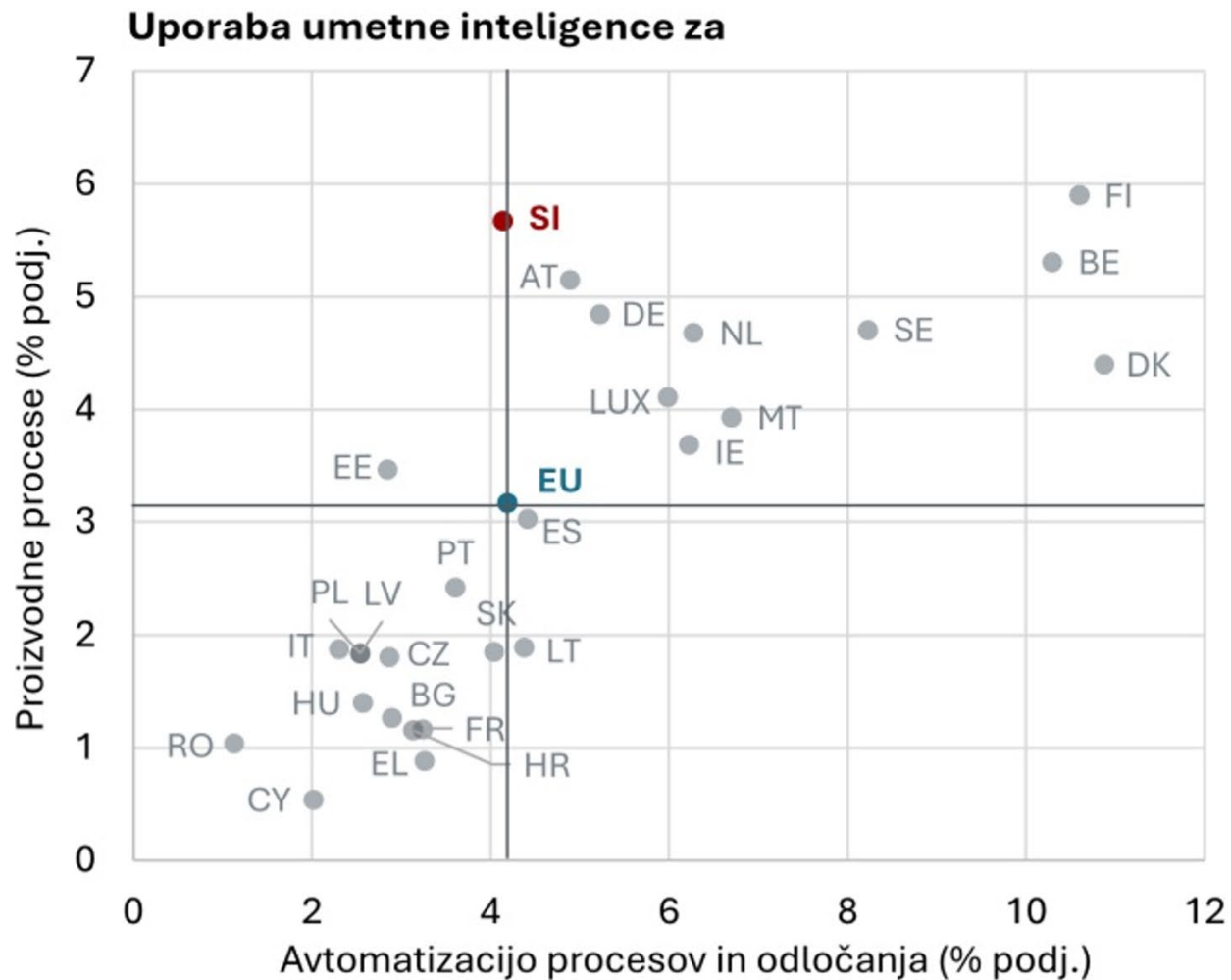
Struktura podjetniških investicij po namenih



Slovenija ima (leto 2023) podpovprečen delež IKT strokovnjakov med zaposlenimi ...

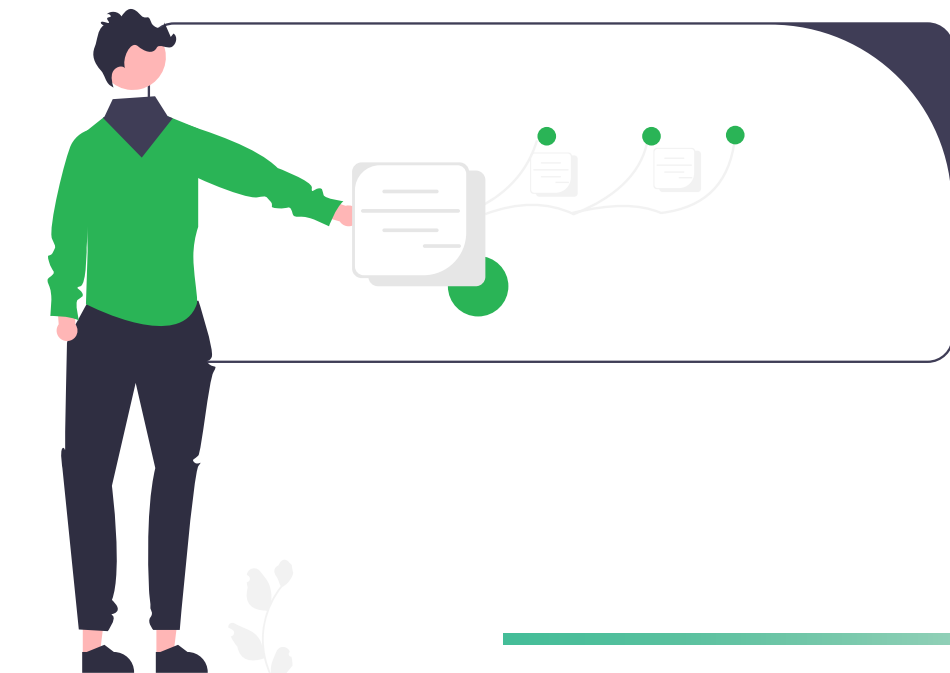


Vir: UMAR,
https://www.umar.gov.si/fileadmin/user_upload/sporocila_za_javnost/2025/Sporocila_za_javnost/Konferenca_POR25/Predstavitev_POR25.pdf



Digitalizacija MSP-jev je resen izziv: delež podjetij, ki meni, da digitalna preobrazba za njih ni bistvena oz. relevantna za uspešno poslovanje, se povečuje:

- med majhnimi podjetji je bilo leta 2024 takšnih 53 % (oz. 4 o. t. več kot leta 2021),
- med srednje velikimi 51 % in kar 18 o. t. več kot leta 2021,
- med velikimi pa četrtna (oz. 6 o. t. več kot 2021).



Novi izzivi za revizorje IS

Hibridne arhitekture

Kibernetska odpornost

Revizija umetne inteligence

FIZIČEN SVET (oprijemljivi)

PLANET

En sam – edini,
ki ga imamo

Vedno bolj
izčrpan

Ponekod
pozitivni trendi

Ali res? Dvom v
resnico.

LJUDJE

Vedno več

Prisotne razlike

„Ustvarjanje“
resnic

Nezaupanje

IZDELKI

Vedno več

Bolj kompleksni

Vgrajena
„senzorika“

Vgrajena
inteligenca

FIZIČNE STORITVE

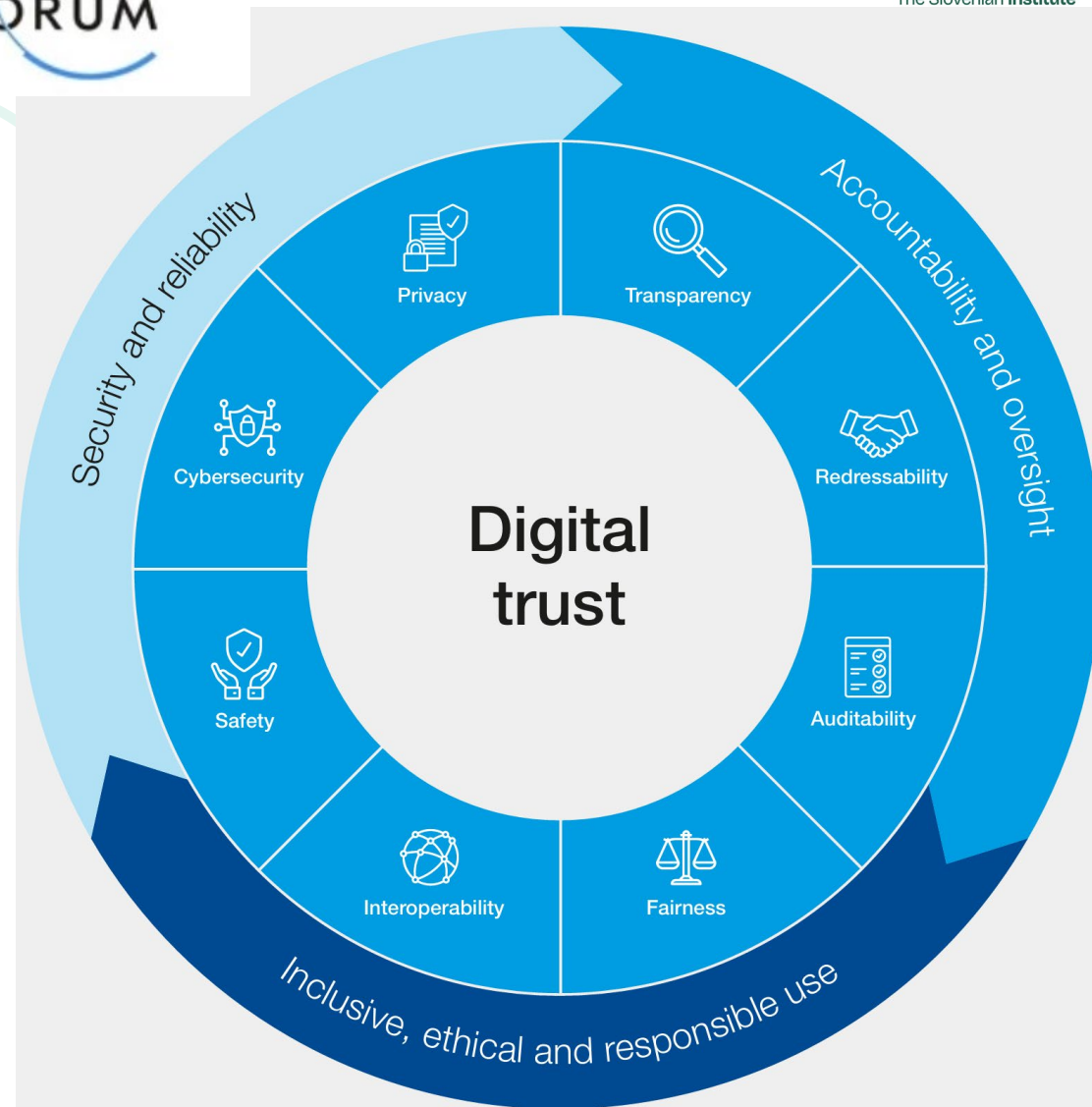
Prehajanje
fizičnih del na
robote

Fizičen svet temelji na digitalnih tehnologijah

Fizičen svet potrebuje **DIGITALNO ZAUPANJE**

Poročilo Svetovnega gospodarskega foruma za leto 2022 Earning Digital Trust je digitalno zaupanje opredelilo kot obljubo,

"da bodo digitalne tehnologije in storitve – ter organizacije, ki jih zagotavljajo – zaščitile interese vseh deležnikov ter podprle družbena pričakovanja in vrednote".



- Vodilni v tehnološkem razvoju si pridobijo zaupanje, ko si zastavijo ambiciozne cilje za varnost in zanesljivost, da zagotovijo odgovornost in nadzor nad svojimi stvaritvami ter za spodbujanje vključenosti, etike in odgovornosti. Svojo predanost tem zaupanja vrednim ciljem **dokazujejo z jasnimi in merljivimi ukrepi v zvezi z razsežnostmi digitalnega zaupanja:**

Kibernetska varnost

Varnost

Interoperabilnost

Zasebnost

Preglednost

Popravlljivost

Etika

Pravičnosti



Okvir ekosistema za Digitalno zaupanje

Overview for ISACA Chapters and Members

Renato Burazer, CISA, CISM, CRISC, CGEIT, CISSP

8.10.2025

Digitalno zaupanje

zaupanje v integriteto odnosov, interakcij in transakcij med ponudniki in potrošniki v digitalnem ekosistemu.

To vključuje sposobnost ljudi, organizacij, procesov, informacij in tehnologije, da **ustvarijo in vzdržujejo zaupanja vreden digitalni svet.**



Poslovne prednosti digitalnega zaupanja

Digitalna Evolucija

Naslednji napredek v **digitalni preobrazbi**

Poganjajo ga poslovne potrebe, ki podjetjem omogočajo, da **ostanejo konkurenčna in izpolnjujejo pričakovanja strank**

Zakaj bi se morala podjetja osredotočiti na digitalno zaupanje?

Digitalno zaupanje je pomemben dejavnik, ki **spodbuja odločitve potrošnikov**

Pomaga **izboljšati ugled podjetij**

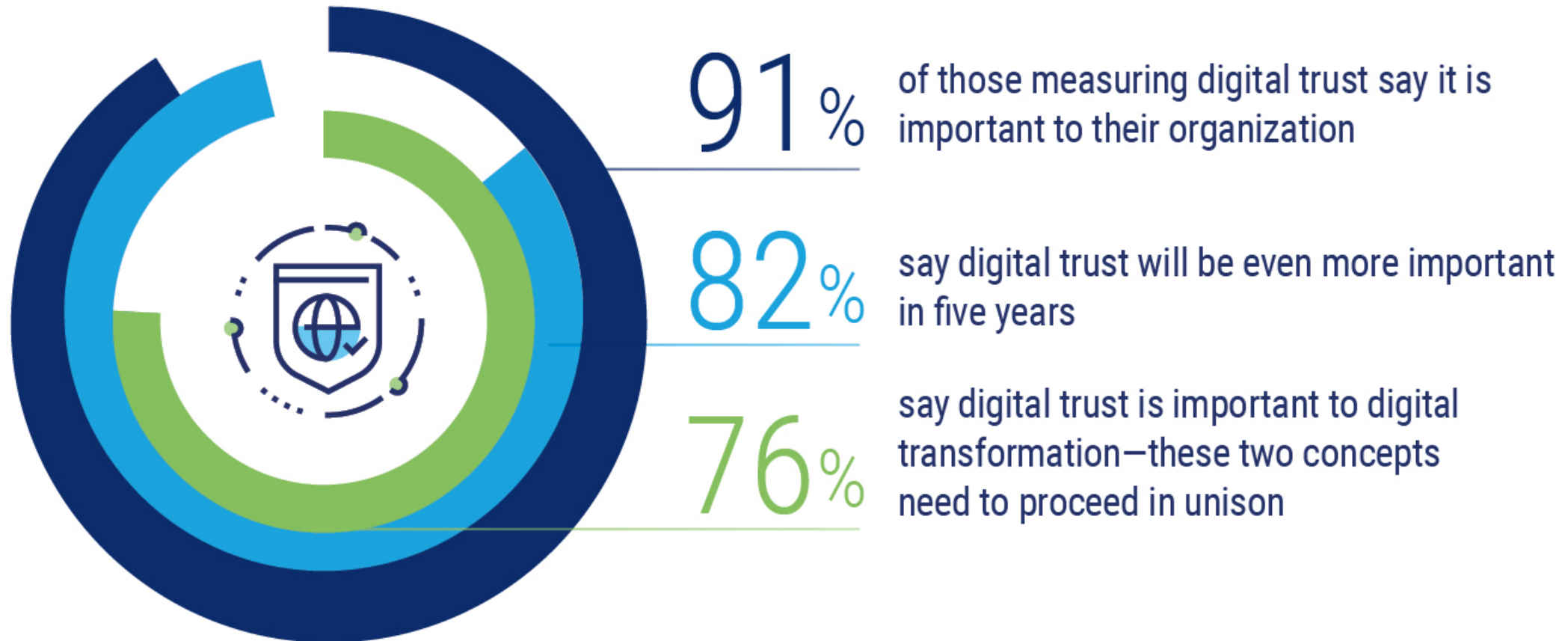
Spodbuja zvestobo strank

Digitalno zaupanje se začne na vrhu

Digitalno zaupanje **mora biti vgrajeno v organizacijo**, da so zaposleni dobri etični skrbniki informacij, izdelkov in storitev.



Digital Trust Is Essential to Digital Transformation



Digitalen zaupanja vreden ekosistem



Kakovost



Varnost in zasebnost



Zanesljivost



Etika in integriteta



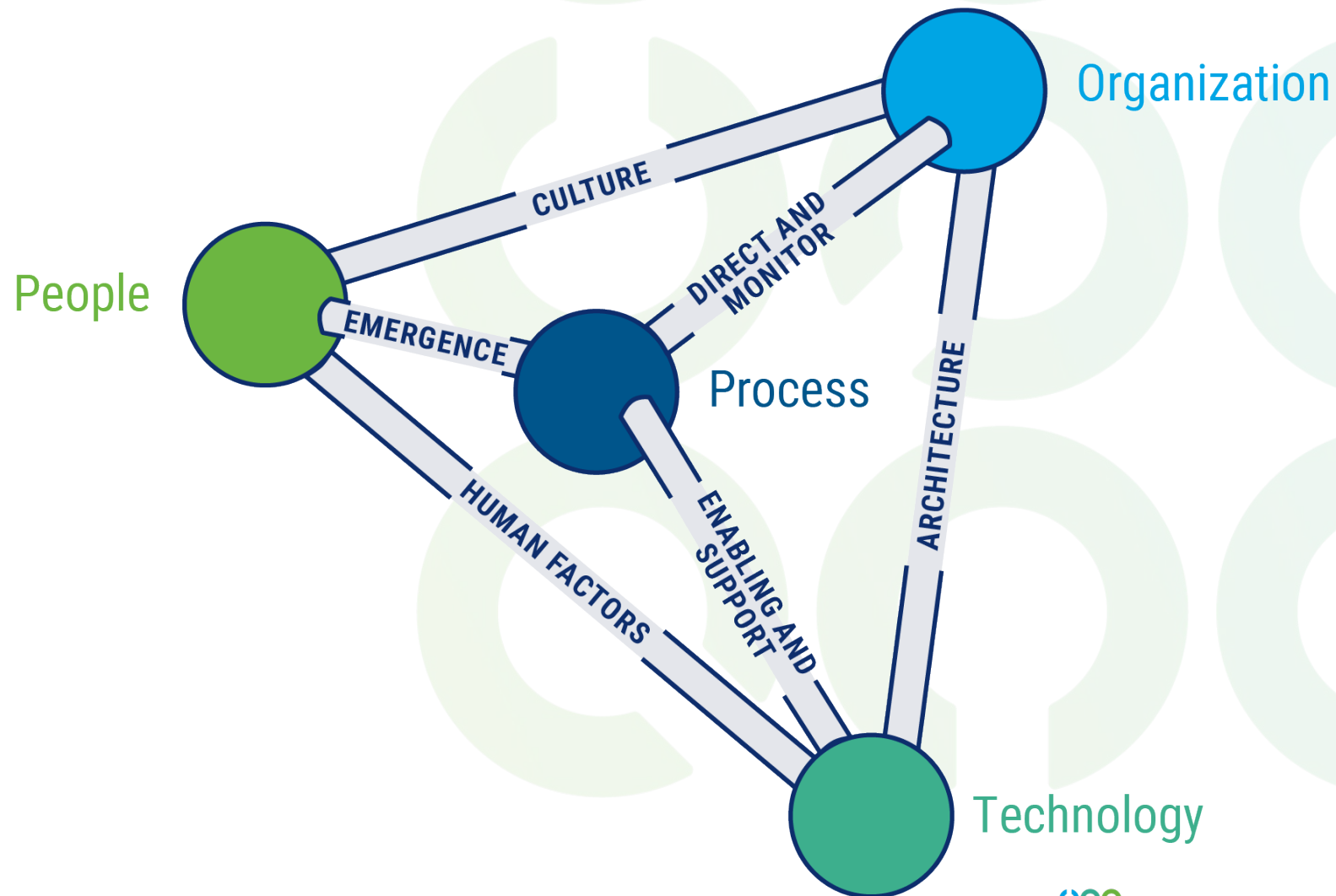
**Preglednost
in poštenost**



Samozavest

ISACA's Digital Trust Ecosystem Framework (DTEF)

DTEF je bil zasnovan tako, da deluje v povezavi z obstoječimi okviri, da bi se izognili preobremenitvi okvirov.



DTEF Vozlišča

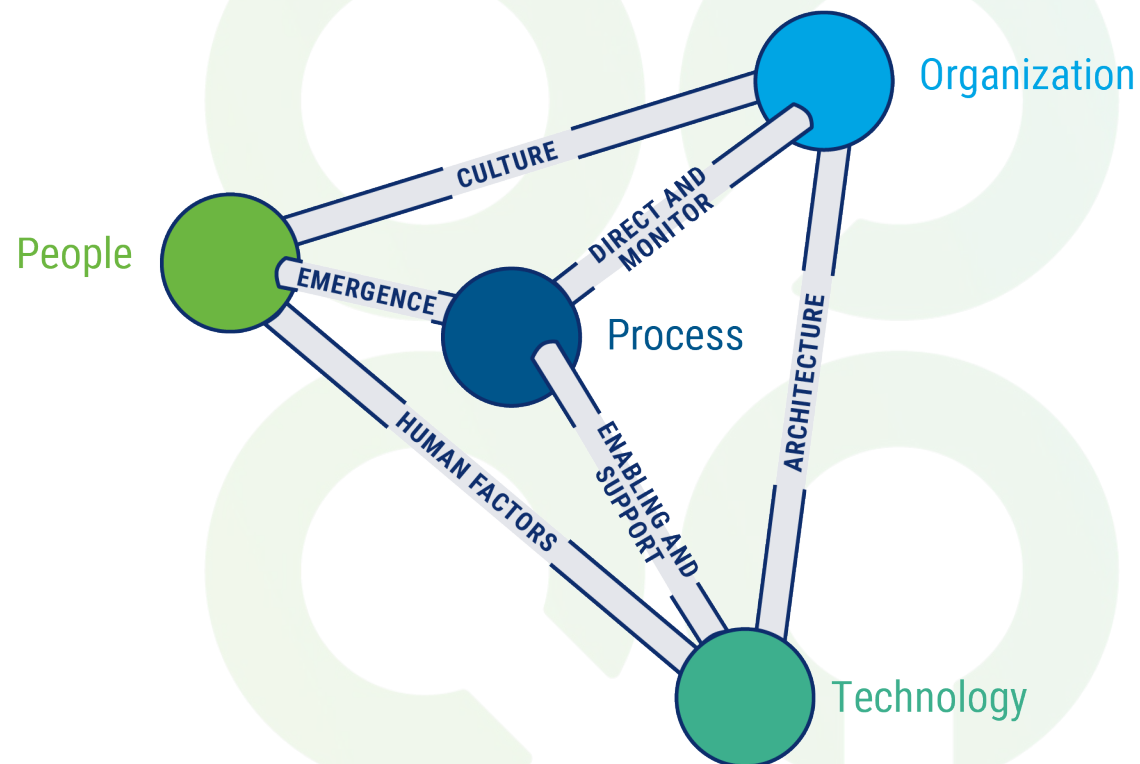
Vozlišča so primarni elementi DTEF:

Ljudje

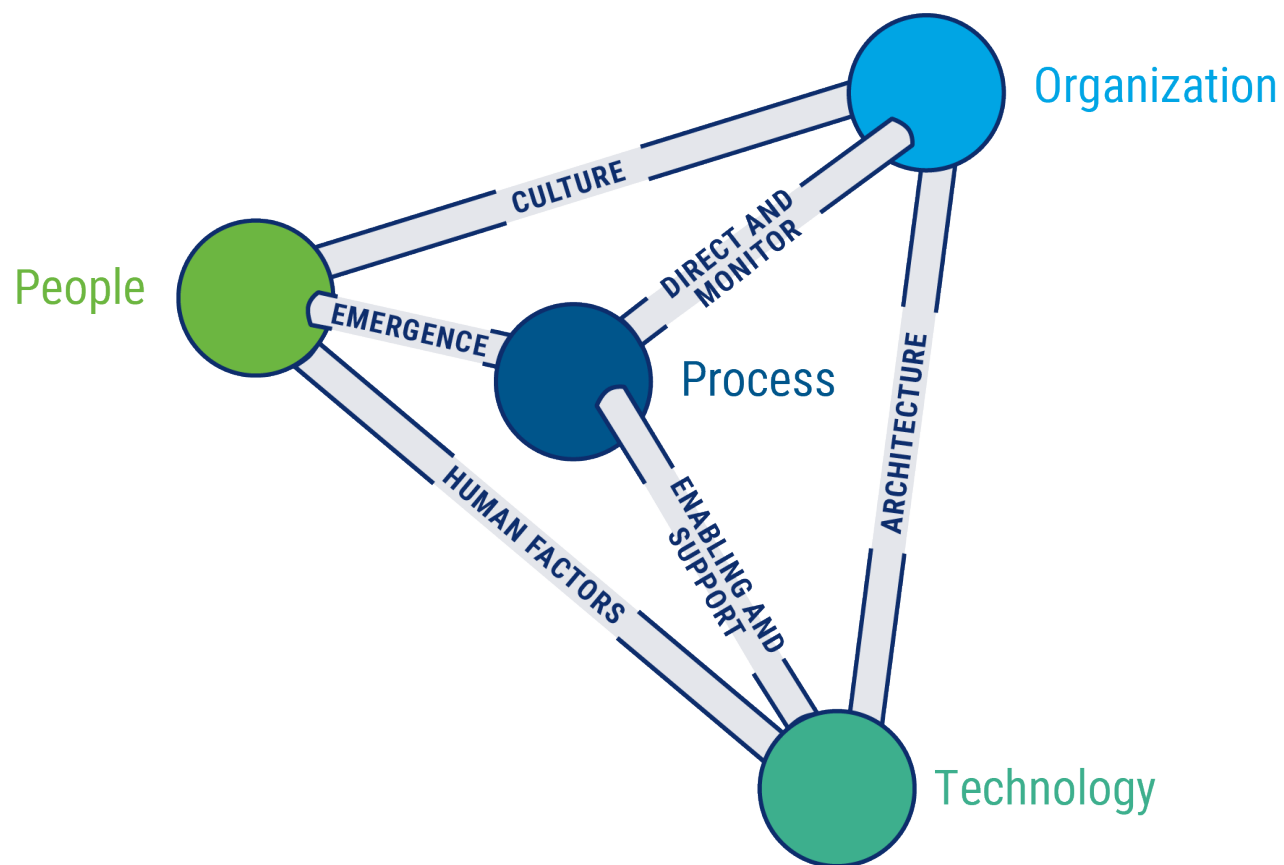
Proces

Tehnologija

Organizacija



DTEF Domene



Domene so prilagodljive in odražajo primarne vplive ali napetosti med vozlišči.

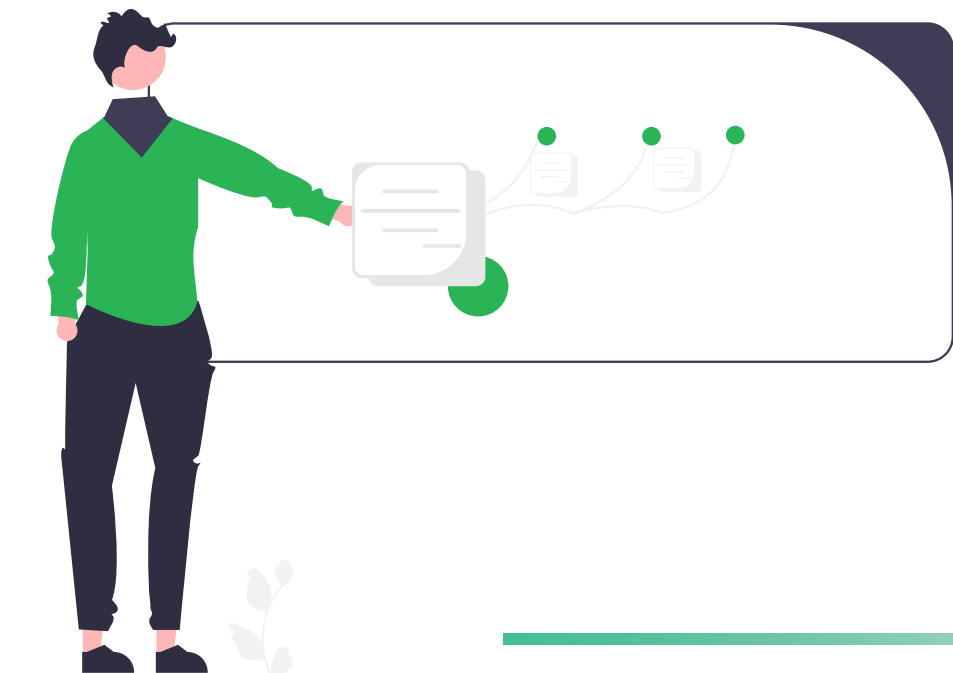
Obstaja šest domen:

- Kultura
- Človeški dejavniki
- Pojav
- Omogočanje in Podpora
- Usmerjaj in spremljaj
- Arhitektura

Hierahija DTEF







Revizor IS 2.0

Kompetence: tehnologija + regulativa + geopolitika + etika

Nova orodja: AI, podatkovna analitika, avtomatizacija

Vloga: od »checkerja« do strateškega svetovalca

MIT:

UI ne more
kontrolirati
ljudi



DEJSTVO:

Inteligenca
omogoča
kontrolno: mi
kontroliramo
tigre ker smo
pametnejši



<https://futureoflife.org/background/aimyths/>

Kaj so dejavniki za vrednotenje kandidatov za zaposlitev za strokovnjake s področja kibernetске varnosti ?

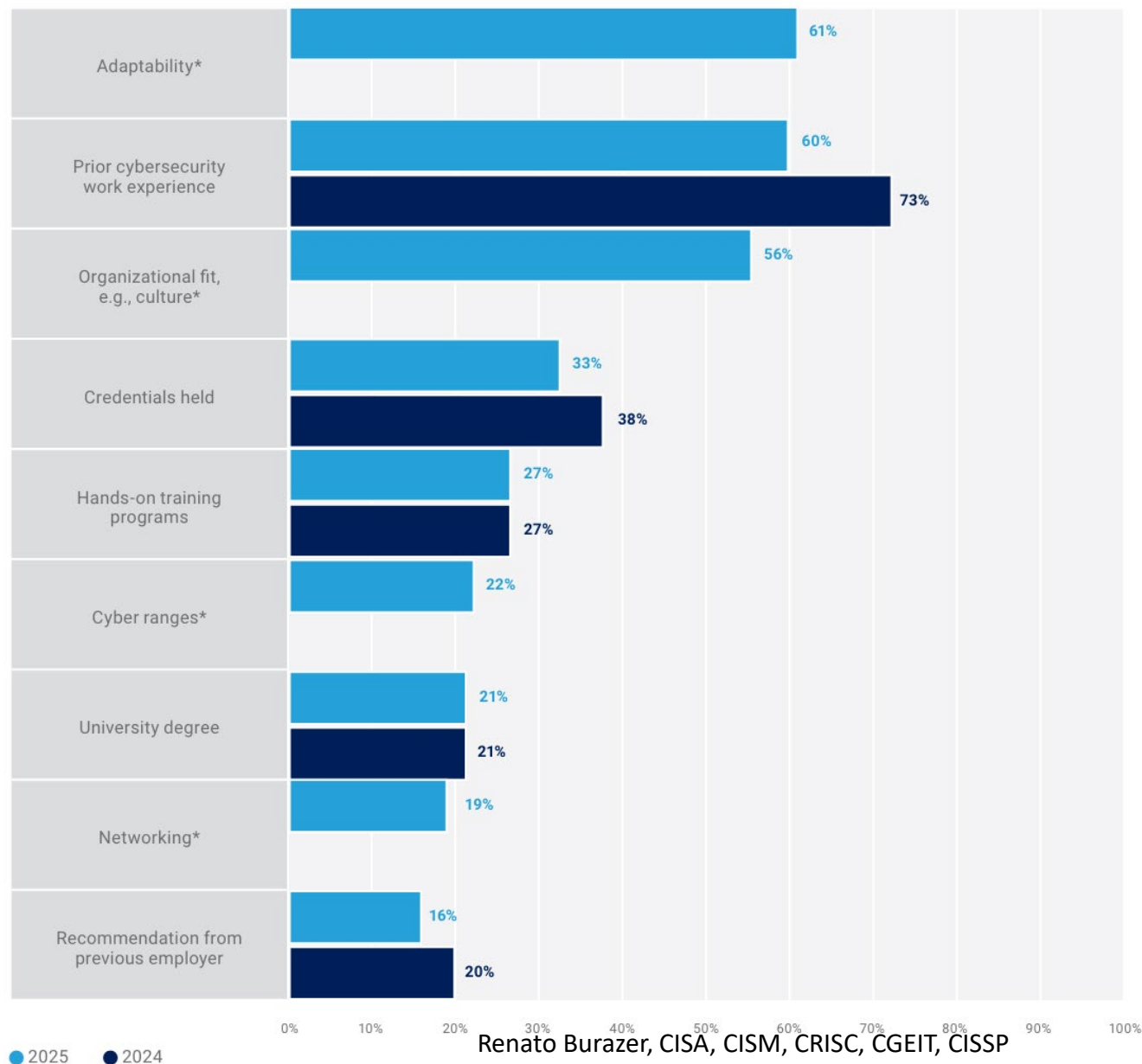
State of Cybersecurity 2025

Global Update on Workforce Efforts, Resources, and Cybersecurity Operations



FIGURE 5: Factors Indicating Candidate Qualification

How important are each of the following factors in determining if a cybersecurity candidate is qualified? Percentages represent respondents indicating these factors as "very important."



*New factor in 2025 survey

FIGURE 13 Skill Gaps in Today's Cybersecurity Professionals

What are the biggest skill gaps you see in today's cybersecurity professionals?

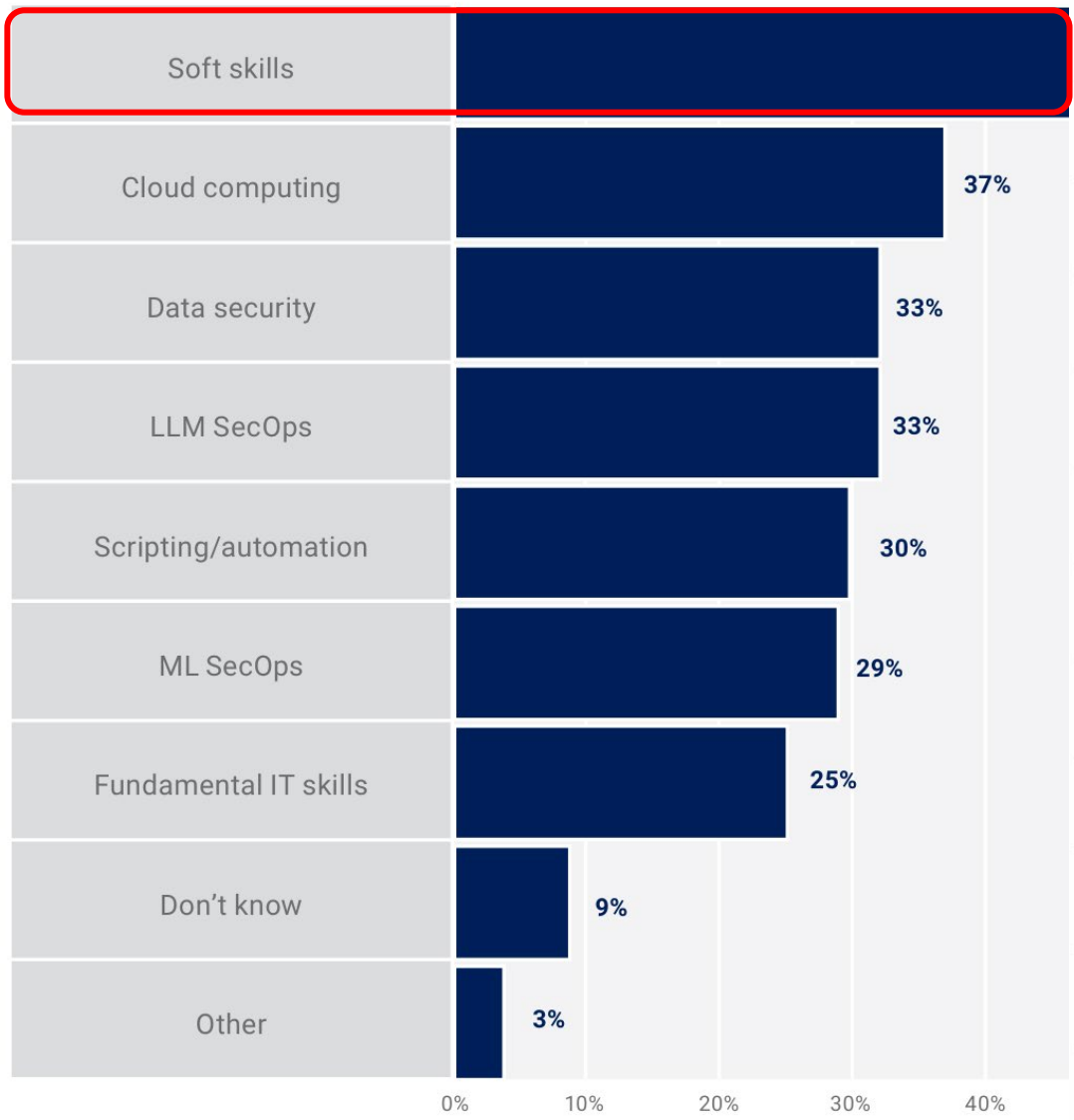
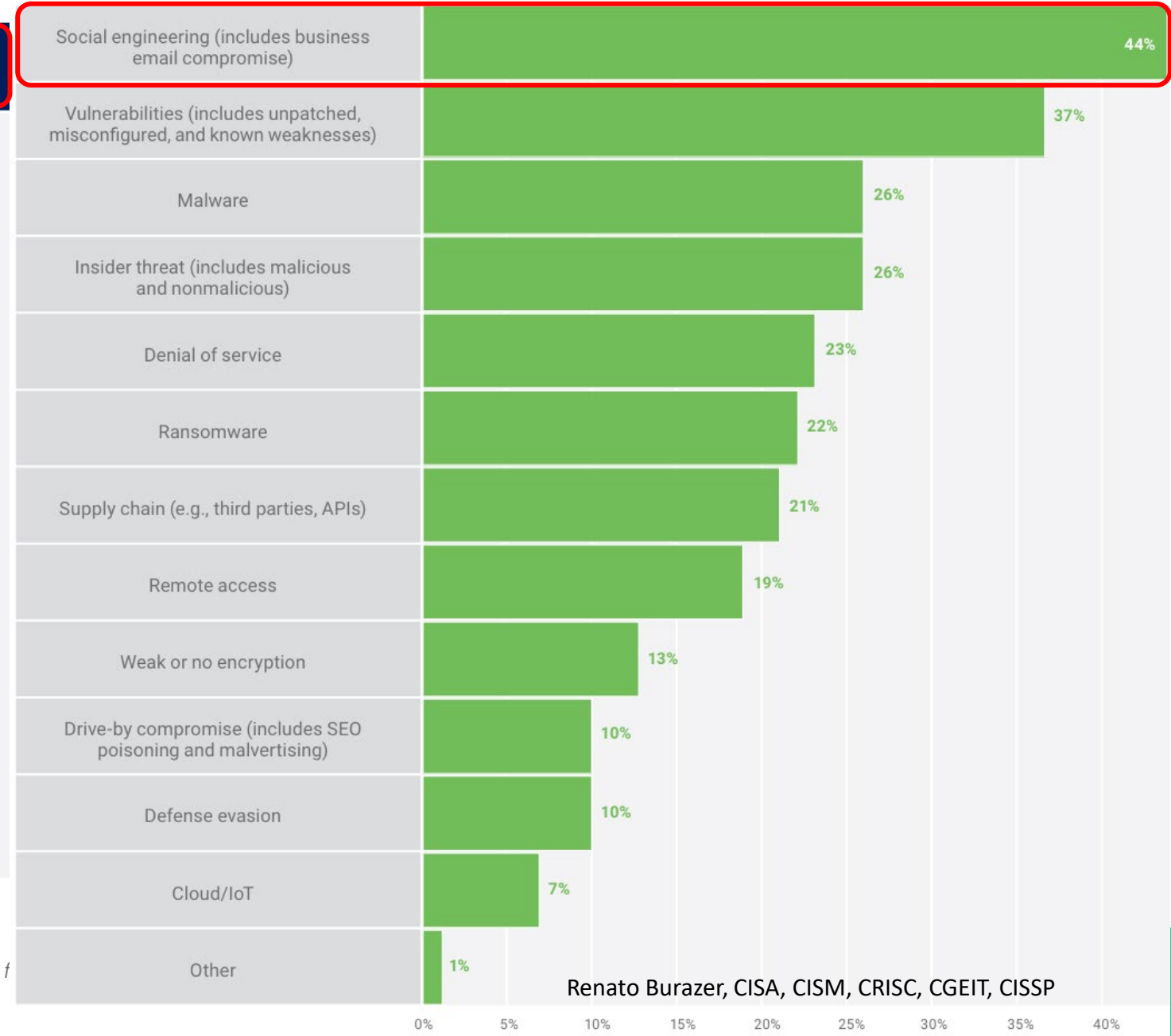


FIGURE 21 Attack Vectors Used

Which of the following attack vectors were used when your organization was compromised?

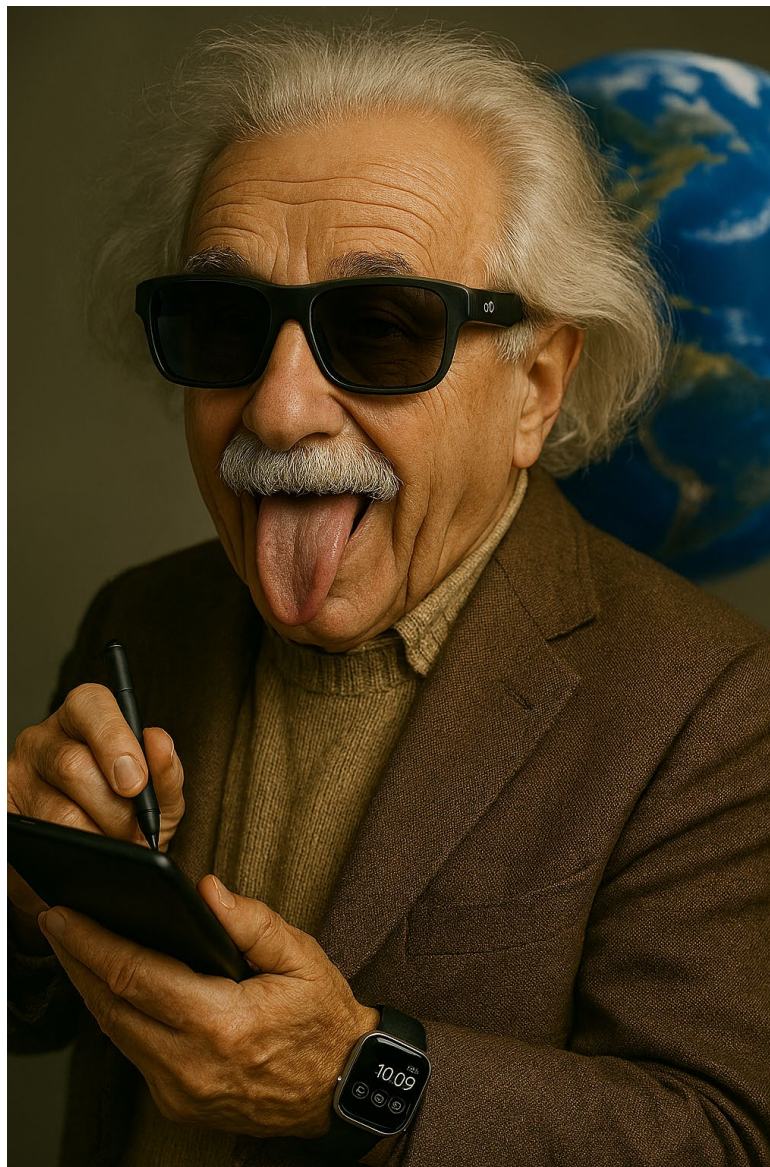


“Učiti se

učiti se

učiti se!”

Avtor:



Vir: General avtor (RB) z orodji UI – MS Copilot

Renato Burazer, CISA, CISM, CRISC, CGEIT, CISSP

- Neprekinjeno
- Podprto s tehnologijo, človeško in umetno inteligenco
- Uporaba podatkovnih jezer, avtomatizacija testiranja populacij, napovedni kazalniki za šibke kontrole ali prevare
- Sodelovanje v hibridnih timih pri podajanju zagotovil v verigi tretjih strani
- Zaupanja vredno svetovanje in etično presojevanje

Revizor IS 2.0 je

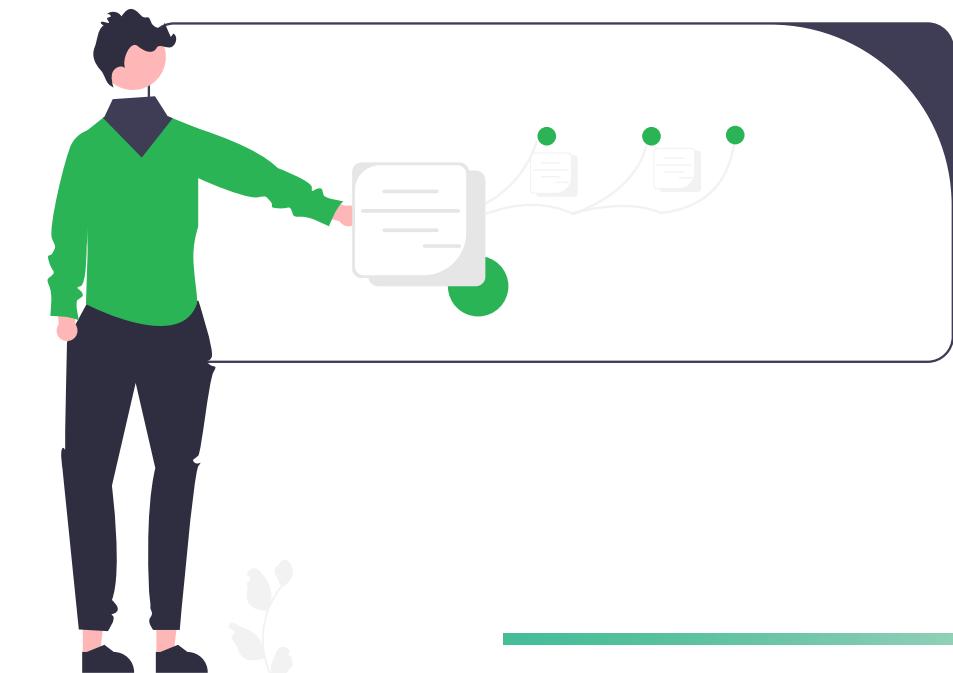
- tehnološki strokovnjak,
- podatkovni znanstvenik in
- strateški svetovalec za tveganja.

Odlično izkorišča
tehnologijo za svoje
postopke.

Podaja presojo in etiko.



Vir: General avtor (RB) z orodji UI – MS Copilot



Perspektiva prihodnosti (2025–2030)

Od skladnosti → k zaupanju

Od kontrole → k odpornosti

Od podjetja → k ekosistemu

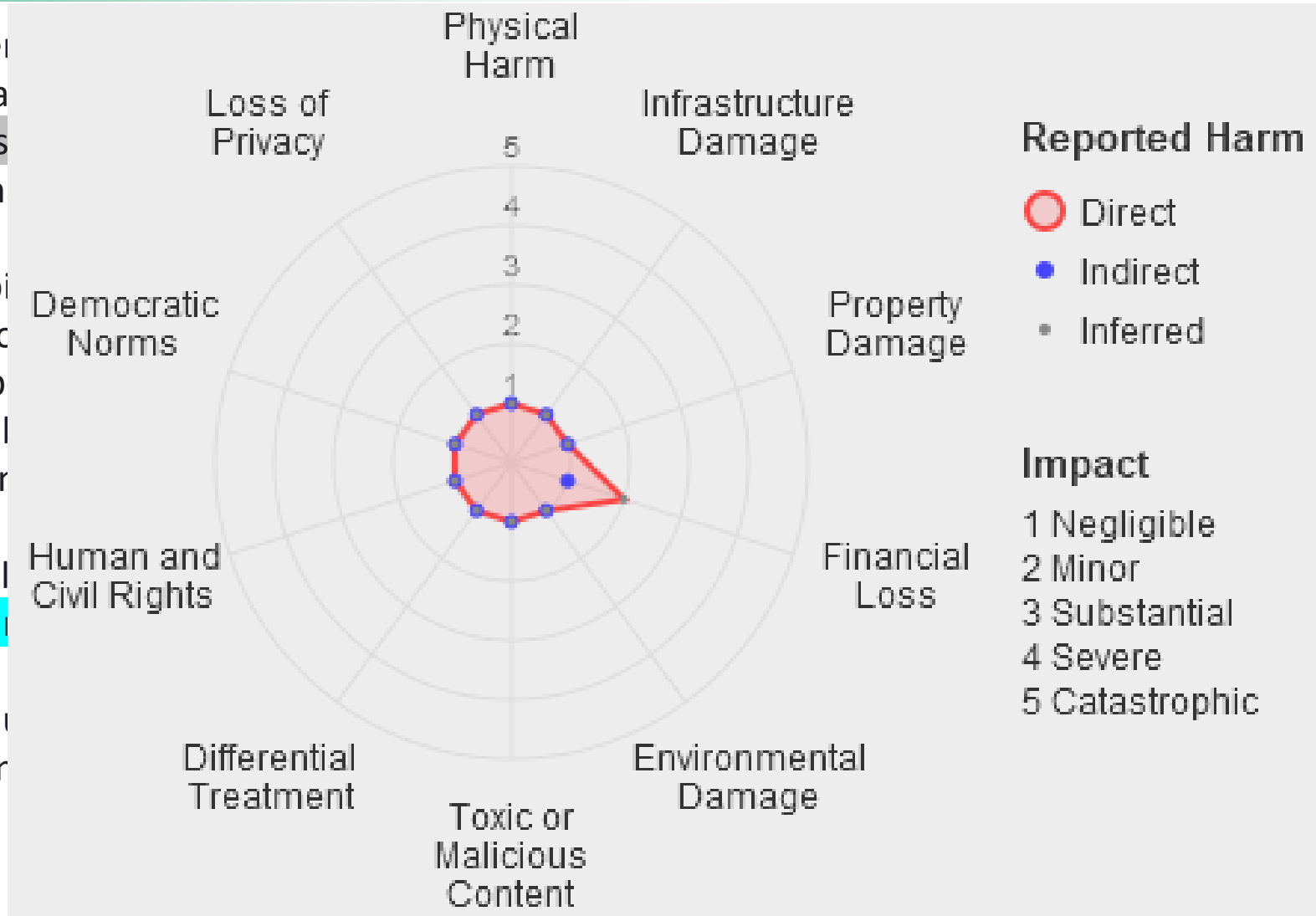
Izmišljena pravna navedba (mnenje, sodba)

Povzetek (AI incident)
BIG4 je pripravil vla
izmišljene akademsk
uporabljena umetn

.... ugotovljeno je bi
za socialno skrbstvo
..... poročilo je vseb
..... poročilo je vsel
se ta navedba dejar

Ko je **BIG4** predložil
reference ne podp

Več akademikov je
zaposlovanje in odr



n, ki je vsebovalo
poročila

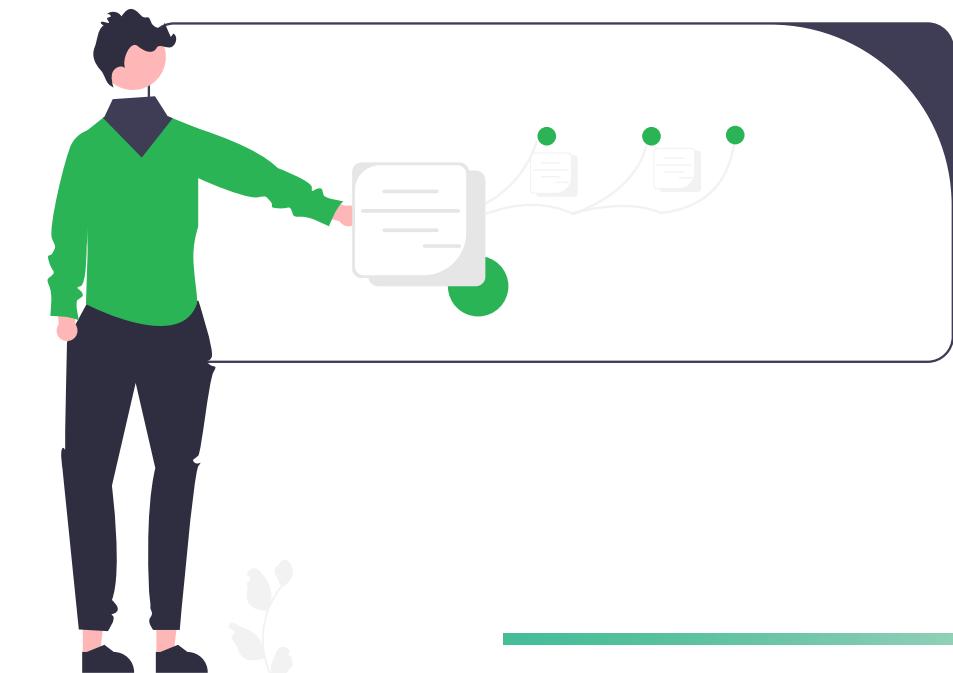
a jih je akademik

bah.

XXXXX, čeprav

, da nove

tvo za



Zaključek (skoraj)



Vir: General avtor (RB) z orodji UI – MS Copilot

Revizija IKT - zaupanja vredna digitalna družba
Revizor IS 2.0 = ključni člen
Vizualizacija prihodnosti revizorja IS z UI (opcija)

Hvala za pozornost!

Renato Burazer, CISA, CISM, CRISC, CGEIT, CISSP

renato@arem-psn.com

