SISTEMATIČNE REŠITVE ZA ZAGOTAVLJANJE KOMPETENTNEGA KADRA NA PODROČJU KIBERNETSKE VARNOSTI: ANALIZA DOBRIH PRAKS V IZBRANIH DRŽAVAH

ANDREJA MARKUN, ALENKA BREZAVŠČEK
Univerza v Mariboru, Fakulteta za organizacijske vede, Kranj, Slovenija
andreja.markun@student.um.si, alenka.brezavscek@um.si

Pomanjkanje strokovnjakov za kibernetsko in informacijsko varnost predstavlja enega ključnih izzivov digitalne preobrazbe, skladnosti z zakonodajo in izboljšanja nacionalne odpornosti. Prispevek predstavlja pripravljalno študijo za doktorsko raziskavo, katere cilj je razviti konceptualni model za zmanjšanje vrzeli med visokim šolstvom in potrebami gospodarstva na področju kibernetske varnosti v Sloveniji. Izhodišče so rezultati preliminarne raziskave na vzorcu 235 slovenskih organizacij, ki je pokazala izrazite kompetenčne vrzeli, strukturne ovire pri razvoju kadrov ter vpliv zakonodaje (NIS2, ZInfV-1) na organizacijske in kadrovske ukrepe. Za umestitev ugotovitev v širši kontekst je izvedena primerjalna analiza Estonije, Finske, Nizozemske, Irske in Kanade. Rezultati potrjujejo kadrovski primanjkljaj v analiziranih državah ter izpostavljajo dobre prakse, kot so nacionalni kompetenčni centri, modeliranje potreb in sistematično spremljanje trga dela. Primerjalna analiza omogoča identifikacijo ključnih elementov, ki lahko služijo kot podlaga za oblikovanje slovenskega modela. Prispevek predstavlja prvi korak k razvoju podatkovno podprtega pristopa za krepitev razpoložljivega kompetentnega kadra v Sloveniji.

DOI
https://doi.org/10.18690/um.fov.3.2026.36

ISBN
978-961-299-124-1

Ključne besede:
kompetence, kibernetska varnost, informacijska varnost, vrzel v znanju, primerjalne analize, razvoj kadrov

Univerzitetna založba Univerze v Mariboru

DOI
https://doi.org/
10.18690/um.fov.3.2026.36

ISBN
978-961-299-124-1

Systematic Solutions for Ensuring a Competent Cybersecurity Workforce: A Comparative Analysis of Best Practices in Selected Countries

Andreja Markun, Alenka Brezavšček
University of Maribor, Faculty of Organizational Sciences, Kranj, Slovenia
andreja.markun@student.um.si, alenka.brezavscek@um.si

Keywords:
competences,
cybersecurity,
information security,
skills gap,
comparative analysis,
workforce development

The shortage of cyber security and information security professionals is a key challenge of digital transformation, regulatory compliance, and national resilience. This paper presents a preparatory study for a doctoral research project aimed at developing a conceptual model to reduce the gap between higher education and labour market needs in cyber security in Slovenia. It builds on findings from a preliminary survey of 235 Slovenian organisations, revealing significant competence gaps, structural barriers to workforce development, and the impact of legislation (NIS2, ZInfV-1) on organisational and HR measures. To place the findings in a broader context, a comparative analysis of Estonia, Finland, the Netherlands, Ireland, and Canada was conducted. The results confirm workforce shortages across the analysed countries and highlight good practices such as national competence centres, needs modelling, and systematic labour market monitoring. The paper represents a first step toward a data-driven approach to strengthening cyber security competences in Slovenia.

University of Maribor Press

1 Uvod

Kibernetska varnost predstavlja eno temeljnih področij sodobne informacijske družbe, saj je neposredno povezana z zanesljivim delovanjem organizacij, varstvom podatkov in zagotavljanjem neprekinjenega poslovanja. Digitalna preobrazba, povečana odvisnost od informacijskih sistemov ter vse bolj kompleksne kibernetske grožnje so v zadnjih letih bistveno povečale potrebo po ustrezno usposobljenem kadru na področju informacijske in kibernetske varnosti. Hkrati številne države in organizacije poročajo o izrazitem pomanjkanju strokovnjakov, kar postaja velika ovira pri doseganju strateških ciljev na področju varnosti in digitalnega razvoja.

Pomanjkanje strokovnega kadra na področju informacijske in kibernetske varnosti ni zgolj posledica tehnološkega napredka, temveč odraža širše strukturno neskladje med izobraževalnimi sistemi, potrebami trga dela in regulatornimi zahtevami. Uveljavljanje novih zakonodajnih okvirov, kot je direktiva NIS2, dodatno povečuje zahteve glede razpoložljivosti ustreznih kompetenc, saj od organizacij zahteva višjo stopnjo formalizacije procesov, jasno razmejene odgovornosti ter strokovno podporo pri obvladovanju kibernetskih tveganj. V tem kontekstu se vprašanje razvoja kibernetskih kompetenc vse pogosteje umešča v širši okvir nacionalne varnosti, odpornosti kritične infrastrukture in dolgoročne konkurenčnosti gospodarstva.

Mednarodne raziskave in poročila kažejo, da je pomanjkanje strokovnjakov za kibernetsko in informacijsko varnost razširjen pojav, ki presega posamezne nacionalne kontekste. Kljub podobnim izzivom se države razlikujejo v načinu, kako sistematično pristopajo k razvoju in zagotavljanju ustreznega kadra. Nekatere so vzpostavile nacionalne strategije in institucionalne mehanizme za spremljanje ter načrtovanje potreb po kompetencah, druge pa problem obravnavajo predvsem z delnimi ali kratkoročnimi ukrepi, ki ne naslavljajo temeljnih vzrokov kadrovskih vrzeli.

Namen prispevka je analizirati sistematične pristope in dobre prakse, s katerimi izbrane države naslavljajo pomanjkanje kompetentnega kadra na področju kibernetske varnosti. Primerjalna analiza vključuje Estonijo, Finsko, Nizozemsko in Irsko kot predstavnice evropskega prostora ter Kanado kot primer širšega mednarodnega okolja. Izbor držav temelji na razpoložljivosti relevantnih

nacionalnih dokumentov, razvitih politik razvoja kompetenc ter obstoju institucionalnih rešitev, namenjenih usklajevanju izobraževanja, trga dela in varnostnih zahtev.

2 Teoretična izhodišča

Znanstvena literatura navaja, da ne bo dovolj ustrezno usposobljenih ljudi na področju informacijske in kibernetske varnosti, kar kaže na sistemski problem, ki vpliva ne le na nekaj organizacij, temveč na celoten gospodarski sistem, javno upravo in nacionalno varnost. Nekateri raziskovalci to pojasnjujejo kot kvantitativno pomanjkanje specialistov, medtem ko drugi opozarjajo na kompetenčno pomanjkanje, saj razkorak v znanju in veščinah presega zgolj kvantitativno pomanjkanje kadrov na področju kibernetske varnosti (Jerman Blažič, 2021; Dupont et al., 2023). Sistematična narava problema se odraža tudi v mednarodnih pregledih (ISC2, 2024), ki poudarjajo večmilijonsko pomanjkanje strokovnjakov na področju kibernetske varnosti po vsem svetu in priznava, da se to kljub številnim pobudam in prizadevanjem ne zmanjšuje, temveč se z digitalizacijo, porastom kibernetskih napadov in zaostrovanjem zakonodaje celo stopnjuje. S tem se potrjuje hipoteza, da pomanjkanje strokovnjakov na področju kibernetske varnosti ni zgolj začasno neravnovesje na trgu dela, temveč predstavlja strukturno in dolgoročno stanje, ki zahteva sistemske in trajnostne rešitve. Literatura, ki obravnava strukturo in vsebino kibernetskih kompetenc, pomembno teoretično prispeva k razumevanju tega vprašanja. Sistematični pregledi literature opozarjajo, da kompetenčna vrzel ne zajema zgolj tehničnih znanj, temveč tudi širše dimenzije, kot so obvladovanje tveganj, upravljanje varnosti, zagotavljanje skladnosti z regulativo ter obvladovanje organizacijske kompleksnosti (Nkongolo et al., 2023).

Takšna širša konceptualizacija predstavlja ključno izhodišče za celovito razumevanje kompetenc, ki presegajo ozko osredotočenost na tehnično usposabljanje. Literatura izpostavlja tudi omejitve tradicionalnih pedagoških pristopov. Hitrost tehnološkega razvoja in dinamika znanja nakazujeta, da formalno izobraževanje samo ne more zagotavljati dolgoročne ustreznosti kadrov. Zato je vse bolj poudarjen pomen vseživljenjskega učenja, prekvalifikacij ter tesnejšega povezovanja izobraževalnih ustanov, gospodarstva in države v okviru kontinuiranega razvoja kompetenc (Jerman Blažič, 2021; ENISA, 2020).

3 Konceptualni analitični okvir nacionalnega sistema razvoja kibernetskih kompetenc

Za namen primerjalne analize nacionalnih pristopov k razvoju kibernetskih kompetenc je bil zasnovan konceptualni analitični okvir, ki omogoča strukturirano, pregledno in primerljivo obravnavo izbranih držav. Okvir ne predstavlja normativnega modela, temveč analitično orodje, ki temelji na sintezi znanstvene literature in analizi nacionalnih strateških dokumentov ter poročil s področja razvoja kibernetskih znanj in kadrov (Jerman Blažič, 2021; ENISA, 2020; Dupont et al., 2023; ISC2, 2024).

Izhodišče za oblikovanje analitičnega okvira je ugotovitev, da se nacionalni sistemi razvoja kibernetskih kompetenc med državami razlikujejo ne le po obsegu vlaganj ali številu izobraževalnih programov, temveč predvsem po načinu institucionalne ureditve, mehanizmih razvoja znanj, stopnji povezovanja s trgom dela ter zrelosti pristopov k spremljanju in dolgoročnemu načrtovanju kadrovskih potreb. Na podlagi pregleda literature in dokumentov je bilo zato identificiranih pet ključnih dimenzij, ki skupaj zajemajo temeljne strukturne značilnosti nacionalnih pristopov.

Prva dimenzija je **institucionalni okvir**, ki se nanaša na razdelitev odgovornosti, koordinacijske mehanizme in stopnjo centralizacije sistema razvoja kibernetskih kompetenc. Druga dimenzija vključuje **mehanizme razvoja in nadgradnje kompetenc**, kot so formalno izobraževanje, neformalno usposabljanje, prekvalifikacije in vseživljenjsko učenje. Tretja dimenzija se nanaša na **povezavo med izobraževalnim sistemom in trgom dela** ter stopnjo vključenosti delodajalcev v oblikovanje in izvajanje izobraževalnih poti. Četrta dimenzija obravnava **spremljanje in načrtovanje kadrovskih potreb**, torej uporabo podatkov, analiz in (potencialno) napovednih mehanizmov za razumevanje sedanjih in prihodnjih potreb. Peta dimenzija se nanaša na **dolgoročno vzdržnost sistema**, zlasti na vpetost razvoja kibernetskih kompetenc v širše nacionalne strategije, stabilnost financiranja in kontinuiteto politik.

Razširjeni analitični okvir, ki povezuje navedene dimenzije s sistemskim, nacionalnim in organizacijskim vidikom, je povzet v Tabeli 1. V nadaljevanju je ta okvir uporabljen kot osnovno orodje za primerjalno analizo izbranih držav v 4.

poglavju, kjer posamezne dimenzije služijo kot struktura za sistematično in vsebinsko primerljivo obravnavo nacionalnih pristopov.

Tabela 1: Razširjen analitični okvir primerjalne analize nacionalnih pristopov

Analitična dimenzija	Sistemsko-nacionalni vidik	Organizacijski vidik	Teoretična podlaga
Institucionalni okvir	Koordinacija politik, nosilci odgovornosti, stabilnost sistema	Preglednost okolja, dostop do podpornih struktur	Jerman Blažič (2021); Dupont et al. (2023)
Mehanizmi razvoja kompetenc	Nacionalni programi, usposabljanja, preusposabljanja	Razpoložljivost in nadgradnja znanj zaposlenih	Nkongolo et al. (2023); ENISA (2020)
Povezava izobraževanja in trga dela	Partnerstva, prilagajanje izobraževalnih programov	Ustreznost znanj kadra	Jerman Blažič (2021)
Spremljanje in načrtovanje potreb	Analize trga dela, napovedni mehanizmi	Zmanjšanje kadrovskih tveganj	Dupont et al. (2023); ISC2 (2024)
Dolgoročna vzdržnost	Vključitev v strategije, stabilno financiranje	Stabilnost kadrovskega okolja	ENISA (2020)

Vir: lasten

4 Primerjalna analiza izbranih držav

Primerjalna analiza nacionalnih pristopov k razvoju kompetentne delovne sile na področju informacijske in kibernetske varnosti temelji na analitičnem okviru, predstavljenem v prejšnjem poglavju. Namen analize ni podati opisni prikaz posameznih nacionalnih ureditev, temveč identificirati ključne razlike in skupne značilnosti med državami glede sistemske organizacije razvoja kibernetskih kompetenc ter njihovih učinkov na organizacije in kadrovske sisteme. Analiza vključuje primere iz Estonije, Finske, Nizozemske, Irske in Kanade, ki predstavljajo različne modele institucionalnih ureditev, ravni vključenosti deležnikov in pristope k razvoju in upravljanju kibernetskih kompetenc.

4.1 Institucionalni okvir razvoja kibernetskih kompetenc

Institucionalni okvir predstavlja temelj nacionalnega sistema razvoja kibernetskih kompetenc, saj določa razdelitev odgovornosti, mehanizme koordinacije med ključnimi akterji ter stabilnost podpornega okolja za organizacije. Znanstvena literatura poudarja, da imajo države z jasno opredeljenimi institucionalnimi vlogami

in učinkovitimi koordinacijskimi strukturami večjo sposobnost dolgoročnega in sistematičnega naslavljanja kadrovskih ter kompetenčnih vrzeli na področju kibernetske varnosti (Jerman Blažič, 2021; Dupont et al., 2023).

Primerjalna analiza nacionalnih dokumentov kaže, da analizirane države uporabljajo tri osnovne tipe institucionalnih ureditev: (1) bolj centraliziran in državno koordiniran model, (2) medresorski ali partnerski model ter (3) hibridni model, ki združuje nacionalne in sektorske ravni. Estonija predstavlja primer izrazito centraliziranega pristopa, v katerem ima država močno koordinacijsko vlogo, razvoj kompetenc pa umešča v širši okvir nacionalne kibernetske odpornosti (Estonian Cyber Security Strategy, 2024; Estonia Cybersecurity Skills Needs Analysis, 2023). Finska uporablja medresorski model, kjer so odgovornosti razdeljene med več državnih organov, poudarek pa je na dolgoročnem usklajevanju in skupnem strateškem okviru (Finland's Cyber Security Strategy, 2024).

Nizozemska in Irska temeljita predvsem na partnerskih in sektorsko usmerjenih institucionalnih ureditvah, v katerih ima pomembno vlogo sodelovanje med državo, industrijo ter izobraževalno-raziskovalnimi institucijami. V nizozemskem primeru je razvoj kompetenc organiziran prek javno-zasebnih partnerstev in mrežnih struktur (Security Delta, 2023), medtem ko je na Irskem poudarek na razvoju kibernetskega ekosistema in vlogi industrijskih pobud pri usklajevanju potreb trga dela in izobraževanja (State of the Cyber Security Sector in Ireland, 2022). Kanada predstavlja hibridni model, kjer nacionalni strateški okvir dopolnjujejo sektorski in regionalni pristopi, kar povečuje raznolikost podpornih mehanizmov in kompleksnost institucionalnega okolja (Cybersecurity Skills Canada, 2023).

Kljub razlikam v stopnji centralizacije in organizaciji institucionalnih ureditev primerjalna analiza kaže, da so uspešnejši in vzdržnejši tisti sistemi, ki zagotavljajo jasno razmejene odgovornosti, stabilne koordinacijske mehanizme in dolgoročno kontinuiteto politik. Takšni institucionalni okviri organizacijam omogočajo bolj predvidljivo okolje za načrtovanje razvoja kadrov ter zmanjšujejo tveganja, povezana s pomanjkanjem ključnih znanj. Povzetek ključnih značilnosti institucionalnih ureditev v izbranih državah je prikazan v Tabeli 2.

Tabela 2: Institucionalni okvir razvoja kibernetskih kompetenc v izbranih državah

Država	Stopnja centralizacije	Ključni nosilci	Tip institucionalnega pristopa
Estonija	Visoka	Državne in varnostne institucije	Centraliziran
Finska	Srednja	Več resorjev	Medresorski
Nizozemska	Nizka	Javno-zasebna partnerstva	Mrežni
Irska	Srednja	Industrijski in državni akterji	Sektorski
Kanada	Nizka–srednja	Zvezni, sektorski in regionalni akterji	Hibridni

Vir: lasten

4.2 Mehanizmi razvoja in nadgradnje kibernetskih kompetenc

Mehanizmi razvoja in nadgradnje kompetenc so osrednji operativni element nacionalnih sistemov za zagotavljanje ustrezno usposobljenega kadra na področju informacijske in kibernetske varnosti. Medtem ko institucionalni okvir določa organizacijo in odgovornosti, ti mehanizmi neposredno vplivajo na to, kako hitro in učinkovito se znanja razvijajo, posodabljajo in prilagajajo potrebam organizacij (Nkongolo et al., 2023; ENISA, 2020).

Primerjalna analiza nacionalnih dokumentov kaže, da kljub skupnemu cilju zmanjševanja kompetenčnih vrzeli obstajajo pomembne razlike v organizaciji razvoja znanj. Na podlagi analiziranih primerov je mogoče identificirati tri prevladujoče tipe pristopov k razvoju kibernetskih kompetenc: (1) državno koordiniran in formaliziran model, (2) model, ki temelji na vseživljenjskem učenju in stalni nadgradnji znanj, ter (3) tržno-partnerski model, ki poudarja prilagodljive, modularne in industrijsko usmerjene oblike usposabljanja.

Estonija predstavlja primer prvega tipa, kjer ima država močno vlogo pri usmerjanju razvoja znanj, formalno izobraževanje, specializirana usposabljanja in ciljno usmerjeni programi pa so vključeni v nacionalno usklajen okvir (Estonia Cybersecurity Skills Needs Analysis, 2023). Finska se bolj približuje drugemu tipu, saj nacionalna strategija izrecno poudarja koncept vseživljenjskega učenja, stalno posodabljanje znanj in prilagodljivost izobraževalnih poti (Finland's Cyber Security Strategy, 2024). Nizozemska, Irska in Kanada v večji meri sledijo tretjemu tipu pristopa, kjer razvoj kompetenc temelji na sodelovanju med državo, industrijo in izobraževalnimi institucijami, z izrazitim poudarkom na modularnih programih,

certifikacijah in ciljno usmerjenih usposabljanjih (Security Delta, 2023; State of the Cyber Security Sector in Ireland, 2022; Cybersecurity Skills Canada, 2023).

Ne glede na izbrani model primerjalna analiza kaže, da so uspešnejši sistemi, ki združujejo več različnih učnih poti in omogočajo fleksibilen prehod med formalnim izobraževanjem, dodatnim usposabljanjem in prekvalifikacijami. Takšni pristopi organizacijam omogočajo hitrejše prilagajanje novim zahtevam področja kibernetske varnosti in zmanjšujejo njihovo odvisnost od izključno dolgoročnih izobraževalnih ciklov. Povzetek ključnih značilnosti mehanizmov razvoja kompetenc v izbranih državah je prikazan v Tabeli 3.

Tabela 3: Mehanizmi razvoja in nadgradnje kibernetskih kompetenc v izbranih državah

Država	Prevladujoči mehanizmi	Vloga države	Organizacijski učinki
Estonija	Formalno izobraževanje, ciljno usmerjena usposabljanja	Visoka	Stabilna baza znanj
Finska	Vseživljenjsko učenje, stalna nadgradnja	Srednja–visoka	Aktualna znanja zaposlenih
Nizozemska	Modularni programi, industrijsko sodelovanje	Srednja	Hitro prilagajanje potrebam
Irska	Certifikacije, industrijska usposabljanja	Srednja	Hiter odziv trga
Kanada	Formalno izobraževanje, preusposabljanje	Raznolika	Širša kadrovska baza

Vir: lasten

4.3 Povezava izobraževalnega sistema in trga dela

Eden ključnih strukturnih vzrokov za pomanjkanje kadra na področju kibernetske varnosti ni zgolj obseg izobraževalnih programov, temveč predvsem razkorak med znanji, ki jih izobraževalni sistem zagotavlja, in dejanskimi potrebami organizacij (Jerman Blažič, 2021; ENISA, 2020). Primerjalna analiza nacionalnih dokumentov zato posebno pozornost namenja mehanizmom, s katerimi države poskušajo sistematično povezovati izobraževanje in trg dela.

Analiza kaže, da vse obravnavane države prepoznavajo vključevanje delodajalcev kot ključen element zmanjševanja tega razkoraka, vendar se bistveno razlikujejo v stopnji formalizacije in institucionalne vpetosti teh mehanizmov. V bolj strukturiranih modelih, kot je estonski, so delodajalci vključeni v oblikovanje učnih izidov, razvoj programov in izvajanje praktičnega usposabljanja v okviru nacionalno

koordiniranega sistema (Estonia Cybersecurity Skills Needs Analysis, 2023). Podobno, vendar v bolj partnerski obliki, Nizozemska in Irska razvijata sodelovanje med izobraževalnimi institucijami in industrijo prek sektorskih pobud in mrežnih struktur (Security Delta, 2023; State of the Cyber Security Sector in Ireland, 2022). V drugih primerih, zlasti v Kanadi, je povezovanje izobraževanja in trga dela bolj razpršeno in poteka prek kombinacije nacionalnih, sektorskih in regionalnih pobud, kar povečuje prilagodljivost sistema, hkrati pa zmanjšuje njegovo preglednost in enotnost (Cybersecurity Skills Canada, 2023). Finska se v tem kontekstu osredotoča predvsem na prožnost izobraževalnih poti in koncept vseživljenjskega učenja, s katerim poskuša omogočiti hitrejše prilagajanje znanj spreminjajočim se potrebam trga dela (Finland's Cyber Security Strategy, 2024).

Skupna značilnost večine analiziranih pristopov je premik od togih, dolgoročnih izobraževalnih programov k bolj modularnim in prilagodljivim oblikam usposabljanja, ki omogočajo hitrejše zapolnjevanje specifičnih vrzeli v znanjih. Primerjalna sinteza dokumentov kaže, da bolj formalizirani in sistemsko vpeti mehanizmi sodelovanja med izobraževalnim sistemom in gospodarstvom prispevajo k večji usklajenosti med ponudbo znanj in potrebami organizacij ter zmanjšujejo obseg dodatnega usposabljanja, ki ga morajo organizacije zagotavljati po zaposlitvi. Ključni poudarki nacionalnih pristopov so povzeti v Tabeli 4.

Tabela 4: Ključni poudarki nacionalnih dokumentov glede povezave izobraževanja in trga dela

Vidik povezovanja	Povzetek ugotovitev iz dokumentov	Primeri virov
Vloga delodajalcev	Soustvarjanje programov, praktično usposabljanje	Estonia Cybersecurity Skills Needs Analysis (2023); Security Delta (2023); Cybersecurity Skills Canada (2023)
Prilagodljivost poti	Modularni programi, vseživljenjsko učenje	Finnish Government (2024); Cybersecurity Skills Canada (2023)
Sektorski pristopi	Industrijska združenja, partnerske mreže	State of the Cyber Security Sector in Ireland (2022)
Sistemskost	Centralizirani in razpršeni modeli	Estonia Cybersecurity Skills Needs Analysis (2023); Cybersecurity Skills Canada (2023)

Vir: lasten

4.4 Spremljanje in načrtovanje kadrovskih potreb

Spremljanje in načrtovanje kadrovskih potreb predstavlja ključen element sistemskega upravljanja kompetenc na področju informacijske in kibernetske varnosti. Medtem ko razvoj izobraževalnih mehanizmov in mehanizmov za usposabljanje naslavlja obstoječe vrzeli, spremljanje potreb omogoča razumevanje dinamike trga dela in predstavlja osnovo za pravočasno prilagajanje politik, programov in organizacijskih praks. Literatura s področja upravljanja kompetenc poudarja, da brez sistematične informacijske podlage nacionalni pristopi ostajajo pretežno reaktivni in omejeni na odzivanje na že zaznane pomanjkljivosti (Jerman Blažič, 2021; ENISA, 2020).

V tem poglavju je spremljanje in načrtovanje kadrovskih potreb analizirano na podlagi nacionalnih strategij in poročil, s poudarkom na mehanizmih zbiranja, analize in uporabe podatkov o potrebah po kibernetskih kompetencah. Analiza se ne osredotoča na obseg primanjkljaja kadra, temveč na vprašanje, ali in kako dokumenti opredeljujejo sistematične pristope k razumevanju sedanjih in prihodnjih potreb trga dela.

Analizirani dokumenti večinoma izpostavljajo uporabo analiz trga dela in poročil o kompetenčnih vrzelih kot osnovni vir informacij za oblikovanje politik. Ta poročila praviloma temeljijo na kombinaciji statističnih podatkov, anket med delodajalci in strokovnih ocen, pri čemer je poudarek predvsem na identifikaciji trenutnega stanja in zaznanih pomanjkljivosti (Estonia Cybersecurity Skills Needs Analysis, 2023; Cybersecurity Skills Canada, 2023). Takšen pristop omogoča razmeroma dobro razumevanje obstoječih potreb, vendar dokumenti le redko navajajo uporabo formaliziranih napovednih modelov za dolgoročno načrtovanje.

Nekateri dokumenti poleg splošnih analiz trga dela omenjajo tudi sektorske ali tematske ocene potreb, ki omogočajo bolj ciljno usmerjen vpogled v posamezne dele kibernetskega ekosistema. Sektorska poročila poudarjajo pomen sodelovanja z industrijo in strokovnimi združenji pri prepoznavanju specifičnih znanj, ki so v določenem obdobju najbolj iskana (State of the Cyber Security Sector in Ireland, 2022). Ti pristopi izboljšujejo relevantnost podatkov, vendar so pogosto omejeni na posamezne sektorje in niso nujno povezani v celovit nacionalni sistem spremljanja.

V nacionalnih strategijah so zaznana prizadevanja za bolj kontinuirano spremljanje potreb po kibernetskih kompetencah, vendar so ti mehanizmi večinoma opisani le na konceptualni ravni. Strategije poudarjajo pomen podatkovno podprtih odločitev in rednega spremljanja trga dela, vendar redkeje navajajo konkretne metodologije, odgovorne institucije ali formalizirane procese napovedovanja prihodnjih potreb (Finnish Government, 2024; Security Delta, 2023). To kaže na razkorak med deklarativnimi cilji in operativno implementacijo sistematičnega načrtovanja kadrovskih potreb.

Pomembna ugotovitev analize je tudi razlika med bolj centraliziranimi in razpršenimi pristopi k spremljanju potreb. V nekaterih dokumentih je spremljanje kadrovskih potreb umeščeno v nacionalne analitične ali koordinacijske strukture, drugod pa je razpršeno med več institucij, sektorjev ali regij (Cybersecurity Skills Canada, 2023). Razpršeni pristopi povečujejo fleksibilnost in prilagodljivost, vendar otežujejo primerljivost podatkov in dolgoročno usklajevanje politik na nacionalni ravni.

Primerjalna sinteza analiziranih dokumentov kaže, da je spremljanje in načrtovanje kadrovskih potreb na področju kibernetske varnosti v večini primerov še vedno pretežno usmerjeno v opis trenutnega stanja. Čeprav dokumenti pogosto prepoznavajo pomen dolgoročnega načrtovanja in napovedovanja prihodnjih potreb, so konkretni mehanizmi za sistematično izvajanje teh nalog redko natančno opredeljeni. Posledično nacionalni sistemi razvoja kompetenc ostajajo v veliki meri reaktivni.

Za organizacije to pomeni omejeno predvidljivost kadrovskega okolja in večjo odvisnost od lastnih mehanizmov spremljanja potreb ter razvoja kompetenc. Z vidika sistemskega upravljanja kompetenc se kot ključni izziv izkazuje prehod od občasnih analiz in poročil h kontinuiranemu, podatkovno podprtemu spremljanju in načrtovanju, ki bi omogočalo bolj usklajene in dolgoročno vzdržne pristope k razvoju kibernetskega kadra.

4.5 Dolgoročna vzdržnost nacionalnih pristopov k razvoju kibernetskih kompetenc

Ko govorimo o pomanjkanju strokovnjakov na področju informacijske in kibernetske varnosti, hitro postane jasno, da posamezni ukrepi ne morejo prinesti trajnih rešitev. Novi študijski programi ali kratkoročna usposabljanja lahko začasno ublažijo najbolj pereče težave, vendar sami po sebi ne spremenijo dejstva, da gre za dolgoročen in strukturni izziv. Da bi imeli takšni ukrepi trajen učinek, morajo biti del širšega, stabilnega in prilagodljivega sistema, ki zna spremljati spremembe v okolju in se nanje pravočasno odzivati (Jerman Blažič, 2021; ENISA, 2020).

Pri pregledu nacionalnih dokumentov izbranih držav se pokaže, da dolgoročna vzdržnost ne temelji na eni sami rešitvi, temveč na kombinaciji več med seboj povezanih elementov. Med najpomembnejšimi so predvsem kontinuiteta institucij, sistematično spremljanje potreb ter sposobnost povezovanja različnih politik in deležnikov v bolj usklajeno celoto. Države, ki razvoj kibernetskih znanj umeščajo v širše strategije digitalnega in družbenega razvoja, s tem praviloma gradijo stabilnejši okvir, ki ne razpade ob koncu posameznega projekta ali političnega cikla (Finnish Government, 2024; Security Delta, 2023).

Eden pomembnejših premikov, ki bi jih bilo treba doseči, je prehod od predvsem reaktivnega k bolj proaktivnemu pristopu. Analiza kaže, da večina dokumentov še vedno izhaja iz opisa trenutnega stanja in že zaznanih vrzeli. Čeprav se pogosto omenja potreba po boljšem napovedovanju prihodnjih potreb, so konkretni mehanizmi za to – kdo, kako in s katerimi orodji naj to izvaja – večinoma še slabo razviti ali ostajajo na ravni splošnih usmeritev (Estonia Cybersecurity Skills Needs Analysis, 2023; Cybersecurity Skills Canada, 2023). Brez takšnih zmogljivosti sistemi težko pravočasno prilagajajo svoje politike, kar dolgoročno resno omejuje njihovo vzdržnost.

Zelo pomembno vlogo ima tudi način, kako je urejeno sodelovanje med različnimi akterji. Na deklarativni ravni skoraj vsi dokumenti poudarjajo pomen sodelovanja med izobraževalnimi institucijami, gospodarstvom in javnim sektorjem. V praksi pa se pokaže, da je velika razlika med sistemi, kjer so vloge jasno razdeljene in so vzpostavljeni trajni mehanizmi usklajevanja, ter tistimi, kjer večina sodelovanja poteka projektno ali znotraj posameznih sektorjev. Prvi praviloma izkazujejo večjo

stabilnost in predvidljivost, drugi pa so precej bolj odvisni od trenutnih pobud in razpoložljivih sredstev (State of the Cyber Security Sector in Ireland, 2022; Security Delta, 2023).

Pri tem ne gre spregledati, da vprašanje dolgoročne vzdržnosti ni zgolj stvar državnih strategij, temveč ima tudi zelo konkretne posledice za organizacije. Kadar nacionalni okvir ne zagotavlja dovolj stabilnega in predvidljivega razvoja kompetenc, so organizacije prisiljene prevzeti večino bremena nase, od lastnih programov usposabljanja do iskanja kadrov na zelo omejenem trgu. To pomeni večje stroške, več negotovosti in večje tveganje, da ključna znanja v določenem trenutku preprosto niso na voljo. V bolj usklajenih sistemih je to tveganje manjše, saj imajo organizacije boljšo osnovo za dolgoročno načrtovanje kadrov in so manj odvisne od improviziranih rešitev.

Če vse to povežemo, se izriše precej jasna slika: dolgoročno vzdržni nacionalni pristopi temeljijo na stabilnih institucionalnih okvirih, sposobnosti sistematičnega spremljanja in načrtovanja potreb ter na dejanskem, ne zgolj deklarativnem sodelovanju ključnih deležnikov. Kadar kateri od teh elementov manjka, obstaja resno tveganje, da politike ostanejo razdrobljene in usmerjene predvsem v kratkoročno »gašenje požarov«, kar dolgoročno ne more bistveno zmanjšati kompetenčnih vrzeli na področju kibernetske varnosti.

5 Sklep

Pomanjkanje strokovnega znanja na področju informacijske in kibernetske varnosti predstavlja kronično in strukturno težavo, ki presega zgolj vprašanje števila razpoložljivega osebja. Namen prispevka je bil izvesti primerjalno analizo sistemskih pristopov na podlagi različnih javno dostopnih nacionalnih dokumentov, v katerih so izbrane države zabeležile razvoj kibernetskih kompetenc, ter odkriti morebitne dobre prakse, ki bi jih bilo smiselno prenesti v slovenski prostor. Rezultati so pokazali, da med državami prevladuje raznolikost na ravni sistematičnosti in težnja po dolgoročni perspektivi razvoja in uporabe kibernetskih kompetenc. Nacionalni sistemi, ki razvoj znanja o kibernetiki umeščajo v širši institucionalni in strateški kontekst, izkazujejo višjo raven kontinuitete in večjo povezanost med izobraževanjem, trgom dela in potrebami organizacij. Strategije, osredotočene predvsem na programe ali sektorske dejavnosti, pa so preveč razdrobljene, da bi bile

trajnostne v spreminjajočem se okolju. Ena ključna ugotovitev prispevka je, da večina pregledanih dokumentov poudarja, da je sistematično spremljanje in načrtovanje potreb osebja nujno, čeprav so empirična orodja za dolgoročno napovedovanje potreb po kompetencah redka ali zgolj konceptualno opredeljena. Ti nacionalni sistemi razvoja kibernetskih kompetenc ostajajo večinoma reaktivni, saj jim primanjkuje sposobnosti hitrega prilagajanja spreminjajočim se tehnološkim in varnostnim okoljem. Študija je tudi pokazala, da dolgoročna trajnost nacionalnih pobud izhaja iz robustnih institucionalnih modelov organizacije, formaliziranega sodelovanja med deležniki ter uporabe podatkov kot orodja za usmerjanje odločanja. Države z rednimi koordinacijskimi okviri med javnim sektorjem, akademskimi institucijami in gospodarstvom so lahko bolj sposobne zmanjšati vrzeli v kompetencah in narediti okolje osebja v organizacijah bolj predvidljivo.

Z vidika Slovenije te ugotovitve nakazujejo, da bi bilo smiselno okrepiti strukturirano spremljanje in dolgoročno načrtovanje potreb po kibernetskih kompetencah ter bolj poenotiti politike, programe in deležnike, ki že obstajajo. Medtem ko bi bilo treba prenos najboljših praks iz tujine prilagoditi nacionalnemu kontekstu, zlasti na ravni institucionalnih ureditev in razpršenosti kompetenc, bo treba proces gradnje kibernetskih kompetenc obravnavati kot strateško in kot ne operativno vprašanje. Pomembna omejitev prispevka je, da analiza temelji izključno na javno dostopnih nacionalnih dokumentih, kar pomeni, da ne zajema dejanskega izvajanja politik in njihovega vpliva v praksi.

Primerjalni pristop prav tako ne omogoča kvantitativne ocene, v kolikšni meri posamezni nacionalni pristopi dejansko prispevajo k zmanjševanju kadrovske vrzeli. Te omejitve nakazujejo smeri nadaljnjih raziskav, zlasti potrebo po empiričnih študijah, poglobljenih analizah primerov ter razvoju celovitih konceptualnih modelov za ocenjevanje prihodnjih potreb po kompetencah na obravnavanem področju.

Kljub navedenim omejitvam prispevek ponuja strukturiran in primerjalno utemeljen vpogled v sistemske ukrepe za razvoj kibernetskih kompetenc ter predstavlja izhodišče za nadaljnje raziskave in strokovno razpravo v slovenskem prostoru.

Viri in literatura

Caldwell, T. (2013). Plugging the cyber-security skills gap. *Computer Fraud & Security, 2013*(7), 5–10. https://doi.org/10.1016/S1361-3723(13)70062-9

Cybersecurity Skills Canada. (2023). *Canadian cyber security skills framework*. Government of Canada. https://www.cyber.gc.ca/sites/default/files/canadian-cyber-security-skills-framework-may-2023.pdf

Dupont, B., Shearing, C., Bernier, M., & Leukfeldt, R. (2023). *The tensions of cyber-resilience: From sensemaking to practice*. Computers & Security, 132, 103372 https://www.sciencedirect.com/science/article/pii/S0167404823002821

ENISA. (2020). *Cybersecurity skills development in the EU*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/cybersecurity-skills-development-in-the-eu

Estonia Cybersecurity Skills Needs Analysis. (2023). *Estonia cybersecurity skills needs analysis*. https://cyberhubs.eu/wp-content/uploads/2024/10/Estonia_Cybersecurity-skills-needs-analysis-report-1.pdf

Finnish Government. (2024). *Finland's cyber security strategy 2024–2035*. https://julkaisut.valtioneuvosto.fi/server/api/core/bitstreams/e5575ec3-1ce2-4f0a-aaff-50154789cb6d/content

Furnell, S. (2021). The cybersecurity workforce and skills. *Computers & Security, 100*, 102080. https://doi.org/10.1016/j.cose.2020.102080

ISC2. (2024). *ISC2 2024 cybersecurity workforce study*. https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study

Jerman Blažič, B. (2021). The cybersecurity labour shortage in Europe: Moving to a strategic approach. *Technology in Society, 67*, 101769. https://doi.org/10.1016/j.techsoc.2021.101769

Nkongolo, M., Mennega, N., & van Zyl, I. (2023). Cybersecurity career requirements: A literature review. *arXiv*. https://doi.org/10.48550/arXiv.2306.09599

Public Safety Canada. (2025). *National cyber security strategy 2025*. Government of Canada. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2025/index-en.aspx

Security Delta (HSD) & Centre for Security and Digitalisation (CVD). (2023). *Human capital agenda security 2023–2026*. https://securitydelta.nl/media/com_hsd/report/617/document/2023-HSD-rapport-human-capital-final-totaal-interactief-final.pdf

State of the Cyber Security Sector in Ireland. (2022). *State of the cyber security sector in Ireland 2022 (Executive summary)*. https://cyberireland.ie/wp-content/uploads/2022/05/State-of-the-Cyber-Security-Sector-in-Ireland-2022-Executive-Summary.pdf