DOI
https://doi.org/10.18690/um.fvv.10.2024.9

ISBN
978-961-286-912-0

KIBERNETSKA VARNOST IN DIGITALNA VKLJUČENOST SKOZI PRIZMO ZAGOTAVLJANJA DOSTOPA DO INFORMACIJ IN ZAŠČITE TEMELJNIH SVOBOŠČIN

IGOR BERNIK
Univerza v Mariboru, Fakulteta za varnostne vede, Ljubljana, Slovenija
igor.bernik@um.si

V digitalni družbi kibernetska varnost in digitalna vključenost igrata ključno vlogo pri doseganju trajnostnega razvoja in vzpostavljanju vključujočih družb. 16. cilj trajnostnega razvoja Združenih narodov poziva k zagotavljanju javnega dostopa do informacij ter zaščiti temeljnih svoboščin v skladu z nacionalno zakonodajo in mednarodnimi sporazumi. Prispevek obravnava pomen kibernetske varnosti pri zaščiti digitalne infrastrukture, ki je ključna za varno in svobodno dostopanje do informacij. Izpostavlja tudi vlogo digitalne vključenosti pri zmanjševanju digitalnega razkoraka in zagotavljanju enakih možnosti za vse. Predstavljeni so primeri dobrih praks iz držav, ki so uspešno implementirale politike za izboljšanje kibernetske varnosti in digitalne vključenosti, s poudarkom na njihovem prispevku k doseganju 16. cilja Združenih narodov. Prispevek prispeva k razumevanju, kako lahko lokalne in nacionalne pobude sodelujejo za krepitev vključujočih in varnih digitalnih okolij, kot temelja za trajnostni razvoj.

Ključne besede:
kibernetska varnost, digitalna vključenost, trajnostni razvoj, dostop do informacij, temeljne svoboščine

Univerzitetna založba Univerze v Mariboru

DOI
https://doi.org/
10.18690/um.fvv.10.2024.9

ISBN
978-961-286-912-0

Cybersecurity and Digital Inclusion Through the Prism of Ensuring Access to Information and Protection of Fundamental Freedoms

Igor Bernik
University of Maribor, Faculty of Criminal Justice and Security, Ljubljana, Slovenia
igor.bernik@um.si

Keywords:
cybersecurity,
digital inclusion,
sustainable development,
information access,
fundamental freedoms

Cyber security and digital inclusion play a crucial role in achieving sustainable development and building inclusive societies in a digital society. The 16th Sustainable Development Goal of the United Nations calls for providing public access to information and protecting fundamental freedoms following national legislation and international agreements. The paper discusses the importance of cyber security in protecting digital infrastructure, which is the key to secure and free access to information. It also highlights the role of digital inclusion in reducing the digital divide and ensuring equal opportunities for all. Examples of good practices from different countries that have successfully implemented policies to improve cyber security and digital inclusion are presented, emphasising their contribution to the achievement of United Nations Goal 16. The paper contributes to understanding how local and national initiatives can work together to strengthen inclusive and safe digital environments as a foundation for sustainable development.

University of Maribor Press

1 Uvod

Digitalizacija je ključen element sodobnih družb, saj omogoča hiter dostop do informacij in s široko dostopno komunikacijo ustvarja številne nove priložnosti za gospodarski, politični in družbeni razvoj (United Nations, 2015). Kibernetska varnost in digitalna vključenost sta dve pomembni komponenti, ki omogočata varno uporabo digitalnih tehnologij in enakopraven dostop do informacij (Bernik, 2024). Širši vplivi digitalne vključenosti se kažejo v preprečevanju digitalne diskriminacije in omogočanju vključujočih digitalnih okolij. Digitalna vključenost zagotavlja, da imajo vsi prebivalci, ne glede na njihove družbene, ekonomske ali geografske pogoje, enakopraven dostop do digitalnih storitev in informacij. S tem se zmanjšuje digitalni razkorak, ki bi lahko prispeval k družbeni neenakosti in krepi sodelovanje v družbeno-političnih procesih. Preprečevanje digitalne diskriminacije je ključno za zagotavljanje enakih možnosti za vse ter krepitev socialne kohezije in trajnostnega razvoja.

2 Kibernetska varnost kot ključni element trajnostnega razvoja

Kibernetska varnost je proces varovanja informacij in digitalne infrastrukture pred kibernetskimi napadi, kar je bistvenega pomena za ohranjanje zaupanja v digitalno infrastrukturo (von Solms in van Niekerk, 2013). Digitalna infrastruktura, kot so spletne platforme in storitve, omogoča dostop do informacij, ki je ključen za doseganje 16. cilja trajnostnega razvoja Združenih narodov (v nadaljevanju ZN), saj omogoča svobodno izražanje in sodelovanje pri sprejemanju odločitev (Filho idr., 2024). Dostop do informacij je temeljna svoboščina, ki omogoča uresničevanje drugih človekovih pravic in krepi demokratično participacijo. Digitalna vključenost pomeni zagotavljanje dostopa do digitalnih tehnologij in informacij za vse prebivalce, ne glede na spol, starost, socialno-ekonomski status ali geografsko lokacijo (Selwyn, 2004). Pomanjkanje digitalne vključenosti lahko povzroči digitalni razkorak, ki vpliva na družbeno neenakost in omejuje možnosti za izobraževanje, zaposlitev ter politično participacijo (Helsper, 2012). Kibernetska varnost je tesno povezana tudi z enakostjo, saj lahko trajnostni nadzor in ustrezna zaščita zmanjšata tveganja digitalne diskriminacije in neenakosti. Nekaterim državam, kot je Estonija, je uspelo vzpostaviti visoko raven kibernetske varnosti in omogočiti svojim prebivalcem varen dostop do digitalnih storitev, kar krepi digitalno vključenost in povečuje zaupanje v digitalno upravljanje (E-Estonia, n. d.). Krepitev kibernetske

varnosti je pomemben dejavnik pri zagotavljanju varnega digitalnega okolja, kar prispeva k trajnostnemu razvoju. Kibernetska varnost je tesno povezana tudi z enakostjo, saj lahko trajnostni razvoj in ustrezna zaščita zmanjšata tveganja digitalne diskriminacije in neenakosti. Predstavljeni primeri povezujejo kibernetsko varnost, enakost, trajnostni razvoj in digitalno transformacijo:

1. Japonska – Družba 5.0: Koncept Družbe 5.0, ki ga je razvila Japonska, združuje napredne tehnologije, kot so umetna inteligenca in internet stvari (IoT), za izboljšanje kakovosti življenja. Japonska je vlagala v kibernetsko varnost in digitalno vključenost, da bi omogočila enakopraven dostop do digitalnih storitev za vse prebivalce. Ta pristop zagotavlja trajnostni razvoj in krepitev socialne enakosti (Yaraş in Kanatlı-Öztürk, 2022).
2. Estonija – digitalna država: Estonija je ena vodilnih držav na področju digitalne transformacije in kibernetske varnosti. Njena rešitev e-Estonia vključuje široko dostopnost digitalnih storitev za vse državljane, kar spodbuja enakopravnost in digitalno vključenost. Poleg tega zagotavlja visoko raven kibernetske varnosti, kar povečuje zaupanje državljanov v digitalne storitve ter omogoča trajnostni razvoj (E-Estonia, n. d.).
3. Finska – digitalna pismenost kot osnovna pravica: Finska je digitalno pismenost prepoznala kot osnovno pravico. Njihova politika zagotavlja vsem prebivalcem dostop do izobraževanja o digitalnih veščinah, kar prispeva k zmanjševanju digitalnega razkoraka in krepi socialno vključenost. Finska je prav tako poskrbela za varnost digitalnih storitev, kar zagotavlja enakopraven dostop do digitalne infrastrukture za vse (Ministry of Transport and Communications, n. d.).
4. Kanada – vključujoča kibernetska varnost: Kanada je sprejela celovit pristop h kibernetski varnosti, ki vključuje podporo marginaliziranim skupinam. Kanadski načrt za kibernetsko varnost vključuje ukrepe za povečanje dostopnosti digitalnih storitev za vse prebivalce, ne glede na njihov socialno-ekonomski položaj ali geografsko lokacijo. Ta pristop omogoča, da so vse skupine v družbi enakopravno zastopane in zaščitene pred kibernetskimi grožnjami, kar prispeva k trajnostnemu razvoju in digitalni transformaciji (Public Safety Canada, 2018).
5. Slovenija – Digitalna koalicija: Slovenija se je z vzpostavitvijo Digitalne koalicije zavezala k izboljšanju digitalne pismenosti in kibernetske varnosti in vključuje različne deležnike, kot so civilna družba (nevladne organizacije, lokalne skupnosti, sindikati, socialna združenja), državni in javni sektor (ministrstva, javna uprava, vlada, agencije), raziskovalno-razvojni sektor (univerze, centri,

inštituti) ter gospodarstvo (zbornice, zagonska podjetja, digitalni ponudniki, industrije). Vloga teh deležnikov je sooblikovanje in usmerjanje digitalizacije, usklajevanje strategij in konceptov ter iskanje sinergij med različnimi akterji, kar omogoča učinkovito digitalno transformacijo in krepi vključenost v digitalni družbi (Digitalna Slovenija, n. d.). S tem omogoča enakopraven dostop do digitalnih storitev in prispeva k zmanjševanju digitalnega razkoraka. Slovenija dejavno spodbuja digitalno vključenost in zagotavlja podporo pri uporabi digitalnih storitev, kar prispeva k trajnostnemu razvoju.

Predstavljeni primeri kažejo, kako kibernetska varnost in digitalna vključenost omogočata trajnostni razvoj in digitalno transformacijo. Estonija je s svojo digitalno državo pokazala, kako lahko kibernetska varnost krepi zaupanje državljanov v digitalne storitve, kar omogoča enakopraven dostop do informacij in storitev. Finska je z obravnavo digitalne pismenosti kot osnovne pravice zmanjšala digitalni razkorak in omogočila trajnostni razvoj ter socialno vključenost. Slovenija je z Digitalno koalicijo pokazala, kako lahko nacionalne pobude zagotovijo enakopraven dostop do digitalnih storitev in izboljšajo digitalno pismenost, kar prispeva k trajnostnemu razvoju. Japonska, s konceptom Družbe 5.0, povezuje napredne tehnologije, kibernetsko varnost in digitalno vključenost, kar omogoča trajnostni razvoj in krepitev socialne enakosti. Kanada pa je s svojim vključujočim pristopom h kibernetski varnosti zagotovila dostopnost digitalnih storitev za vse, ne glede na njihov socialno-ekonomski položaj, kar spodbuja digitalno transformacijo in trajnostni razvoj.

Dostop do informacij je torej ključen za zagotavljanje temeljnih svoboščin in zmanjševanje neenakosti v družbi. Digitalna vključenost in enakost prispevata tudi k večji vključenosti marginaliziranih skupin, s čimer se krepi družbena kohezija in omogoča trajnostni razvoj, obenem pa zmanjšuje razkorak med različnimi (etničnimi, starostnimi, ekonomskimi) skupinami.

3 Digitalni prehod za prehod v Družbo 5.0

Družba 5.0 skozi koncept, ki ga je razvila Japonska in predstavlja vizijo prihodnosti, v kateri tehnologija in digitalizacija prispevata k boljši kakovosti življenja in reševanju družbenih izzivov (Yaraş in Kanatlı-Öztürk, 2022), omogoča digitalni prehod in je ključnega pomena za integracijo naprednih tehnologij, kot so umetna inteligenca,

IoT in podatkovna analitika, za reševanje problemov na različnih področjih, kot so npr. zdravstvo, izobraževanje in javna uprava.

Pri tem sta digitalna vključenost in kibernetska varnost ključna elementa tudi za uspešen prehod v Družbo 5.0. Dostop do informacij kot temeljna svoboščina omogoča enakopraven dostop do digitalnih tehnologij in storitev, to pa prispeva k večji družbeni enakosti in vključevanju vseh prebivalcev v digitalno gospodarstvo. Primer Japonske kaže, da se da z vlaganjem v digitalno infrastrukturo in zagotavljanjem visoke ravni kibernetske varnosti postati vodilen pri implementaciji koncepta Družbe 5.0 (Cabinet Office, n. d.). S tem pristopom pa se približujemo dosegu 16. cilja razvoja ZN. Ker že imamo uspešne implementacije in znanje, le to lahko prenesemo tudi na druge države. Primeri dobrih praks na področju kibernetske varnosti in digitalne vključenosti iz različnih držav kažejo, kako lahko lokalne in nacionalne politike prispevajo k trajnostnemu razvoju. Večkrat omenjeni Estoniji kot vodilni državi na področju digitalizacije je uspelo vzpostaviti varen in dostopen digitalni ekosistem, ki omogoča prebivalcem varno uporabo digitalnih storitev. Podoben primer je tudi Južna Koreja, ki je investirala v digitalno infrastrukturo in izobraževanje, da bi zagotovila visoko raven digitalne pismenosti in vključenosti (Norqvist, 2023).

Opisani pristopi prispevajo k doseganju 16. cilja ZN, saj omogočajo javni dostop do informacij ter zaščito temeljnih svoboščin. Digitalna vključenost omogoča večje sodelovanje prebivalcev v družbeno-političnih procesih, kar krepi demokracijo in spodbuja trajnostni razvoj. Primeri, kot sta Japonska in Estonija, kažejo, da je možno ustvariti vključujoča in varna digitalna okolja, ki prispevajo k Družbi 5.0 in trajnostnemu razvoju.

4 Razprava in zaključek

Kibernetska varnost in digitalna vključenost sta medsebojno povezani komponenti, ki prispevata k trajnostnemu razvoju. Medtem ko kibernetska varnost zagotavlja varno okolje za uporabo digitalnih storitev, digitalna vključenost omogoča enakopraven dostop do teh storitev za vse. Skupaj ustvarjata pogoje za družbeno enakost, demokratično participacijo in trajnostni razvoj. Zato poudarjamo pomen sodelovanja med lokalnimi in nacionalnimi akterji pri vzpostavljanju vključujočih in varnih digitalnih okolij. Sodelovanje med državnimi institucijami, zasebnim

sektorjem in civilno družbo je ključno za uspešno implementacijo politik, ki spodbujajo kibernetsko varnost in digitalno vključenost. Prehod v Družbo 5.0 zahteva usklajeno delovanje vseh akterjev, da se zagotovi dostop do informacij kot temeljne svoboščine ter varno in vključujoče digitalno okolje.

Doseganje digitalnih pravic in kibernetske varnosti za Slovenijo pomeni, da imajo prebivalci pravico do varnega in enakopravnega dostopa do interneta ter digitalnih storitev. Tako so osebni podatki zaščiteni, komunikacija varna, vsi prebivalci – ne glede na starost, kraj bivanja ali socialni status – pa uporabljajo tehnologijo brez strahu pred zlorabo ali napadi. Konkretno se soočamo z grožnjami, kot so kraje identitete, vdori v osebne podatke, dezinformacije ter druge kibernetske grožnje, ki lahko vplivajo na vsakodnevno življenje in poslovanje.

Pozitivne rešitve za omenjene izzive temeljijo na znanju in veščinah, ki jih prebivalci, učitelji, lokalni voditelji in drugi akterji pridobijo skozi izobraževanje in usposabljanje o varni uporabi tehnologije in prepoznavanju tveganj. To vodi v zmanjšanje digitalnega razkoraka, večjo varnost prebivalcev, zaupanje v digitalne storitve, ter povečanje vključevanja prebivalcev v digitalno družbo. Negativni izidi, če ukrepi niso ustrezni, pa so povečanje ranljivosti na kibernetske napade, neenak dostop do tehnologije za posamezna skupine ter posledično poglobitev družbenih neenakosti.

Za zagotavljanje digitalnih pravic in kibernetske varnosti mora država in lokalne oblasti zagotoviti več programov usposabljanja o varni uporabi interneta, ter vzpostaviti mehanizme pomoči, kot so na primer centri za pomoč žrtvam kibernetskih napadov. Nekatere rešitve, na primer vzpostavitev nacionalne Digitalne koalicije, ki spodbuja digitalno pismenost in zagotavlja orodja za izboljšanje varnosti, so že v izvajanju. Rešitve, ki se jih v posameznih primerih že poslužujemo, gredo v smer vzpostavitev dostopnih digitalnih točk, prost dostop do interneta, kot tudi postavitev terminalov za opravljanje storitev, zlasti v območjih, kjer prebivajo marginalizirane skupine. Pomembna je tudi izvedba programov izobraževanj in usposabljanj z organizacijo delavnic in izobraževalnih programov za različne skupine, s poudarkom na osnovni digitalni pismenosti in kibernetski varnosti. Posebna pozornost naj bo namenjena ranljivejšim skupinam. Zelo koristni je tesno sodelovanje z nevladnimi organizacijami, ki že delujejo znotraj različnih skupnosti ali marginaliziranih skupin, da se zagotovi, da so digitalne storitve in programi prilagojeni specifičnim potrebam. V to kategorijo sodi izvedba izobraževanj ali

izvajanja storitev v jezikih, ki jih prebivalci razumejo. Vključevanje predstavnikov različnih lokalnih skupnosti v posvetovalna telesa pri načrtovanju digitalnih politik pa zagotovi, da so posamezne potrebe ustrezno naslovljene in upoštevane.

Predlagani in drugi ukrepi lahko izboljšajo digitalno vključenost vseh prebivalcev, zmanjšajo digitalni razkorak ter povečajo zaupanje v uporabo digitalnih storitev. Možni pozitivni izidi teh ukrepov so boljša integracija različnih skupnosti, boljše možnosti za izobraževanje in zaposlitev ter večje sodelovanje prebivalcev pri družbeno-političnih vprašanjih. Negativni izidi pa lahko nastanejo, če pri izvedbi ukrepov ne namenimo zadostnih sredstev ali če bi prebivalci, katerim so programi namenjeni, ne pokažejo interesa ali zaupanja.

Tako bo nadaljnje delo in raziskovanje usmerjeno v iskanje načinov za izboljšanje digitalne pismenosti in vključenosti, kar bo privedlo do večje odpornosti družbe na kibernetske grožnje ter zmanjšanje digitalnega razkoraka. Ključno je tudi preučevanje sodelovanja med državnimi institucijami, zasebnim sektorjem in civilno družbo za vzpostavitev celovitih in trajnostnih strategij za zaščito digitalnih pravic in zagotavljanje varnih digitalnih okolij za vse prebivalce.

Viri in literatura

Bernik, I. (2024). *Kibernetski prostor in kibernetska varnost v luči trajnostnega razvoja: Sinergija lokalnih skupnosti v družbi 5.0*. V G. Meško in K. Eman (ur.), *Varnost v lokalnih skupnostih – multidisciplinarne perspektive* (str. 313–338). Univerza v Mariboru, Univerzitetna založba; Univerza v Mariboru, Fakulteta za varnostne vede. doi:10.18690/um.fvv.6.2024.14

Cabinet Office. (n. d.). *Society 5.0*. https://www8.cao.go.jp/cstp/english/society5_0/index.html

Digitalna Slovenija. (n. d.). *Digitalna koalicija*. https://www.digitalna.si/digitalna-koalicija

E-Estonia. (n. d.). e-*Estonia story*. https://e-estonia.com/story/

Filho, W. L., Kautish, S., Wall, T., Rewhorn, S. in Paul, S. K. (2024). *Digital technologies to implement the UN sustainable development goals: Opportunities and challenges*. Springer.

Helsper, E. J. (2012). A corresponding fields model for the links between social and digital exclusion. *Communication Theory, 22*(4), 403–426. doi:10.1111/j.1468-2885.2012.01416.x

Ministry of Transport and Communications. (n. d.). *Areas of expertice*. https://lvm.fi/en/areas-of-expertise

Norqvist, L. (2023). *Analysis of the digital transformation of society: Its impact on young people's lives*. European Union, Council of Europe. https://pjp-eu.coe.int/documents/42128013/47262517/Analysis+of+the+Digital+Transformation+of+Society+its+Impact+on+Young+People+Lives+-+Lars+Norqvist.pdf/efaff33a-89bc-3947-b618-01160e693872

Public Safety Canada. (2018). *National cyber security strategy*. Her Majesty the Queen in Right of Canada. https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf

Selwyn, N. (2004). Reconsidering political and popular understandings of the digital divide. *New Media & Society, 6*(3), 341–362. doi:10.1177/1461444804042519

United Nations. (2015). *Transforming our world: the 2030 agenda for sustainable development*. https://sdgs.un.org/2030agenda

Von Solms, R. V. in van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38,* 97–102. doi:10.1016/j.cose.2013.04.004

Yaraş, Z. in Kanatlı-Öztürk, F. (2022). Society 5.0 in human technology integration: digital transformation in educational organizations. *International Journal of Progressive Education, 18*(1), 458–474. doi:10.29329/ijpe.2022.426.26