DOI
https://doi.org/
10.18690/um.fvv.8.2023.15

ISBN
978-961-286-792-8

VARNOST UPORABE KIBERNETSKEGA PROSTORA IN VLOGA DRUŽBENEGA NADZORSTVA V RURALNEM OKOLJU V DOBI UMETNE INTELIGENCE

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

Zaradi hitrega razvoja tehnologije, še posebej na področju umetne inteligence in kibernetskega prostora ter prehoda v Družbo 5.0 se v vsakdanjik prenašajo inovacije kot tudi novi izzivi, ki se nanašajo na varnost uporabe kibernetskega prostora. Varnost uporabe kibernetskega prostora v ruralnem okolju je ključnega pomena za zagotavljanje zasebnosti, zaščito osebnih podatkov in ohranjanje integritete teh območij. S prihodom umetne inteligence so se pojavili novi izzivi in dileme, ki zahtevajo skrbno raziskovanje, ozaveščanje in ustrezne ukrepe za zagotavljanje kibernetske varnosti v ruralnem okolju. Poleg tega je treba posebno pozornost nameniti tudi družbenemu nadzoru, saj ima lahko pomemben vpliv na ruralne skupnosti. Etika in izzivi družbenega nadzora v ruralnem okolju morajo biti temeljno upoštevani pri razvoju in implementaciji kibernetskih rešitev. Z izobraževanjem uporabnikov, uporabo tehnoloških ukrepov, vzpostavitvijo ustrezne zakonodaje in odgovornim družbenim nadzorom lahko dosežemo varnejšo uporabo kibernetskega prostora v ruralnih okoljih tudi v dobi generativne umetne inteligence.

Ključne besede:
uporabniki,
varnost,
družbeni nadzor,
kibernetski prostor,
umetna inteligenca

Univerzitetna založba
Univerze v Mariboru

DOI
https://doi.org/
10.18690/um.fvv.8.2023.15

ISBN
978-961-286-792-8

Cyber Space Usage Security and the Role of Social Surveillance in Rural Environment in the Era of Artificial Intelligence

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

Keywords:
users,
security,
social surveillance,
cyberspace,
artificial intelligence

Due to the rapid advancement of technology, particularly in the field of Artificial Intelligence and cyberspace, and the transition to Society 5.0, innovations and new challenges of security of cyberspace usage are becoming a part of our lives. Ensuring the security of cyberspace usage in rural environments is paramount for preserving privacy, safeguarding personal data, and maintaining the integrity of these areas. Artificial intelligence has brought new challenges and dilemmas requiring careful research, awareness, and appropriate measures to ensure cyber security in rural environments. Special attention must be given to social surveillance, as it can significantly impact rural communities. The ethics and challenges of social surveillance in rural environments should be considered in developing and implementing cyber solutions. By educating users, employing technological measures, establishing appropriate legislation, and practising responsible social surveillance, we can achieve safer cyberspace usage in rural environments, even in the era of generative artificial intelligence.

University of Maribor Press

1 Pomen kibernetske varnosti v ruralnih okoljih

Kibernetska varnost je postala ključno vprašanje v današnjem digitalnem svetu, vendar se njen pomen in izzivi razlikujejo med različnimi geografskimi in infrastrukturnimi okolji. Ruralna območja, z razlikami v infrastrukturi, povezljivosti in dostopnosti do interneta, se soočajo s svojimi specifičnimi izzivi in potrebami. Ruralna in urbana infrastruktura se v Sloveniji bistveno ne razlikujeta glede na razpoložljivost tehnoloških sredstev (Bernik, 2022). V splošnem so urbana območja običajno bolj razvita in omogočajo več različnih priklopov na telekomunikacijsko in internetno infrastrukturo, ki omogoča hitro in zanesljivo povezljivost. V nasprotju s tem so ruralna območja pogosto slabše opremljena s širokopasovnim internetom in tehnološkimi zmogljivostmi (Ayo-Obiremi in Omowale, 2020), zato so načini priklopov in izbira med ponudniki manjši. Dostop do interneta v ruralnih okoljih predstavlja ključni izziv. Številne študije so dokumentirale, da so ruralna območja podvržena počasnejši internetni povezljivosti in večjim izpadom omrežja v primerjavi z urbano infrastrukturo (Divyashree in Rangaraju, 2018). Slaba povezljivost omejuje dostop do spletnih storitev, kar lahko negativno vpliva na gospodarstvo in kakovost življenja v ruralnih skupnostih. Vendar ugotavljamo, da je večini prebivalstva Slovenije priklop na širokopasovni internet omogočen (Bernik, 2022), zato povezljivost ne omejuje rabe storitev.

Kibernetska varnost v ruralnih okoljih se sooča s specifičnimi izzivi. Hitra internetna povezljivost povečuje ranljivost za kibernetske napade (Hambly in Rajabiun, 2021). Pomanjkanje izobraževanja in ozaveščenosti o kibernetski varnosti v teh skupnostih prav tako prispeva k tveganjem. Obenem pa se je med storitve interneta v tem letu vmešala še relativno široka raba generativne umetne inteligence (v nadaljevanju UI). S širšo rabo odpira nove priložnosti uporabnikom, obenem pa pomaga zagotavljati določene varnostne mehanizme. Tako ima UI potencial za izboljšanje kibernetske varnosti in obrambe pred nevarnostmi s spleta, lahko pomaga pri prepoznavanju nenavadnih vzorcev v omrežnem prometu in napovedovanju morebitnih napadov (Ahmed idr., 2016). Poleg tega omogoča avtomatizacijo odzivov na napade, kar lahko zmanjša časovno okno za odzivanje na grožnje. Tako se UI uporablja za različne naloge v kibernetskem prostoru, vključno z analizo logov, zaznavanjem vdorov, upravljanjem groženj in avtomatizacijo varnostnih procesov (Ramotsoela idr., 2018). UI lahko s svojo sposobnostjo samoučenja in prilagajanja pomaga prepoznati nove in kompleksne grožnje ter pripomore k izboljšanju

kibernetske varnosti, ne glede na omejitve infrastrukture. Avtomatizacija in hitra odzivnost UI lahko pomagata zaščititi ranljive skupnosti pred grožnjami, ki bi lahko resno ogrozile njihovo infrastrukturo in podatke.

Kljub mnogim prednostim obstajajo tudi potencialne nevarnosti pri uporabi UI. Pomanjkanje izkušenj in virov za implementacijo ter vzdrževanje sistemov UI povečuje tveganje za napake in nepravilnosti. Potencialne nevarnosti pri uporabi UI razdelimo na področja:

- Pomanjkanje izkušenj uporabnikov in dostopnost virov: Ruralna okolja pogosto nimajo enakega dostopa do tehničnih strokovnjakov ali virov za implementacijo in vzdrževanje sistemov kot urbana okolja. To pomanjkanje izkušenj in sredstev lahko poveča tveganje za napake in nepravilnosti pri uporabi UI. Brez ustreznega znanja in podpore obstaja nevarnost, da sistemi UI ne bodo delovali pravilno ali bodo ranljivi za napade.
- Varstvo podatkov: Uporaba UI vključuje zbiranje in obdelavo velikih količin podatkov. V ruralnih okoljih obstaja večja možnost pomanjkanja ozaveščenosti o varstvu podatkov in zasebnosti, kar lahko vodi do neprimernega ravnanja z osebnimi podatki prebivalcev, kar posledično škoduje njihovi zasebnosti.
- Dostopnost in upravljanje tehnologije: Okolja se soočajo z izzivi glede dostopnosti do napredne tehnologije in interneta. Če sistemi UI niso ustrezno prilagojeni tem omejitvam, se lahko ustvari digitalna vrzel, ki omejuje koristi UI za prebivalstvo.

Menimo, da je pri rabi vseh oblik UI pomembno upoštevati etična vprašanja, povezana z zasebnostjo podatkov in avtonomijo. Če izpostavimo najpomembnejše:

- Zasebnost podatkov: Zbiranje in uporaba osebnih podatkov prebivalcev za namene UI morata biti izvedena z visokimi standardi varstva zasebnosti. Prebivalci imajo pravico do nadzora nad svojimi podatki, zato je ključno zagotoviti, da se podatki na noben način ne zlorabljajo.
- Avtonomija in etično odločanje: Uporaba UI lahko vključuje avtonomne sisteme, kot so avtonomna vozila, avtonomni sistemi za zagotavljanje (kibernetske) varnosti ali odločitveni algoritmi. Prebivalci morajo imeti

možnost, da sodelujejo pri oblikovanju sistemov in da razumejo, kako delujejo. Pomembno je, da se prepreči vsiljevanje avtonomnih odločitev, ki bi lahko negativno vplivale na skupnost.

- V skladu z načeli etične rabe UI je ključno, da se sistemi UI v ruralnih okoljih razvijajo in uporabljajo na način, ki spoštuje človekove pravice, vključno s pravico do zasebnosti in avtonomije. Prav tako je treba zagotoviti izobraževanje in ozaveščenost o teh vprašanjih, da se zmanjšajo tveganja in izboljša uporaba UI za dobrobit skupnosti.

Kibernetska varnost je v ruralnih okoljih enako pomembna kot v urbanih. Razlike v infrastrukturi, dostopnosti do interneta in izobraževanju ustvarjajo specifične izzive, ki jih je treba nasloviti. UI lahko igra ključno vlogo pri izboljšanju varnosti v skupnosti, vendar je treba hkrati obravnavati njene potencialne nevarnosti. Vključevanje strokovnjakov za kibernetsko varnost, izobraževanje in razvoj ustrezne infrastrukture so ključni koraki v zagotavljanju kibernetske varnosti v ruralnih okoljih. Ker postaja z razvojem tehnologije, zlasti UI, varovanje zasebnosti in osebnih podatkov vse bolj pomembno, se v nadaljevanju osredotočamo na pomen zasebnosti v dobi UI ter obravnavo zbiranja, obdelave in zaščite osebnih podatkov v ruralnem okolju.

2 Varovanje zasebnosti in osebnih podatkov v dobi umetne inteligence

Zasebnost, kot temeljna človekova pravica, ima v dobi UI še večji pomen. UI uporablja napredne algoritme za obdelavo ogromnih količin podatkov, kar lahko privede do zlorab, vohunjenja in neželenega dostopa do osebnih informacij. Varovanje zasebnosti postaja ključno, saj posamezniki potrebujejo nadzor nad tem, kako se njihovi osebni podatki zbirajo, hranijo in uporabljajo (Clarke, 2019). Osebni podatki se zbirajo in obdelujejo na različne načine, kar vključuje zbiranje informacij o prebivalcih, njihovih nakupih, zdravstvenem stanju in druge osebne podatke. Prebivalci pogosto nimajo ustrezne ravni ozaveščenosti o zasebnosti in varnosti podatkov, kar je še bolj značilno za ruralna kot urbana okolja. Posamezniki na ruralnih območjih morda niso seznanjeni s svojimi pravicami ali tveganji, povezanimi z zbiranjem osebnih podatkov (Martin in Murphy, 2017) ali pa jim preprosto ni mar. To pa povečuje potrebo po pravilni zaščiti zasebnosti. Tako moramo za zagotovitev zaščite zasebnosti in osebnih podatkov uporabnikov, tudi v ruralnem okolju, izvajati smernice o zbiranju podatkov. Izdelati in uveljaviti je treba

jasne smernice o tem, kako se smejo zbirati in obdelovati osebni podatki. Posamezniki bi morali biti obveščeni o tem, kateri podatki se zbirajo in za kakšen namen. V Sloveniji za področje varovanja osebnih podatkov, tudi skladno z Uredbo o varstvu osebnih podatkov, skrbi Informacijski pooblaščenec, je pa potrebna stalna skrb zagotavljanja visoke stopnje varovanja osebnih podatkov. Varnostne tehnologije in njihova uporaba, kot so šifriranje podatkov, požarni zidovi in varnostne posodobitve, so ključne za zaščito osebnih podatkov. Tudi ruralna okolja bi morala investirati v tehnologije, ki zagotavljajo varno hranjenje in prenos podatkov (Ahmed idr., 2016). Tovrstna infrastruktura je v urbanih okoljih na voljo in široko dosegljiva.

2.1 Družbeni nadzor v času kibernetske povezljivosti

Družbeni nadzor se kot pojem nanaša na sistem nadzora, spremljanja in regulacije družbenih dejavnosti, vključno z uporabo tehnologije in UI za sledenje, analizo in obvladovanje različnih vidikov človekovega življenja. V kontekstu ruralnih okolij ima lahko družbeni nadzor poseben vpliv. V dobi UI je družbeni nadzor postal še bolj sofisticiran in razširjen, saj UI omogoča avtomatizirano zbiranje in analizo podatkov na različnih ravneh (Lyon, 2018). To vključuje analizo družbenih omrežij, obnašanja na spletu in celo uporabo naprednih algoritmov za prepoznavanje obrazov, hoje, govora in podobno. Zato je vpliv družbenega nadzora kompleksen. Po eni strani lahko družbeni nadzor prispeva k večji varnosti in boljšemu upravljanju v skupnostih. Na primer, tehnologija za nadzor prometa lahko pripomore k večji varnosti. Po drugi strani pa pretirana uporaba tehnologije za nadzor lahko vodi v nadzor zasebnosti in svobode prebivalcev. Pri tem je treba opozoriti, da so ruralna okolja pogosto manj seznanjena s posledicami družbenega nadzora, s tem pa se pojavi nevarnost nadzornih praks, ki niso v skladu z etičnimi načeli.

Pri zagotavljanju etičnosti in še sprejemljive ravni družbenega nadzora se soočamo z etičnimi izzivi, ki vključujejo:

- Zasebnost; osebni podatki prebivalcev ruralnih okolij se morajo ustrezno varovati in nikakor zlorabljati. Skladnost z zakonodajo je izhodišče, (najvišji) etični standardi pa cilj.

- (Digitalna) diskriminacija: preprečiti je treba, da bi algoritmi za družbeni nadzor v ruralnih okoljih prispevali k diskriminaciji, na primer pri razporejanju virov ali storitev.
- Transparentnost in odgovornost: transparentnost in odgovornost pri uporabi družbenega nadzora je nujna. Zagotoviti je treba, da prebivalci razumejo, kako se podatki zbirajo in zakaj se uporabljajo.

Vprašanja etike in pravičnosti so ključna pri razmišljanju o učinkih družbenega nadzora v ruralnih okoljih. Ruralna skupnost se mora zavedati teh izzivov in sodelovati pri oblikovanju pravil in smernic, ki bodo zagotavljale uravnotežen in etičen družbeni nadzor v dobi UI.

Na izpostavljene dileme moramo odgovoriti pri razvoju družbe in prehodu skupnosti v Družbo 5.0. Tako bomo zagotovili digitalno pravičnost, preprečili digitalno diskriminacijo in dejansko zagotovili vse vključujočo družbo z boljšim življenjem za vse. S tem bomo sledili tudi agendi Združenih narodov, strategijam razvoja Evropske unije in Republike Slovenije ter zagotavljali dolgoročno vzdržno in prijazno družbo za prebivalce.

2.2 Ukrepi za zagotavljanje varnosti

V kibernetskem prostoru je zagotavljanje varnosti pomembno kot v urbanem okolju, vendar so potrebni posebni ukrepi za naslavljanje specifičnih izzivov. Eden najpomembnejših ukrepov za zagotavljanje kibernetske varnosti v ruralnih okoljih je izobraževanje uporabnikov. Študije kažejo, da je ozaveščenost in znanje uporabnikov ključno za preprečevanje kibernetskih napadov (Shillair idr, 2022). Ruralna skupnost bi se morala osredotočiti na osnovne koncepte kibernetske varnosti, prepoznavanje groženj in ukrepanje v primeru napadov. Organizacije in lokalne skupnosti bi morale nuditi izobraževalne programe in kampanje za dvig ozaveščenosti o kibernetskih tveganjih.

Poleg izobraževanja je ključno implementirati tehnične varnostne ukrepe za zaščito kibernetskega prostora. To vključuje vzpostavitev učinkovitih požarnih zidov, protivirusne programske opreme in varnostnih posodobitev (Ahmed idr., 2016). Prav tako je pomembno redno izvajati varnostne preglede in analize, da bi odkrili morebitne šibke točke v sistemu. Vse to pa izhaja iz smernic osnovnega

izobraževanja oziroma, kot pogosto navajamo, higiene na področju kibernetske varnosti.

Za zagotavljanje kibernetske varnosti je potreben jasen pravni okvir, ki mora določiti tudi sankcije za kršitelje varnostnih predpisov. Lokalne skupnosti bi morale tesno sodelovati pri oblikovanju in izvajanju pravnih okvirov, da bi bili prilagojeni (tudi) potrebam ruralnega okolja. S pravilno izobraženimi uporabniki, ustreznimi tehničnimi ukrepi ter jasnim pravnim okvirom se lahko ruralna skupnost zaščiti pred kibernetskimi grožnjami in zagotovi varna uporaba kibernetskega prostora.

Predlagani osnovni koraki za višjo stopnjo kibernetske varnosti so:

- Ozaveščanje prebivalstva: V nekaterih ruralnih skupnostih so organizirani projekti ozaveščanja o kibernetski varnosti. Vključujejo izobraževalne delavnice, predavanja in razširjanje informativnih materialov, s čimer se povečuje ozaveščenost prebivalcev o varnostnih tveganjih (Singer idr., 2020), z mreženjem na dogodkih pa se doseže samopomoč med lokalnim prebivalstvom.
- Sodelovanje z lokalnimi ponudniki internetnih storitev zagotavlja boljšo varnostno infrastrukturo in storitve za ruralna območja (Ahmed idr., 2016). To npr. vključuje vzpostavitev sistemov zaznave groženj, opozarjanje uporabnikov in varnostno usposabljanje.
- Uporaba tehnologije za zajemanje podatkov, ki pomaga prepoznati nenavadne dejavnosti in potencialne napade na kibernetsko infrastrukturo (Ayo-Obiremi in Omowale, 2020). To lahko vključuje uporabo senzorjev in pametnih naprav za zgodnje opozarjanje.

Primeri dobrih praks in priporočila za izboljšanje kibernetske varnosti so ključni za zaščito skupnosti pred kibernetskimi tveganji. S pravilnim in ustreznim izobraževanjem, sodelovanjem in uporabo varnostnih orodij lahko ruralna okolja in vključujoči posamezniki izboljšajo odpornost na kibernetske grožnje in zavarujejo podatke.

3 Zaključki

V dobi UI, kjer se kibernetska varnost in zagotavljanje podatkovne zasebnosti soočata s številnimi izzivi, je raziskovanje vloge kibernetske varnosti v ruralnih okoljih ključno za znanost, stroko in javnost. Proučevanje prispeva k razumevanju specifičnih izzivov, s katerimi se soočajo ruralne skupnosti, ter oblikovanju smernic za izboljšanje varnosti.

Za znanost je to področje pomembno, saj poudarja potrebo po prilagodljivih in dostopnih rešitvah za kibernetsko varnost, ki so prilagojene ruralnim okoljem. S poglobljenimi analizami in študijami želimo identificirati ključna tveganja, razviti tehnološke rešitve ter oblikovati smernice za izobraževanje in ozaveščanje prebivalcev. Prispevek k znanosti je tudi prepoznavanje izzivov, s katerimi se soočajo ruralna območja pri vzpostavljanju kibernetske infrastrukture in iskanju trajnostnih rešitev. Za stroko ta področja pomenijo izhodišče za razvoj praktičnih smernic in varnostnih protokolov, ki so prilagojeni ruralnemu okolju. Razvoj tehničnih rešitev, izobraževalnih programov in sodelovanje z lokalnimi oblastmi postajajo nujni za izboljšanje kibernetske varnosti. Poleg tega lahko stroka pomaga pri vzpostavitvi standardov in smernic za učinkovito družbeno nadzorstvo ter zagotavljanje skladnosti s pravnimi okviri. Javnost je treba ozaveščati o pomenu kibernetske varnosti, zavedati se mora kibernetskih tveganj in ukrepov za zaščito podatkov. Pomembno je, da javnost razume vlogo lokalnih oblasti, organizacij in posameznikov pri zagotavljanju in izboljšanju varnosti.

Koraki za nadaljnje proučevanje predstavljenega področja vključujejo raziskave o specifičnih potrebah in izzivih ruralnih okolij, razvoj in testiranje inovativnih tehnoloških rešitev ter izvajanje študij o učinkovitosti izobraževalnih programov in družbenega nadzorstva. Nenehno je treba spremljati in po potrebi prilagajati pravne okvire, da ustrezajo spreminjajočim se potrebam kibernetske varnosti. S sodelovanjem znanosti, stroke in lokalnih skupnosti lahko dosežemo boljšo kibernetsko varnost ter prispevamo k splošni ozaveščenosti o predstavljenih temah.

Literatura

Ahmed, M., Mahmood, A. N. in Hu, J. (2016). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications, 60*(1), 19–31. doi:10.1016/j.jnca.2015.11.016

Ayo-Obiremi, I. in Omowale, A. (2020). Internet and changing audience role in news processes. *Research Journal of Mass Communication and Information Technology*, *6*(1), 24–36. https://www.iiardjournals.org/get/RJMCIT/VOL.%206%20NO.%201%202020/Internet%20and%20Changing%20Audience.pdf

Bernik, I. (2022). Trajnostni razvoj in zmanjševanje neenakosti dostopa do kibernetskega prostora v Sloveniji: uporabniki na podeželju in mestih. V G. Meško in I. Kokoravec (ur.), *8. Nacionalna konferenca o varnosti v lokalnih skupnostih: cilji trajnostnega razvoja in varnost v lokalnih skupnostih* (str. 179–190). Univerza v Mariboru, Univerzitetna založba.

Clarke, R. (2019). Introduction to dataveillance and information privacy, and definitions of terms. V E. Clarke in M. R. Wigan (ur.), *You are what you surf: The actions of users exposed by do not track and related privacy efforts* (str. 1–28). Springer.

Divyashree, M. in Rangaraju, H. G. (2018). Internet of things (IoT): A survey. *2018 International Conference on Networking, Embedded and Wireless Systems (ICNEWS)* (str. 1-6). Bangalore. doi:10.1109/ICNEWS.2018.8903919

Hambly, H. in Rajabiun, R. (2021). Rural broadband: Gaps, maps, and challenges. *Telematics and Informatics*, *60*, 101565. doi:10.1016/j.tele.2021.101565

Lyon, D. (2018). *The culture of surveillance: Watching as a way of life*. John Wiley & Sons.

Martin, A. in Murphy, E. (2017). *Data protection law in Ireland: Sources and issues*. Round Hall.

Ramotsoela, D., Abu-Mahfouz, A. in Hancke, G. (2018). A survey of anomaly detection in industrial wireless sensor networks with critical water system infrastructure as a case study. *Sensors, 18*(8), 2491. doi:10.3390/s18082491

Shillair, R., Esteve-González, P., Dutton, W. H., Creese, S., Nagyfejeo, E. in von Solms, B. (2022). Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. *Computers & Security*, 119, 102756. doi:10.1016/j.cose.2022.102756

Singer, N., Perlroth, N. in Shane, S. (2020). Suspected Russian hack of U.S. Government said to have gone undetected for months. *The New York Times*. https://www.nytimes.com/2020/12/13/us/politics/russia-hack-nsa-homeland-security-pentagon.html