KIBERNETSKI PROSTOR IN KIBERNETSKA VARNOST V LUČI TRAJNOSTNEGA RAZVOJA: SINERGIJA LOKALNIH SKUPNOSTI V DRUŽBI 5.0

IGOR BERNIK

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

V času digitalne in zelene preobrazbe se lokalne skupnosti soočajo s prepletanjem kibernetske varnosti in trajnostnega razvoja. Pri prehodu v Družbo 5.0 stremimo k harmonični integraciji tehnologij v vsakdanje življenje. Ključnega pomena so strategije varne uporabe kibernetskega prostora ter vloga kibernetskega prostora in njegov vpliv na vsakdanje življenje. Pomemben del trajnostnega razvoja je digitalna enakost kot temelj za oblikovanje odpornega, vključujočega in trajnostno naravnanega kibernetskega okolja za prehod v Družbo 5.0. Izpostavljamo pomen enakopravnega dostopa do kibernetskega prostora ter uporabe kibernetskega prostora za krepitev vezi skupnosti, ob tem pa upoštevamo vplive realnega okolja. Vsebina se prepleta s cilji trajnostnega razvoja Organizacije združenih narodov, ki se usmerjajo proti zmanjševanju neenakosti in spodbujanju trajnostnega razvoja. Prikazano je, kako lahko sodobne tehnologije in storitve kibernetskega prostora, skupaj z varnostnimi politikami v kibernetskem prostoru podpirajo zeleni prehod in digitalno preobrazbo, hkrati pa ohranjajo lokalno identiteto in spodbujajo globalno sodelovanje za doseganje globalnih razvojnih ciljev.

DOI
https://doi.org/10.18690/um.fvv.6.2024.14

ISBN
978-961-286-875-8

Ključne besede:
lokalne skupnosti,
kibernetska varnost,
trajnostni razvoj,
digitalna enakost,
Družba 5.0

Univerzitetna založba Univerze v Mariboru

DOI
https://doi.org/
10.18690/um.fvv.6.2024.14

ISBN
978-961-286-875-8

Cyberspace and Cybersecurity in the Light of Sustainable Development: Synergy of Local Communities in Society 5.0

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

Keywords:
local communities,
cybersecurity,
sustainable development,
digital equality,
Society 5.0

During the digital and green transformation era, local communities face the intertwining challenges of cybersecurity and sustainable development. It is crucial to develop strategies for securing cyberspace and recognising its impact on daily life. An aspect of sustainable development is digital equality, the foundation for creating a resilient, inclusive, and sustainably oriented cyber environment for the transition to Society 5.0. The importance of equal access to cyberspace and its use to strengthen the bonds between individuals and the community while considering the influences of the real environment is highlighted. Analysing studies and research intertwines with the United Nations' sustainable development goals, which focus on reducing inequalities and promoting sustainable development globally. The chapter demonstrates how modern technologies, cyberspace services, and cybersecurity policies can support the green transition and digital transformation while preserving local identity and fostering global cooperation to achieve international development goals.

University of Maribor Press

1 Uvod

Kibernetski prostor predstavlja kompleksno in dinamično okolje. Prostor je digitalni ekosistem, kjer se prepletajo digitalne tehnologije, komunikacijska omrežja in uporabniki. Razumevanje tega prostora je ključnega pomena za učinkovito upravljanje in zaščito pred kibernetskimi grožnjami. Trajnostni razvoj skozi digitalizacijo sloni na ključni uporabi kibernetskega prostora in omogoča (tudi) globalno sodelovanje vseh deležnikov. V kibernetskem prostoru se vsakodnevno prepletajo različni uporabniki, od posameznikov in podjetij do državnih institucij, ki se na različnih ravneh med seboj povezujejo tako lokalno kot globalno. Uporabniki kibernetskega prostora imajo ključno vlogo pri oblikovanju in delovanju tega kompleksnega okolja.

V kibernetskem prostoru so uporabniki aktivni ustvarjalci vsebin, obenem pa tudi potrošniki digitalnih vsebin. S pomočjo socialnih omrežij, blogov, forumov in drugih spletnih platform uporabniki ustvarjajo in delijo vsebine, ki prispevajo k nenehnemu širjenju informacij in znanja (Anderson in Rainie, 2021). Tako kibernetski prostor prinaša številne priložnosti in načine sodelovanja, vendar predstavlja tudi tveganja, povezana z varnostjo in zasebnostjo uporabnikov. Grožnje, kot so kibernetski napadi, kraja identitete in zlonamerna programska oprema, lahko resno ogrozijo varnost osebnih podatkov in zasebnost uporabnikov (Chertoff in Simon, 2020). Kibernetska varnost je zato ključnega pomena za zaščito uporabnikov v tem prostoru. Pomemben vidik kibernetskega prostora je tudi digitalna enakost, ki zagotavlja, da imajo vsi uporabniki, ne glede na njihov socialno-ekonomski status, dostop do digitalnih tehnologij in omrežij. Digitalna enakost omogoča širše vključevanje v digitalno družbo in spodbuja trajnostni razvoj (United Nations, 2020). Le ta sta vključena v več ciljev trajnostnega razvoja (ang. *Sustainable Development Goals – SDGs*) Organizacije združenih narodov. Najbolj relevantna sta cilja (United Nations, 2020) 9 in 10. Cilj 9: Industrija, inovacije in infrastruktura poudarjajo potrebo po izgradnji odporne infrastrukture, spodbujanju trajnostne industrializacije in podpiranju inovacij. Vključuje dostop do informacijskih in komunikacijskih tehnologij ter prizadevanje za univerzalni dostop do interneta v najmanj razvitih državah. Cilj 10: Zmanjšanje neenakosti se osredotoča na zmanjševanje neenakosti znotraj držav in med njimi. Vključuje zagotavljanje enakih možnosti ter zmanjševanje neenakosti v prihodkih. Digitalna enakost je ključni del tega cilja, saj omogoča dostop do izobraževanja, zaposlitvenih priložnosti in drugih pomembnih

storitev za vse ljudi, ne glede na njihovo družbeno ali gospodarsko ozadje. Tudi cilj 4 (United Nations, 2020): Kakovostna izobrazba prispeva k digitalni enakosti z zagotavljanjem vključujoče in enakopravne kakovostne izobrazbe ter spodbujanjem vseživljenjskega učenja za vse. Poudarja pomen digitalne pismenosti kot dela sodobne izobrazbe; cilj 17 (United Nations, 2020): Partnerstva za doseganje ciljev pa poudarja pomen globalnega partnerstva za trajnostni razvoj, vključno s sodelovanjem pri tehnologiji, znanju in finančnih sredstvih za doseganje ciljev. Vključuje krepitev mednarodnega sodelovanja pri znanosti, tehnologiji in inovacijah ter izboljšanje dostopa do tehnologij, zlasti informacijskih in komunikacijskih tehnologij. Uporaba kibernetskega prostora močno prispeva k transparentni in vključujoči družbi. Predstavljeni cilji skupaj pa pomagajo ustvariti okolje, ki podpira digitalno enakost in trajnostni razvoj na globalni ravni.

Kibernetski prostor s svojo vseprisotnostjo in globalnostjo močno vpliva na družbo in kulturo. Uporabniki s(m)o nosilci sprememb, saj s svojimi dejanji, interakcijami in inovacijami oblikujemo digitalne skupnosti in (sub)kulture. Tako kibernetski prostor omogoča globalno povezovanje in sodelovanje, kar vodi do izmenjave idej in kulturnih vplivov (Geels idr., 2017). Zato so uporabniki kibernetskega prostora pomembni snovalci prihodnjih družb, s svojo vlogo in vplivi pa sodelujejo tudi pri spodbujanju trajnostnega razvoja. S sodelovanjem v digitalnih iniciativah, ki podpirajo okoljevarstvene projekte, družbeno odgovorne prakse in trajnostne inovacije, prispevajo k ustvarjanju bolj trajnostne prihodnosti (United Nations, 2020). Kibernetski prostor je torej dinamično okolje, kjer uporabniki igrajo ključno vlogo pri oblikovanju digitalne pokrajine, zagotavljanju varnosti, spodbujanju digitalne enakosti in trajnostnega razvoja. Kibernetska varnost, kot del dejavnosti posameznika in rabe tehnologij za polno rabo kibernetskega prostora, vključuje ukrepe in strategije za zaščito informacijskih sistemov in podatkov pred nepooblaščenim dostopom, napadi in drugimi škodljivimi dejanji (Chertoff in Simon, 2020). Pomen kibernetske varnosti zato narašča z rastjo digitalizacije in povezanosti različnih sistemov v naših življenjih in je neločljivo povezan z napredkom družbe in prehodom v Družbo 5.0, kjer svojo moč črpa iz sinergij med realnim in navideznim-kibernetskim prostorom in povezovanjem (lokalnih) skupnosti v globalnem prostoru.

2 Kibernetska varnost v luči Družbe 5.0 in digitalnega prehoda

Kibernetska varnost igra ključno vlogo v prehodu k Družbi 5.0, kjer je cilj harmonična integracija naprednih tehnologij v vsakdanje življenje za izboljšanje kakovosti življenja in trajnostni razvoj. Družba 5.0, ki jo je prvič predlagala Japonska, se osredotoča na uporabo tehnologij, kot so umetna inteligenca, internet stvari (IoT) in veliki podatki (BigData), za reševanje družbenih izzivov ter ustvarjanje pametnih skupnosti (Fukuyama, 2018). V Družbi 5.0 je kibernetska varnost ključnega pomena zaradi naslednjih razlogov:

- *Zaščita občutljivih podatkov in sistemov*: Ker Družba 5.0 temelji na obsežni uporabi digitalnih tehnologij, je zaščita občutljivih podatkov in sistemov ključnega pomena. Brez ustreznih varnostnih ukrepov so osebni podatki, zdravstveni zapisi, finančni podatki in drugi kritični podatki ranljivi za kibernetske napade (Sandip Foundation, 2023).
- *Zaupanje in varnost*: Za uspešno integracijo naprednih tehnologij v vsakdanje življenje je potrebno zaupanje uporabnikov. Kibernetska varnost zagotavlja, da so digitalne storitve in platforme varne za uporabo, kar povečuje zaupanje uporabnikov in spodbuja širšo uporabo teh tehnologij (Von Solms in Van Niekerk, 2013).
- *Ohranjanje gospodarske in državne stabilnosti*: Kibernetski napadi lahko povzročijo velike gospodarske izgube ali vplivajo na državno stabilnost. Varnostne rešitve in digitalno varnostna opismenjenost in opolnomočenje uporabnikov pomagajo zaščititi podjetja pred finančnimi izgubami, ki jih povzročijo kibernetski napadi, ter zagotavljajo nemoteno delovanje gospodarstva (Ponemon Institute, 2020), na državni ravni pa preprečujejo vmešavanje tujih deležnikov s svojimi politikami in mednarodno manipulacijo.
- *Podpora trajnostnemu razvoju*: Kibernetska varnost skozi sodelovanje različnih deležnikov z intenzivno rabo kibernetskega prostora omogoča varno izvajanje trajnostnih projektov, kot so npr. pametna omrežja, pametna mesta in e-zdravje. Varna digitalna infrastruktura, kot hrbtenica zagotavljanja delovanja interneta, in izvajanje dejavnosti v kibernetskem prostoru podpirata trajnostne rešitve, ki prispevajo k okoljski zaščiti in družbeni blaginji (World Economic Forum, 2020). Obenem pa z zmanjševanjem potreb po potovanjih in globalnim povezovanjem v

kibernetskem prostoru pomembno vplivajo na zmanjševanje ogljičnega odtisa.

Kibernetski prostor in kibernetska varnost igrata pomembno vlogo pri podpori trajnostnemu razvoju in zmanjševanju ogljičnega odtisa. Uporaba digitalnih tehnologij, kot so internet stvari (ang. *Internet of Things – IoT*), pametna mesta in pametna omrežja, omogoča učinkovitejše upravljanje virov, kar zmanjšuje porabo energije in emisije (Geels idr., 2017). Digitalizacija omogoča daljinsko delo in telekomunikacije, kar zmanjšuje potrebo po fizičnih potovanjih. Pametna logistika optimizira transportne poti, kar vodi k manjši porabi goriva in emisij. Poleg tega digitalne tehnologije omogočajo boljšo integracijo obnovljivih virov energije v omrežja, kar zmanjšuje odvisnost od fosilnih goriv (United Nations, 2020). Kot ugotavljata Titus in Russell (2023), kibernetska varnost zagotavlja zaščito teh digitalnih sistemov pred napadi, kar je ključno za zanesljivo delovanje trajnostnih tehnologij.

2.1 Izzivi in strategije za kibernetsko varnost

Izzivi kibernetske varnosti v Družbi 5.0 vključujejo nenehno razvijajoče se kibernetske grožnje, soočanje s pomanjkanjem strokovnjakov za kibernetsko varnost in naraščajočo potrebo po globalnem sodelovanju. Reševanje teh izzivov zahteva celovit pristop, ki vključuje naslednje strategije:

- *Izobraževanje in usposabljanje*: Povečanje znanja in zavedanja o kibernetski varnosti med uporabniki in strokovnjaki je ključno za preprečevanje kibernetskih napadov (Soomro idr., 2016). Opolnomočenje uporabnikov je glavni cilj te točke strategije.
- *Razvoj naprednih varnostnih tehnologij*: Uporaba naprednih tehnologij, kot so generativna umetna inteligenca, mehke logike, nevronske mreže in strojno učenje, za zaznavanje in preprečevanje kibernetskih groženj v realnem času (Li idr., 2020). Te tehnologije se stalno razvijajo in so vse bolj uporabljene in uporabne pri zaščiti kibernetskega prostora.
- *Mednarodno sodelovanje*: Kibernetske grožnje ne poznajo meja, zato je mednarodno sodelovanje bistvenega pomena za izmenjavo informacij, najboljših praks in skupnih varnostnih standardov (International Telecommunication Union – ITU, 2018).

Kibernetska varnost je torej temeljni element za uspešen prehod v Družbo 5.0, saj zagotavlja varno in zanesljivo uporabo naprednih tehnologij, ki prispevajo k trajnostnemu razvoju in izboljšanju kakovosti življenja. Trajnostni razvoj pa se nanaša na uravnoteženje gospodarskega razvoja, socialne vključenosti in okoljskega varstva, da bi zadostili potrebam sedanjih generacij, ne da bi pri tem ogrozili zmožnosti prihodnjih generacij (United Nations, 2020). Integracija naprednih tehnologij v vsakdanje življenje igra ključno vlogo pri doseganju harmonije med digitalno in zeleno preobrazbo (Geels idr., 2017). Kibernetska varnost je torej ključni element pri uresničevanju trajnostnega razvoja in digitalnega prehoda, zlasti v kontekstu lokalnih skupnosti. Sinergija med omenjenimi elementi (trajnostni razvoj, digitalni prehod, varen kibernetski prostor) omogoča ustvarjanje varnih, odpornih in vključujočih digitalnih okolij, ki spodbujajo trajnostne cilje. Ker pa je kibernetski prostor stičišče dogajanj v sodobni družbi in omogoča trajnostni razvoj, je njegova vloga pri trajnostnem razvoju naslednja:

- *Varna digitalna infrastruktura*: Za doseganje trajnostnih ciljev je nujno, da lokalne skupnosti vzpostavijo varno in zanesljivo digitalno infrastrukturo. To vključuje zaščito pametnih omrežij, energetskih sistemov, komunikacijskih omrežij in drugih kritičnih infrastruktur pred kibernetskimi grožnjami (ITU, 2018). Varna digitalna infrastruktura omogoča učinkovito upravljanje virov in zmanjšuje okoljski odtis.
- *Podpora pametnim mestom, skupnostim in vasem*: Kibernetska varnost je temelj delovanja pametnih mest, ki so osrednji del trajnostnega razvoja. Pametne skupnosti uporabljajo tehnologije, kot so IoT, veliki podatki in umetna inteligenca za izboljšanje kakovosti življenja, zmanjšanje porabe energije in boljše upravljanje urbanih virov. Kot ugotavlja Fukuyama (2018), so te tehnologije ranljive brez ustreznih varnostnih ukrepov za napade, ki lahko ogrozijo njihove koristi.
- *Zaščita podatkov in (podatkovne) zasebnosti*: Trajnostni razvoj vključuje varovanje podatkov in zasebnosti prebivalcev lokalnih skupnosti. Kibernetska varnost zagotavlja, da so osebni podatki, zdravstveni zapisi, finančni in drugi občutljivi podatki zaščiteni pred nepooblaščenim dostopom in zlorabami (Von Solms in Van Niekerk, 2013), obenem pa posameznik lahko ustrezno zavaruje svojo zasebnost. To povečuje zaupanje prebivalcev v digitalne rešitve in spodbuja njihovo širšo uporabo.

Varnostne politike in strategije, ki podpirajo digitalno preobrazbo in zeleni prehod, pomagajo zmanjševati neenakosti in spodbujajo trajnostni razvoj na globalni ravni.

2.2 Varnostne politike za digitalno preobrazbo

Celovita kibernetska varnost vključuje razvoj in izvajanje politik za zaščito digitalne infrastrukture pred kibernetskimi napadi, varovanje podatkov in zaščito osebnih informacij. Digitalna preobrazba pa vključuje integracijo digitalnih tehnologij v vse vidike družbe in gospodarstva. Za uspešno izvedbo te preobrazbe so potrebne močne zaveze, ki jih implementiramo skozi varnostne politike. Tako se zagotovi boljša zaščita podatkov, omrežij in sistemov pred kibernetskimi grožnjami. Varnostne politike morajo vključevati več ključnih elementov za zagotovitev učinkovite kibernetske varnosti in podpore digitalni preobrazbi. Varnostne politike morajo vključevati naslednje ključne elemente:

- *Celovita kibernetska varnost:* Temeljni element digitalne preobrazbe. Vključuje razvoj in izvajanje politik, ki zaščitijo digitalno infrastrukturo pred kibernetskimi napadi, zagotavljajo varnost podatkov in zaščito osebnih informacij. Kot navaja Chertoff (2020), morajo organizacije sprejeti celovit pristop h kibernetski varnosti, ki vključuje preprečevanje, zaznavanje, odzivanje in obnovo po kibernetskih napadih.
- *Izobraževanje in ozaveščanje:* Digitalna preobrazba zahteva visoko raven ozaveščenosti in usposobljenosti na področju kibernetske varnosti med vsemi uporabniki digitalnih tehnologij. Uporabniki morajo biti seznanjeni s tveganji in naučeni, kako se zaščititi pred kibernetskimi grožnjami. Tako npr. Hatamian idr. (2019) poudarjajo pomen izobraževalnih kampanj in programov za ozaveščanje o kibernetski varnosti ter doseganje opolnomočenja uporabnikov.
- *Regulacija in skladnost:* Varnostne politike morajo vključevati regulativne okvire, ki določajo standarde in smernice za kibernetsko varnost. Organizacije morajo upoštevati te standarde in zagotavljati skladnost s predpisi, kot sta npr. Uredba o varstvu podatkov (General data protection rule – GDPR) v Evropi in Zakon o zasebnosti potrošnikov (California Consumer Privacy Act– CCPA) v Kaliforniji. Regulacija pomaga zagotoviti, da so varnostne prakse usklajene in učinkovite (Lewis, 2018).

Chertoff (2020) poudarja, da moramo sprejeti celovit pristop h kibernetski varnosti, ki vključuje preprečevanje, zaznavanje, odzivanje in obnovo po kibernetskih napadih. Izobraževanje in ozaveščanje sta ključna za uspešno digitalno preobrazbo, saj je potrebna visoka raven ozaveščenosti in usposobljenosti na področju kibernetske varnosti med vsemi uporabniki digitalnih tehnologij.

2.3 Strategije za zeleni prehod

Zeleni prehod vključuje prehod na trajnostne prakse in tehnologije, ki zmanjšujejo okoljski in ogljični odtis ter spodbujajo uporabo obnovljivih virov energije, trajnostni transport in digitalizacijo. Pri podpori zelenemu prehodu se opiramo na elementa:

- *Pametna omrežja in obnovljivi viri energije*: Pametna omrežja omogočajo učinkovitejšo rabo energije in integracijo obnovljivih virov energije. Vendar pa so ta omrežja ranljiva za kibernetske napade, zato je pomembno zagotoviti njihovo varnost. Lee idr. (2013) poudarjajo pomen kibernetske varnosti pri zaščiti pametnih omrežij in zagotavljanju stabilnega delovanja energetskih sistemov. Za uspeh pa je treba dodati vse dele kritične in ključne infrastrukture.
- *Trajnostne urbane rešitve*: Pametne skupnosti, ki uporabljajo digitalne tehnologije za upravljanje virov in izboljšanje kakovosti življenja, igrajo ključno vlogo pri zelenem prehodu. Varnostne politike, ki naslavljajo rabo kibernetskega prostora, morajo opredeliti zaščito digitalnih sistemov pred kibernetskimi grožnjami, da se zagotovita njihova zanesljivost in učinkovitost delovanja. Primeri uspešnih pametnih mest, kot je Ljubljana, (Seidl, 2022) kažejo, kako lahko varnostne politike podpirajo trajnostni razvoj.

Zagotavljanje varnega dostopa do digitalnih tehnologij za vse člane družbe zmanjšuje digitalni razkorak in spodbuja vključujoč razvoj. Združeni narodi (United Nations, 2020) poudarjajo pomen zagotavljanja enakih možnosti za dostop do digitalnih virov in storitev za vse prebivalce. Varnostne politike, ki podpirajo uporabo trajnostnih tehnologij, prispevajo k doseganju trajnostnih ciljev. Varnostne politike, ki podpirajo digitalno preobrazbo in zeleni prehod, imajo ključno vlogo pri zmanjševanju neenakosti in spodbujanju trajnostnega razvoja na globalni ravni. Na primer, Masdar City v Združenih arabskih emiratih uporablja napredne tehnologije

za energetsko učinkovitost in obnovljive vire energije, hkrati pa zagotavlja kibernetsko varnost za zaščito svojih digitalnih sistemov (Reiche, 2010). Globalne varnostne politike in standardi pomagajo uskladiti prizadevanja za kibernetsko varnost in trajnostni razvoj po vsem svetu. Mednarodno sodelovanje pri izmenjavi informacij, najboljših praks in tehnologij je ključnega pomena za obvladovanje globalnih izzivov (ITU, 2018).

Pri rabi kibernetskega prostora je za uspešno digitalno preobrazbo in trajnostni razvoj ključna sinergija med kibernetsko varnostjo in lokalnimi skupnostmi. Sodelovanje med lokalnimi skupnostmi, vladami in zasebnim sektorjem pri razvoju in izvajanju varnostnih politik je bistvenega pomena za ustvarjanje varnega in trajnostno naravnanega digitalnega okolja (Chertoff in Simon, 2020). Lokalne skupnosti lahko delujejo kot katalizatorji sprememb, saj z izvajanjem trajnostnih projektov in varnostnih ukrepov prispevajo k doseganju globalnih razvojnih ciljev. Skupnosti, sodelujoče v digitalnih pobudah, ki podpirajo trajnostne in varnostne prakse, prispevajo k ustvarjanju bolj varne in trajnostne prihodnosti za vse (Soomro idr., 2016). Z zagotavljanjem varnosti in zanesljivosti digitalnih sistemov lahko lokalne skupnosti učinkovito izkoristijo prednosti digitalizacije za trajnostno in vključujočo prihodnost.

Z digitalizacijo in prehodom od klasičnega v kibernetski prostor pa se vloga lokalnih skupnosti spreminja. Lokalno postaja vse bolj globalno, lokalno delovanje ima širši vpliv, vpliv globalnega pa vpliva na večino lokalnih dejavnosti. Digitalni prehod v lokalnih skupnostih vodimo skozi naslednje korake:

- *Vključujoča digitalizacija*: Lokalnim skupnostim omogoča dostop do digitalnih tehnologij in storitev, kar zmanjšuje digitalni razkorak in spodbuja digitalno enakost. Vsi člani skupnosti, ne glede na njihov socialno-ekonomski status, imajo dostop do digitalnih virov, izobraževanja in storitev.
- *Krepitev lokalne identitete in sodelovanja*: Digitalne platforme omogočajo lokalnim skupnostim, da krepijo svojo identiteto in sodelovanje. Kibernetska varnost zagotavlja varno okolje za izmenjavo informacij, sodelovanje pri lokalnih projektih in komunikacijo med člani skupnosti; to spodbuja občutek pripadnosti in krepi socialno kohezijo.
- *Spodbujanje trajnostnih praks*: Digitalni prehod lokalnim skupnostim omogoča, da sprejmejo trajnostne prakse, podprte z informacijskimi tehnologijami in

storitvami kibernetskega prostora, kot so recikliranje, zmanjšanje porabe energije in uporaba obnovljivih virov energije. Kibernetska varnost zagotavlja, da so sistemi za upravljanje teh praks zaščiteni pred napadi in motnjami, kar omogoča njihovo učinkovito delovanje.

Kombinacija kibernetskega prostora in trajnostnega razvoja ponuja edinstvene priložnosti za lokalne skupnosti, da izboljšajo svojo odpornost, vključenost in trajnostno naravnanost. Predstavitev pomena integracije naprednih tehnologij v vsakdanje življenje z namenom doseganja harmonije med digitalno in zeleno preobrazbo pa včasih predstavlja težavo, saj vpliva na odpornost (ang. *resilience*) posameznika, gospodarskih družb, držav in družbenih skupnosti.

Konflikti, ki smo jim trenutno priča – v Ukrajini, Palestini in na drugih kriznih območjih, kažejo na pomen kibernetskega prostora, storitev in odpornosti družbe ob pojavu nove realnosti in novih groženj. Kibernetsko bojevanje in kibernetski napadi so postali del sodobnih konfliktov, kar vpliva na stabilnost in varnost globalne skupnosti. In posredno seveda vpliva na lokalne skupnosti, varnost – tako v realnem kot kibernetskem prostoru in odpira hibridne grožnje.

V kontekstu kibernetskega prostora, kibernetske varnosti in trajnostnega razvoja so hibridne grožnje še posebej pomembne, saj združujejo različne oblike napadov in taktike za dosego kompleksnih ciljev. Hibridne grožnje vključujejo kombinacijo kibernetskih napadov, dezinformacij, gospodarskega pritiska in drugih oblik asimetričnega bojevanja, kar ustvarja večplastne izzive za varnost in stabilnost. Kot vidimo, so značilnosti hibridnih groženj podobne značilnostim kibernetske varnosti in kibernetskega bojevanja:

- *Kombinacija različnih taktik*: Hibridne grožnje združujejo kibernetske napade z drugimi oblikami napadov, kot so dezinformacijske kampanje in ekonomski pritiski, kar otežuje zaznavanje in odzivanje nanje. To (Borghard in Lonergan, 2017) lahko povzroči destabilizacijo in dolgotrajno škodo za tarčne države ali organizacije.
- *Vpliv na kritično infrastrukturo*: Kibernetski napadi, ki so del hibridnih groženj, lahko ciljajo na kritično infrastrukturo, kar ima lahko hude posledice za energetske sisteme, vodooskrbo, promet in zdravstvene storitve. Napadi na

ukrajinsko elektroenergetsko omrežje (Greenberg, 2019) so primer grožnje, ki lahko povzroči obsežne izpade in motnje.

- *Dezinformacijske kampanje*: Uporaba dezinformacij kot dela hibridnih groženj lahko vpliva na javno mnenje, povzroči zmedo in zmanjša zaupanje v institucije. Te taktike se pogosto uporabljajo za destabilizacijo političnih sistemov in manipulacijo volitev (Wardle in Derakhshan, 2017).
- *Nujnost celovitega pristopa*: Boj proti hibridnim grožnjam zahteva celovit pristop, ki vključuje krepitev kibernetske varnosti, izobraževanje in ozaveščanje prebivalstva ter mednarodno sodelovanje. Pomembno je vzpostaviti regulativne okvire in politike, ki podpirajo odpornost proti hibridnim grožnjam (Lewis, 2018).

Hibridne grožnje lahko neposredno vplivajo na trajnostni razvoj, saj napadi na kritično infrastrukturo in dezinformacije lahko upočasnijo ali celo onemogočijo doseganje trajnostnih ciljev. Zato je ključnega pomena, da varnostne politike vključujejo ukrepe za zaščito pred hibridnimi grožnjami in spodbujajo odpornost skupnosti. Seveda pa vse elemente kibernetskega prostora napredno uporabljajo države, ki so v konfliktu z drugimi državami (Rusija – Ukrajina), entitetami (Izrael – Hamas Palestina) ali organizacijami (ZDA – Huawei).

3 Kibernetski prostor in konflikti

Kibernetski prostor je postala pomembna platforma za ustvarjanje konfliktov in manipulacijo, ki se pogosto dosega s kibernetskim bojevanjem in drugimi oblikami digitalnih napadov. Kibernetski prostor vključuje vse digitalne infrastrukture in omrežja, ki omogočajo komunikacijo, shranjevanje in obdelavo informacij. Zaradi globalne povezanosti in odvisnosti od teh tehnologij je kibernetski prostor ključni cilj za tiste, ki želijo destabilizirati nasprotnike ali pridobiti strateške prednosti. Konflikte se ustvarja predvsem z naslednjimi dejavnostmi:

- *Kibernetsko bojevanje:* V sodobnih konfliktih se kibernetski prostor uporablja kot bojišče. Kibernetsko bojevanje vključuje napade na kritične infrastrukture, komunikacijske sisteme, finančne institucije in druge ključne sektorje, kar povzroča motnje in škodo (Kostyuk in Zhukov, 2019). Primeri vključujejo ruske kibernetske napade na Ukrajino, kjer so napadi na elektroenergetski sistem povzročili obsežne izpade električne energije

(Greenberg, 2019). Kibernetsko bojevanje vključuje uporabo kibernetskih napadov za doseganje vojaških ali političnih ciljev. Te operacije lahko vključujejo napade na kritično infrastrukturo, kot so energetski sistemi, vodni viri, transportna omrežja in komunikacijski sistemi, kar lahko povzroči hude motnje in škodo. Prav tako vključujejo finančne napade, ki lahko povzročijo gospodarsko škodo, destabilizirajo trg in zmanjšajo zaupanje v finančne sisteme. To obsega krajo podatkov, izsiljevalsko programsko opremo in druge oblike finančnih goljufij. Vohunske operacije, ki vključujejo krajo občutljivih informacij, in vohunske dejavnosti lahko oslabijo nasprotnikove zmogljivosti in omogočijo strateško prednost. To vključuje vdor v vladne sisteme, vojaške podatkovne baze in druge ključne tarče. Za proučevanje pa je treba poznati elemente kibernetskega bojevanja, ki so:

- *Kibernetski napadi (ang. Cyber Attacks):* Vključujejo različne oblike napadov, kot so napadi z zavrnitvijo storitve (DDoS), zlonamerna programska oprema (ang. *malware*), ribarjenje (ang. *phishing*) in vdor v sisteme (ang. *hacking*). Tovrstni napadi (Lewis, 2018) so usmerjeni v destabilizacijo, krajo podatkov ali povzročanje gospodarske škode.
- *Kibernetska obramba (ang. Cyber Defense):* Vključuje vse ukrepe in strategije za zaščito informacijskih sistemov pred kibernetskimi napadi. To vključuje (Von Solms in Van Niekerk, 2013) uporabo požarnih zidov, šifriranje, varnostne protokole in nenehno spremljanje sistemov.
- *Kibernetsko obveščanje (ang. Cyber Intelligence):* Vključuje zbiranje in analizo podatkov za prepoznavanje in preprečevanje kibernetskih groženj. Obveščevalne službe in varnostni strokovnjaki uporabljajo te informacije za razvoj učinkovitih obrambnih strategij (Borghard in Lonergan, 2017).
- *Operacije v kibernetskem prostoru (ang. Cyber Operations):* Vključujejo načrtovane in usklajene dejavnosti za izvajanje kibernetskih napadov ali obrambo pred njimi. Kot predstavljata Titus in Russell (2023), so vključene tako ofenzivne kot defenzivne operacije.

- *Propaganda in dezinformacije*: Kibernetski prostor se uporablja tudi za širjenje propagande in dezinformacij, kar vpliva na javno mnenje in destabilizira

družbo. Po Wardle in Derakhshanu (2017) so te taktike pogosto uporabljene za manipulacijo informacij, kar povzroča zmedo in zmanjšuje zaupanje v (klasične) medije in (državne, uradne) institucije. Kibernetski prostor omogoča hitro in široko razširjanje informacij, kar se izkorišča za širjenje propagande in dezinformacij, z naslednjimi taktikami:

- *Manipulacija informacij:* Lažne novice, zavajajoče informacije in teorije zarote se širijo prek družbenih omrežij in drugih digitalnih platform. To lahko vpliva na javno mnenje, povzroča zmedo in zmanjšuje zaupanje v medije in institucije.
- *Kampanje vplivanja:* Organizirane kampanje za vplivanje na volitve, politične odločitve in družbene konflikte lahko destabilizirajo države in regije. Te kampanje pogosto vključujejo uporabo botov[1], lažnih profilov in ciljanih oglasov za širjenje specifičnih narativov.
- *Psihološke operacije:* Uporaba psiholoških tehnik za vplivanje na vedenje in prepričanja ljudi. To vključuje širjenje strahu, negotovosti in dvomov, kar lahko oslabi nasprotnikovo odpornost in povečanje notranjih konfliktov.

Ker kibernetski prostor omogoča najrazličnejše manipulacije, je, kot omenjeno, opolnomočenje uporabnikov nujno, uporaba naprednih tehnoloških rešitev za identifikacijo neželenih elementov iz kibernetskega prostora pa predstavlja osnovno higieno sodobne rabe informacijsko-komunikacijskih tehnologij. S tem dosežemo tudi (ustrezno?) stopnjo družbene odpornosti. Zaradi konflikta interesov in dejanskega vpliva (globalnega) kibernetskega prostora na družbo pa iščemo elemente družbene odpornosti, ki jo dosegamo z različnimi elementi. Glavni elementi so:

- *Izobraževanje in ozaveščanje:* Povečanje zavedanja o kibernetskih grožnjah in izobraževanje prebivalstva o varnostnih ukrepih sta ključna za krepitev odpornosti družbe. Uporabniki morajo biti seznanjeni s tehnikami

[1] Bot je računalniški program, zasnovan za izvajanje določenih nalog samodejno, brez človeškega posredovanja. Boti se uporabljajo v različnih kontekstih, od preprostih spletnih robotov, ki zbirajo podatke z interneta, do zapletenih chatbotov, ki komunicirajo z uporabniki v naravnem jeziku. Pri uporabi botov je pomembno razumeti in upoštevati etične in varnostne vidike, zlasti kadar gre za bote, ki širijo dezinformacije ali izvajajo zlonamerna dejanja.

prepoznavanja dezinformacij in zaščite pred kibernetskimi napadi (Hatamian idr., 2019).

- *Razvoj varnostnih politik:* Države in organizacije morajo razviti in izvajati celovite varnostne politike, ki vključujejo preventivne ukrepe, hitro odzivanje na incidente in obnovitvene strategije po napadih. Vključuje tudi mednarodno sodelovanje pri izmenjavi informacij in najboljših praks (Kello, 2018).
- *Uporaba naprednih tehnologij:* Uporaba umetne inteligence, strojnega učenja in drugih naprednih tehnologij za zaznavanje in preprečevanje kibernetskih groženj lahko bistveno izboljša odpornost sistemov. Te tehnologije omogočajo hitro prepoznavanje nenavadnih vzorcev in odzivanje na potencialne grožnje v realnem času (Titus in Russell, 2023).
- *Krepitev kritične infrastrukture:* Zaščita kritične infrastrukture, kot so energetski sistemi, zdravstvene storitve in komunikacijska omrežja, je bistvenega pomena za ohranjanje stabilnosti med konflikti. Robustne varnostne ukrepe je treba vključiti v načrtovanje in upravljanje teh sistemov (Lewis, 2018).

Ti elementi omogočajo in ob pravilni izvedbi zagotovijo visoko raven odpornosti na kibernetskovarnostne incidente, v primeru incidentov pa se skrajša čas okrevanja in povrnitve informacijskih sistemov in ponovnega, celovitega dostopa do informacij v krajšem času oziroma zagotavlja elemente neprekinjenega delovanja. Neprekinjeno delovanje je element varnosti kibernetskega prostora in v povezavi s skupnostjo/mi zagotovi ustrezno tehnično zmogljivost za digitalno preobrazbo v prihajajočo Družbo 5.0.

4 Družbeni prehod

Povezava med kibernetskim prostorom, storitvami in lokalnimi skupnostmi prinaša številne prednosti, kot so krepitev socialne kohezije, izboljšanje kakovosti življenja in povečanje odpornosti na kibernetske grožnje. Pri prehodu v Družbo 5.0 lokalne skupnosti predstavljajo ključno vlogo pri gradnji odporne družbe, še posebej v kontekstu digitalnega prehoda in trajnostnega razvoja. Z vključevanjem lokalnih pobud v varnostne strategije in zagotavljanjem, da so lokalne infrastrukture zaščitene, lahko povečamo odpornost na kibernetske grožnje. Lokalne skupnosti lahko služijo kot prvi odziv na incidente in pomagajo pri obnovi po napadih, kar krepi celotno odpornost družbe (Cybersecurity and Infrastructure Security Agency -

CISA, 2021). Za povečanje odpornosti družbe na kibernetske grožnje je ključno izobraževanje in ozaveščanje prebivalstva. Poleg tega morajo države in organizacije razvijati celovite varnostne politike, ki vključujejo preventivne ukrepe, hitro odzivanje na incidente in obnovitvene strategije po napadih. To vključuje tudi mednarodno sodelovanje pri izmenjavi informacij in najboljših praks. Uporaba naprednih tehnologij bistveno izboljša odpornost sistemov. Te tehnologije omogočajo hitro prepoznavanje nenavadnih vzorcev in odzivanje na potencialne grožnje v realnem času. Dostop do sodobne digitalne infrastrukture, vključno s hitrim internetom, pametnimi napravami in izobraževalnimi viri, je bistven za zmanjšanje digitalnega razkoraka in omogoča enakopravno sodelovanje vseh članov skupnosti v digitalni dobi. Spodbujanje lokalnih pobud in projektov, ki temeljijo na uporabi digitalnih tehnologij, lahko izboljša kakovost življenja v skupnosti. Primeri vključujejo pametne rešitve za (pametna) mesta, skupnosti (Pametna mesta, 2024) in vasi (Pametne vasi, 2024), kot so pametna osvetlitev, upravljanje odpadkov in prometni sistemi, ki povečujejo učinkovitost in trajnost. E-participacija in spletne skupnosti lahko okrepijo demokratične procese ter spodbujajo transparentnost in odgovornost lokalnih oblasti. Kibernetski prostor omogoča tudi vzpostavljanje in krepitev socialnih vezi med prebivalci lokalnih skupnosti. S pomočjo digitalnih orodij lahko prebivalci komunicirajo, sodelujejo v skupnih projektih in si medsebojno pomagajo, kar krepi socialno kohezijo in pripadnost skupnosti. Povezava med kibernetskim prostorom, storitvami in lokalnimi skupnostmi je ključna za zagotavljanje varne, odporne in trajnostne prihodnosti. S krepitvijo digitalne infrastrukture, izobraževanjem o kibernetski varnosti, spodbujanjem socialne kohezije in pripravljenostjo na incidente lahko lokalne skupnosti učinkovito izkoristijo prednosti digitalizacije in povezovanja v kibernetskem prostoru za boljše življenje. Prehod v Družbo 5.0 stremi k harmonični integraciji naprednih tehnologij v vsakdanje življenje z namenom izboljšanja kakovosti življenja in doseganja trajnostnega razvoja. V tej novi družbeni paradigmi imajo kibernetski prostor, digitalne storitve in odpornost na kibernetske grožnje ključno vlogo.

Družba 5.0 temelji na uporabi naprednih tehnologij, predvsem umetne inteligence, IoT in velikih podatkov za reševanje družbenih izzivov ter ustvarjanje pametnih skupnosti. Ključni element družbenega prehoda skozi digitalizacijo je robustna in varna digitalna infrastruktura, ki vključuje širokopasovne internetne povezave, pametne naprave in digitalne platforme, ki omogočajo učinkovito upravljanje virov in izboljšanje javnih storitev (Fukuyama, 2018). Poleg tega ne smemo pozabiti, da je

za uspešen prehod bistvenega pomena kibernetska varnost. Kibernetski prostor, kjer se prepletajo digitalne tehnologije in komunikacijska omrežja, mora biti zaščiten pred grožnjami kibernetskih napadov, kraj podatkov in zlonamerne programske opreme. Kot navajata Kostyuk in Zhukov (2019), brez ustreznih varnostnih ukrepov lahko napadi na kritično infrastrukturo, kot so energetski sistemi in komunikacijska omrežja, povzročijo hude motnje in škodo. V ta sklop sodi tudi priprava in upoštevanje varnostnih politik in strategij, ki vključujejo preventivne ukrepe, hitro odzivanje na incidente in obnovitvene strategije.

4.1 Digitalna enakost

Pomembna prednost oziroma lastnost prehoda v Družbo 5.0 je krepitev socialne kohezije in spodbujanje digitalne enakosti. Digitalne platforme omogočajo prebivalcem, da aktivno sodelujejo pri odločanju o zadevah, ki vplivajo na njihovo skupnost. Kot navajajo Geels idr. (2017), e-participacija in spletne skupnosti lahko okrepijo demokratične procese ter spodbujajo transparentnost in odgovornost lokalnih oblasti.

Digitalna enakost je ključna za zagotavljanje dostopa digitalnih virov in storitev vsem članom skupnosti, kar zmanjšuje digitalni razkorak in spodbuja vključujoč razvoj. Dostop do hitrega interneta, izobraževalnih virov in digitalnih orodij omogoča vsem prebivalcem, da izkoristijo prednosti digitalizacije in prispevajo k trajnostnemu razvoju (United Nations, 2020). Pri tem imajo lokalne skupnosti ključno vlogo. Z zagotavljanjem varne in zanesljive digitalne infrastrukture ter izobraževanjem prebivalstva o kibernetski varnosti lahko lokalne skupnosti povečajo svojo odpornost na kibernetske grožnje. Kot ugotavlja CISA (2021), je izmenjava informacij, virov in najboljših praks med lokalnimi organi, podjetji in prebivalci bistvena za izgradnjo odpornih skupnosti. Poleg tega morajo lokalne skupnosti razvijati načrte za obnovo po kibernetskih napadih ali drugih incidentih. Hitri in učinkoviti odzivni ukrepi ter strategije za obnovitev normalnega delovanja kritične infrastrukture so ključni za ohranjanje stabilnosti in varnosti.

Prehod v Družbo 5.0 ponuja edinstveno priložnost za sinergijo med kibernetskim prostorom, trajnostnim razvojem in lokalnimi skupnostmi. Uporaba naprednih tehnologij za izboljšanje javnih storitev, upravljanje virov in spodbujanje socialne kohezije prispeva k ustvarjanju bolj trajnostnih in odpornih skupnosti. Sodelovanje

med lokalnimi, nacionalnimi in mednarodnimi akterji pa je ključno za dosego teh ciljev. Povezava med kibernetskim prostorom, storitvami in lokalnimi skupnostmi je torej ključna za zagotavljanje varne, odporne in trajnostne prihodnosti.

5 Kibernetski prostor in trajnostna prihodnost

Kibernetski prostor in trajnostni razvoj sta medsebojno povezana in se medsebojno dopolnjujeta na več ravneh. Kibernetski prostor, ki zajema digitalne tehnologije, komunikacijska omrežja in podatkovne infrastrukture, igra ključno vlogo pri spodbujanju trajnostnega razvoja, saj omogoča učinkovito upravljanje virov, boljše storitve in povečuje vključenost vseh članov družbe. Za trajno prihodnost so posebej pomembni naslednji elementi:

- *Učinkovito upravljanje virov:* Pomemben prispevek kibernetskega prostora k trajnostnemu razvoju je omogočanje učinkovitega upravljanja virov. Digitalne tehnologije (predvsem IoT, veliki podatki in umetna inteligenca) omogočajo zbiranje in analizo podatkov v realnem času. S tem se izboljšuje upravljanje naravnih virov (voda, energija, kmetijska zemljišča). Pametni sistemi za upravljanje energije, na primer, omogočajo optimizacijo porabe energije, zmanjšanje izgube in povečanje uporabe obnovljivih virov energije.
- *Izboljšanje javnih storitev:* Kibernetski prostor prispeva k izboljšanju javnih storitev. Digitalizacija javnih storitev, kot so zdravstvo, izobraževanje in javni prevoz, omogoča večjo dostopnost, učinkovitost in kakovost teh storitev. E-zdravstvo, na primer, omogoča oddaljeni dostop do zdravstvenih storitev, kar zmanjšuje potrebo po potovanju in s tem povezane emisije ter izboljšuje zdravstveno oskrbo prebivalcev, zlasti na oddaljenih območjih.
- *Povečevanje vključenosti:* Digitalna enakost je pomemben vidik trajnostnega razvoja. Kibernetski prostor omogoča digitalno vključenost, kar zmanjšuje digitalni razkorak in omogoča vsem prebivalcem, da izkoristijo prednosti digitalizacije. To vključuje dostop do izobraževalnih virov, zaposlitvenih priložnosti in socialnih storitev, kar prispeva k večji socialni koheziji in zmanjševanju neenakosti.
- *Spodbujanje trajnostnih praks*: Kibernetski prostor omogoča spodbujanje trajnostnih praks in vedenj. Digitalne platforme in aplikacije lahko

spodbujajo trajnostno vedenje posameznikov, kot so recikliranje, zmanjšanje porabe energije in uporaba javnega prevoza. Informacijske kampanje in izobraževalni programi na spletu lahko povečajo zavedanje o okoljskih vprašanjih in spodbujajo trajnostne življenjske sloge.

- *Varovanje okolja*: Uporaba naprednih tehnologij v kibernetskem prostoru omogoča tudi boljše spremljanje in varovanje okolja. Senzorji in naprave IoT lahko spremljajo okoljske pogoje, kot so kakovost zraka, onesnaženje vode in stanje ekosistemov, kar omogoča pravočasno ukrepanje in zmanjšanje negativnih vplivov na okolje. Veliko rezerv opažamo tudi v optimizaciji prometa in zamenjavo načina prevoza. Podatki, zbrani z naprednimi digitalnimi tehnologijami, pomagajo pri oblikovanju učinkovitih politik in ukrepov za varovanje okolja.
- *Krepitev odpornosti*: Kibernetski prostor prispeva tudi h krepitvi odpornosti družb na okoljske in druge grožnje. Digitalne tehnologije omogočajo hitrejše in učinkovitejše odzivanje na naravne nesreče, kot so poplave, požari in potresi, ter izboljšujejo sisteme zgodnjega opozarjanja. S pomočjo digitalnih orodij skupnosti načrtujejo in upravljajo obnovo po nesrečah, kar povečuje njihovo odpornost in prilagodljivost.

Za trajno prihodnost je sinergija med kibernetskim prostorom in trajnostnim razvojem ključna za doseganje trajnostnih ciljev. Kibernetski prostor je globoko prepleten z našim vsakdanjim življenjem, omogoča številne prednosti (izboljšana komunikacija, dostop do informacij, boljše storitve in povečana produktivnost), a prinaša tudi izzive, kot so vprašanja zasebnosti, varnosti in digitalne enakosti.

5.1 Vpliv kibernetskega prostora na vsakdanje življenje

Digitalne tehnologije in komunikacijska omrežja so revolucionarno spremenili način komuniciranja. Internet, socialna omrežja in aplikacije za sporočanje omogočajo hitro in učinkovito komunikacijo na daljavo. Anderson in Rainie (2021) znova poudarjata, da internet in digitalne tehnologije ljudem omogočajo, da se povezujejo z družino, prijatelji in sodelavci ne glede na geografske razdalje. Poleg tega omogočajo dostop do ogromne količine informacij prek spletnih iskalnikov, digitalnih knjižnic in spletnih medijev, kar prispeva k širšemu razumevanju sveta in spodbuja izobraževanje ter osebni razvoj.

Digitalizacija javnih in zasebnih storitev je ena izmed pomembnih možnosti kibernetskega prostora. E-uprava omogoča državljanom, da urejajo uradne zadeve prek spleta, kar zmanjšuje potrebo po osebnih obiskih uradov in povečuje učinkovitost storitev. Chertoff (2020) ugotavlja, da digitalizacija zdravstvenih storitev omogoča oddaljeni dostop do zdravnikov in zdravstvenih informacij, kar izboljšuje zdravstveno oskrbo, zlasti na oddaljenih območjih. Kibernetski prostor prav tako povečuje produktivnost z omogočanjem boljše organizacije dela in sodelovanja. Digitalna orodja za upravljanje projektov, komunikacijske platforme in oblačne storitve omogočajo delovnim skupinam, da učinkovito sodelujejo, ne glede na njihovo lokacijo. To prispeva k večji fleksibilnosti dela in boljši izrabi časa.

Kibernetski prostor pa prinaša tudi (varnostne) izzive, zlasti na področju zasebnosti in varnosti. S povečanjem količine osebnih podatkov, ki se zbirajo in obdelujejo v digitalnih sistemih, se povečuje tveganje za kršitve zasebnosti. Tako Sandip Foundation (2023) opozarja, da so osebni podatki pogosto tarča kibernetskih napadov, kar lahko vodi do kraje identitete, finančnih izgub in drugih škodljivih posledic. Tudi zato je kibernetska varnost ključna za zaščito podatkov in zagotavljanje zasebnosti uporabnikov. Uporabniki morajo biti ozaveščeni o varnostnih grožnjah in izvajati ustrezne varnostne ukrepe (uporaba močnih gesel, dvofaktorska avtentikacija, redno posodabljanje programske opreme).

Digitalna enakost je še en pomemben vidik vpliva kibernetskega prostora, ki zagotavlja, da imajo vsi člani družbe enak dostop do digitalnih tehnologij in storitev. Vendar pa digitalni razkorak še vedno obstaja, saj nekateri deli prebivalstva nimajo dostopa do interneta ali digitalnih naprav. Združeni narodi (United Nations, 2020) poudarjajo, da je pomembno, da se sprejmejo ukrepi za zmanjšanje digitalnega razkoraka in zagotavljanje enakih možnosti za vse. Digitalna vključenost omogoča večjo socialno kohezijo in prispeva k zmanjševanju neenakosti v družbi. Posebej je treba paziti, da z digitalizacijo in uvajanjem novih storitev ne pride do digitalne diskriminacije[2] in izključevanja posameznih skupin prebivalstva (starejše osebe,

[2] Digitalna diskriminacija je pojav, kjer določeni posamezniki ali skupine nimajo enakega dostopa do digitalnih tehnologij, interneta ali digitalnih veščin, kar vodi v neenakosti in izključenost iz digitalne družbe. Ta oblika diskriminacije se lahko manifestira skozi pomanjkanje infrastrukture na ruralnih območjih, finančne omejitve, ki preprečujejo nakup potrebne opreme, ali pomanjkanje izobraževalnih priložnosti za razvijanje digitalnih veščin. Posledično lahko prizadeti težje dostopajo do informacij, izobraževanja, zaposlitvenih priložnosti in socialnih storitev, kar poglablja obstoječe družbene in ekonomske neenakosti.

otroci, invalidi …). Dostop do izobraževalnih virov, zaposlitvenih priložnosti in socialnih storitev prek kibernetskega prostora lahko izboljša kakovost življenja in spodbuja trajnostni razvoj. Brez digitalne enakosti sta digitalni prehod in sinergija v skupnosti ogrožena.

Za razumevanje uporabe kibernetskega prostora in pristopov h kibernetski varnosti v luči trajnostnega razvoja predstavljamo nekaj primerov dobrih praks.

6 Sinergija lokalnih skupnosti v Družbi 5.0

Lokalne skupnosti imajo pri prehodu v Družbo 5.0 ključno vlogo kot katalizatorji sprememb. V tej preobrazbi gre za vključevanje naprednih tehnologij in digitalnih rešitev, ki so namenjene izboljšanju kakovosti življenja in trajnostnemu razvoju. Lokalni projekti in pobude so pogosto bolj prilagodljivi in lahko hitreje implementirajo inovativne rešitve, kar jih postavlja v ospredje teh sprememb. Eden od načinov, kako lokalne skupnosti prispevajo k Družbi 5.0, je z izvajanjem projektov pametnih mest, vasi.

Poudarjanje dobrih praks je ključno za razumevanje in širjenje učinkovitih rešitev, ki združujejo kibernetski prostor, kibernetsko varnost in trajnostni razvoj. Te prakse ne izboljšujejo le lokalnega življenja, temveč prispevajo tudi k doseganju globalnih trajnostnih ciljev. Z izmenjavo znanja in izkušenj ter povezovanjem teorije in prakse lahko ustvarimo bolj varno, trajnostno in povezano družbo v Družbi 5.0. Posebno pozornost smo namenili lokalnim skupnostim, ki so uspešno implementirale napredne tehnologije za dosego trajnostnih ciljev. Primere navajamo v časovnem zaporedju, ki prikazujejo, da je odločitev za digitalni prehod nujna, da se bivanje, sinergije in dobrobiti skupnosti odrazijo v daljšem časovnem obdobju.

- *Pametna skupnost Masdar, Združeni arabski emirati* (Reiche, 2010): Masdar City je ena najbolj trajnostnih mestnih skupnosti na svetu, ki uporablja napredne tehnologije za dosego trajnostnih ciljev. Mesto je zasnovano z uporabo najsodobnejših tehnologij za energetsko učinkovitost, obnovljive vire energije in trajnostno arhitekturo. Masdar City uporablja pametne mreže za

Na Univerzi v Mariboru, Fakulteti za varnostne vede področje digitalne diskriminacije proučujemo v okviru projekta Zelen in odporen prehod za varno in uspešno družbo. Projekt sofinancirata Republika Slovenija, Ministrstvo za visoko šolstvo, znanost in inovacije in Evropska unija – NextGenerationEU.

upravljanje porabe energije in vode, kar zmanjšuje porabo virov in ogljični odtis. Opremljeno je z naprednimi kibernetskimi varnostnimi rešitvami za zaščito svojih digitalnih sistemov in podatkov. Poleg tega mesto spodbuja raziskave in razvoj novih trajnostnih tehnologij ter sodelovanje med akademskimi institucijami, podjetji in vladnimi agencijami.

- *Pametno mesto Songdo, Južna Koreja* (Lee idr., 2013): Songdo je visoko tehnološko pametno mesto, ki je zasnovano kot model trajnostnega razvoja. Mesto je zgrajeno na načelih zelene gradnje in uporablja napredne digitalne tehnologije za upravljanje virov. Songdo uporablja integrirane IoT sisteme za spremljanje porabe energije, upravljanje prometa in ravnanja z odpadki. Zasnovano je tako, da spodbuja uporabo javnega prevoza in kolesarjenje, kar ugodno vpliva (tudi) na zmanjšan ogljični odtis. Songdo prav tako uporablja napredne kibernetske varnostne ukrepe za zaščito svojih digitalnih sistemov in podatkov, kar zagotavlja varnost in zanesljivost mestnih storitev.
- *Pametno mesto Barcelona, Španija* (Ajuntament de Barcelona, 2020): Barcelona je eno vodilnih pametnih mest na svetu, ki uspešno združuje digitalne tehnologije s trajnostnim razvojem. Mesto je implementiralo pametne mreže, ki izboljšujejo energetsko učinkovitost in zmanjšujejo porabo energije. Barcelona uporablja IoT tehnologije za spremljanje porabe vode in energije v realnem času, kar omogoča učinkovitejše upravljanje virov. Prav tako so razvili digitalne platforme za participacijo prebivalcev, kar jim omogoča sodelovanje v odločanju o mestnih zadevah. Te platforme so zaščitene z naprednimi kibernetskimi varnostnimi ukrepi, kar zagotavlja varnost podatkov in zaupanje prebivalcev v digitalne storitve.
- *Pametno mesto Ljubljana, Slovenija* (Seidl, 2022): Ljubljana je primer uspešnega pametnega mesta, ki združuje kibernetski prostor, kibernetsko varnost in trajnostni razvoj. Mesto je uvedlo vrsto naprednih tehnologij za izboljšanje kakovosti življenja svojih prebivalcev in trajnostno upravljanje virov. Ljubljana uporablja pametne senzorske sisteme za spremljanje kakovosti zraka, upravljanje prometa in ravnanje z odpadki. Senzorji zbirajo podatke v realnem času, kar omogoča mestnim oblastem, da sprejemajo informirane odločitve in zmanjšujejo negativne vplive na okolje. Poleg tega mesto uporablja napredne kibernetske varnostne ukrepe za zaščito svojih digitalnih sistemov pred grožnjami, kar zagotavlja varno in zanesljivo delovanje mestnih storitev.

Prikaz dobrih praks vključuje več ključnih vidikov učinkovite implementacije, ki služijo kot konkretni primeri uspešnih implementacij in vzor drugim skupnostim za izmenjavo znanja in izkušenj, tudi med različnimi skupnostmi in regijami. Uspešno implementirani obstoječi sistemi spodbujajo širjenje inovacij in najboljših praks, kar je ključno za doseganje trajnostnih ciljev na globalni ravni. Dobre prakse povezujejo teoretične koncepte trajnostnega razvoja in kibernetske varnosti z dejanskimi primeri iz prakse. To pa pomaga bolje razumeti, kako je možno razvite koncepte učinkovito prenesti v realno okolje.

Ti projekti vključujejo uporabo digitalnih tehnologij za upravljanje infrastrukture, kot so pametna osvetlitev, prometni sistemi in ravnanje z odpadki. Na primer, Ljubljana je uvedla vrsto tehnologij za spremljanje kakovosti zraka in upravljanje prometa, kar ne izboljšuje le kakovosti življenja, temveč zmanjšuje tudi okoljski odtis mesta (Seidl, 2022). Poleg tega lokalne skupnosti lahko prispevajo k doseganju globalnih razvojnih ciljev OZN z vključevanjem trajnostnih praks v svoje vsakodnevne dejavnosti. To vključuje uporabo obnovljivih virov energije, spodbujanje recikliranja in zmanjševanje porabe virov. Pametno mesto Songdo v Južni Koreji je primer, kjer so z uporabo naprednih tehnologij in trajnostnih praks dosegli visoko raven energetske učinkovitosti in zmanjšali ogljične odtise (Lee idr., 2013). Sodelovanje med lokalnimi in globalnimi akterji je ključno za širjenje najboljših praks in inovacij. Mednarodne organizacije, vlade in podjetja lahko podpirajo lokalne pobude z izmenjavo znanja, tehnologij in financiranja. Masdar City v Združenih arabskih emiratih je odličen primer, kjer so lokalni trajnostni projekti podprti z globalnimi partnerstvi, kar omogoča napredek v zelenih tehnologijah in energetski učinkovitosti (Reiche, 2010). Pomemben vidik sinergije lokalnih skupnosti v Družbi 5.0 je tudi digitalna enakost. Zagotavljanje dostopa do digitalnih tehnologij in internetnih storitev za vse prebivalce zmanjšuje digitalni razkorak in omogoča enakopravno sodelovanje vseh članov skupnosti v digitalni dobi. To vključuje izobraževanje prebivalcev o uporabi digitalnih orodij in zagotavljanje infrastrukture, ki omogoča dostop do interneta.

Lokalne skupnosti lahko služijo kot prvi odziv na kibernetske grožnje in druge krizne situacije. S hitrim odzivanjem in učinkovitimi varnostnimi ukrepi lahko zmanjšajo vpliv kibernetskih napadov na lokalno infrastrukturo in storitve. Poleg tega sodelovanje med lokalnimi oblastmi in nacionalnimi agencijami povečuje celotno odpornost skupnosti (CISA, 2021). Vse te pobude in projekti, ki izhajajo iz lokalnih

skupnosti, so ključni za prehod v Družbo 5.0. S spodbujanjem inovacij, trajnostnih praks in sodelovanja lahko lokalne skupnosti bistveno prispevajo h globalnim ciljem trajnostnega razvoja in izboljšanju kakovosti življenja.

7 Sklep

Pri prehodu v Družbo 5.0 imajo lokalne skupnosti ključno vlogo kot katalizatorji sprememb. S svojimi inovativnimi projekti in pobudami lahko hitro implementirajo napredne tehnologije, ki izboljšujejo kakovost življenja in spodbujajo trajnostni razvoj. Primeri, kot sta mesti Ljubljana in Songdo, kažejo, kako lahko lokalne skupnosti uporabljajo digitalne tehnologije za učinkovito upravljanje virov, zmanjšanje okoljskega odtisa in izboljšanje mestnih storitev (Lee idr., 2013; Seidl, 2022). Poleg tega lokalne skupnosti prispevajo k doseganju globalnih razvojnih ciljev OZN z vključevanjem trajnostnih praks in spodbujanjem digitalne enakosti. Masdar City je odličen primer, kjer globalna partnerstva podpirajo lokalne trajnostne projekte, kar omogoča napredek v zelenih tehnologijah in energetski učinkovitosti (Reiche, 2010).

Digitalna enakost je pomemben vidik sinergije lokalnih skupnosti v Družbi 5.0. Zagotavljanje dostopa do digitalnih tehnologij in internetnih storitev za vse prebivalce zmanjšuje digitalni razkorak in omogoča enakopravno sodelovanje vseh članov skupnosti v digitalni dobi. Vse pobude in vsi projekti digitalizacije in uvajanja trajnostnih praks, podprtih s tehnološkimi rešitvami in inovacijami, ki izhajajo iz lokalnih skupnosti, so ključni za digitalni prehod. S spodbujanjem inovacij, trajnostnih praks in sodelovanja lahko lokalne skupnosti bistveno prispevajo h globalnim ciljem trajnostnega razvoja in izboljšanju kakovosti življenja. Sinergija med kibernetskim prostorom, kibernetsko varnostjo in trajnostnim razvojem je torej ključna za zagotavljanje varne, odporne in trajnostne prihodnosti z vključevanjem vseh. Znanstvene in strokovne implikacije vključujejo razvoj celovitih varnostnih politik, ki naslavljajo tako digitalno kot fizično infrastrukturo, ter spodbujanje mednarodnega sodelovanja pri izmenjavi znanja in tehnologij (CISA, 2021; ITU, 2018). Vrednost za splošno javnost se odraža v povečani odpornosti na kibernetske grožnje, boljši kakovosti javnih storitev in večji socialni vključenosti, kar skupaj prispeva k bolj trajnostni in pravični prihodnosti.

Pri prehodu v Družbo 5.0 imajo lokalne skupnosti ključno vlogo kot katalizatorji sprememb. S svojimi inovativnimi projekti in pobudami lahko hitro implementirajo napredne tehnologije, ki izboljšujejo kakovost življenja in spodbujajo trajnostni razvoj. Digitalna enakost je pomemben vidik sinergije lokalnih skupnosti z zagotavljanjem dostopa do digitalnih tehnologij in internetnih storitev za vse. Zmanjšuje digitalni razkorak in omogoča enakopravno sodelovanje vseh članov skupnosti v digitalni dobi. Sinergija med kibernetskim prostorom, kibernetsko varnostjo in trajnostnim razvojem je ključna za zagotavljanje varne, odporne in trajnostne prihodnosti. Digitalni prehod se odraža v izboljšanju kakovosti življenja skozi boljše upravljanje mestnih virov, povečano odpornost na kibernetske grožnje in zmanjšanje digitalnega razkoraka. Lokalna skupnost je tako močnejša, bolj povezana in trajnostno naravnana, kar pozitivno vpliva na globalno raven trajnostnega razvoja.

Viri in literatura

Ajuntament de Barcelona. (2020). *Smart City Barcelona.* https://www.barcelona.cat/infobarcelona/en/tema/smart-city.

Anderson, J. Q. in Rainie, L. (2021). *The future of digital spaces and their impact on society. Pew Research Center.* https://www.pewresearch.org/internet/2021/11/22/the-future-of-digital-spaces-and-their-role-in-democracy/

Hatamian, M., Serna, J. in Rannenberg, K. (2019). Revealing the unrevealed: Mining smartphone users' privacy perception on app markets. *Computers & Security, 83*, 332–353. https://doi.org/10.1016/j.cose.2019.02.010

Borghard, E. D. in Lonergan, S. (2017). The logic of coercion in cyberspace. *Security Studies, 26*(3), 452–481. https://doi.org/10.1080/09636412.2017.1306396

CISA. (2021). *Critical infrastructure security and resilience. Cybersecurity and Infrastructure Security Agency.* https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience

Chertoff, M. (2020). *The cybersecurity playbook: How every leader and employee can contribute to a culture of security*. Wiley.

Fukuyama, M. (2018). Society 5.0: Aiming for a new human-centered society. *Japan SPOTLIGHT*, (July/August 2018), 47–50.

Geels, F. W., Sovacool, B. K., Schwanen, T. in Sorrell, S. (2017). Sociotechnical transitions for deep decarbonization: Accelerating innovation is as important as climate policy. *Science, 357*(6357), 1242–1244. https://doi.org/10.1126/science.aao3760

Greenberg, A. (2019). *Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers*. Doubleday.

Titus, A. in Russell, A. (2023). *The promise and peril of artificial intelligence: Violet teaming offers a balanced path forward.* https://ar5iv.labs.arxiv.org/html/2308.14253

ITU. (2018). *Global Cybersecurity Index (GCI) 2018*. International Telecommunication Union. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx

Sandip Foundation. (2023). *What is the future of cyber security in the digital world?.* https://www.sandipfoundation.org/blog/what-is-the-future-of-cyber-security-in-the-digital-world/

Kello, L. (2018). *The virtual weapon and international order*. Yale University Press.
Kostyuk, N. in Zhukov, Y. M. (2019). Invisible digital front: Can cyber attacks shape battlefield events? *Journal of Conflict Resolution, 63*(2), 317–347. https://doi.org/10.1177/0022002717737138
Lee, J., Phaal, R. in Lee, S. H. (2013). An integrated service-device-technology roadmap for smart city development. *Technological Forecasting and Social Change, 80*(2), 286–306. https://doi.org/10.1016/j.techfore.2012.09.020
Lewis, J. A. (2018). *Rethinking cybersecurity: Strategy, mass effect, and states*. Center for Strategic and International Studies. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/180108_Lewis_ReconsideringCybersecurity_Web.pdf
Pametne vasi. (2024). *Pametne vasi*. https://pametne-vasi.info/
Reiche, D. (2010). Renewable energy policies in the Gulf countries: A case study of the carbon-neutral 'Masdar City' in Abu Dhabi. *Energy Policy, 38*(1), 378–382. https://doi.org/10.1016/j.enpol.2009.09.028
Seidl, P. (29. 4. 2022). *Zgled drugim evropskim mestom: Ljubljana podnebno nevtralno pametno mesto*. Ljubljanainfo. https://ljubljanainfo.com/novica/lokalno/zgled-drugim-evropskim-mestom-ljubljana-podnebno-nevtralno-pametno-mesto/133172
Soomro, Z. A., Shah, M. H. in Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management, 36*(2), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009
United Nations. (2020). *The Sustainable Development Goals Report 2020*. https://unstats.un.org/sdgs/report/2020/
Von Solms, R. in Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004
Wardle, C. in Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policy making*. Council of Europe. https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c
World Economic Forum. (2020). *The global risks report 2020*. http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf