sciendo

Sodobni vojaški izzivi, 2024 – 26/št. 2
Contemporary Military Challenges, 2024 – 26/No. 2

Urban Praprotnik

DOI: 10.2478/cmc-2024-0011

NAČELO RAZLIKOVANJA V KIBERNETSKEM VOJSKOVANJU

PRINCIPLE OF DISTINCTION IN CYBER WARFARE

Povzetek Kot eno temeljnih načel mednarodnega humanitarnega prava za zaščito civilnega prebivalstva, načelo razlikovanja določa, da morajo vpleteni v sovražnosti vselej razlikovati med civilnimi objekti in vojaškimi cilji, ter civilisti in borci. Članek z analizo uporabe tega načela naslovi vprašanje o zadostnosti zaščite, ki jo načelo ponuja v kibernetski domeni. Velika odvisnost vojska od civilne kibernetske infrastrukture namreč razširi nabor vojaških ciljev na sisteme, na katere se zanašajo ključne civilne dejavnosti. Nejasnosti se pojavljajo tudi pri zadostitvi na videz enostavnim pogojem za status borca ter udeležbi civilistov pri izvajanju kibernetskih operacij.

Ključne besede ***Načelo razlikovanja, kibernetsko vojskovanje, mednarodno humanitarno pravo, izbira vojaških ciljev.***

Abstract Principle of distinction, one of the fundamental principles of international humanitarian law dictates, that participants in hostilities at all times distinguish between civilian objects and military objectives, as well as between civilians and combatants. This article addresses the adequacy of the protection offered by the principle in the cyber domain. Great reliance of militaries on civilian cyberinfrastructure expands the range of military objectives to the systems which key civilian activities depend on. There are many unknowns in fulfilling even the simple conditions for the combatant status, as well as in regulation of civilian direct participation in hostilities.

Key words ***Principle of distinction, cyber warfare, international humanitarian law, targeting.***

Uvod

Informacijsko-komunikacijska tehnologija nudi številne priložnosti za razvoj civilne družbe, zaradi česar se ta nanjo čedalje bolj zanaša. Vseprisotnejša digitalizacija širi napadalno površino za kibernetske operacije, kar pomeni povečano ranljivost (ICRC, 2020, str. 33). Nekatere kibernetske operacije so že povzročile veliko ekonomsko škodo (Nash idr., 2018), dosedanji napadi na kritično infrastrukturo pa razkrivajo ranljivost ključnih civilnih storitev na kibernetske napade (ICRC, 2020, str. 47–50). Zaradi potencialno uničujočih kibernetskih operacij za visokotehnološkega nasprotnika, sta varnost lastnega in dominiranje nad nasprotnikovim kibernetskim prostorom za sodobne oborožene sile ključnega pomena. Razumeti gre torej stališče Odprte delovne skupine za razvoj na področju informacij in telekomunikacij v kontekstu mednarodne varnosti (OEWG), da se bo uporaba kibernetskih operacij nadaljevala tudi v prihodnosti (Generalna skupščina Združenih narodov, 2021, odst. 16).

Bistvena značilnost kibernetskega prostora je medsebojna povezanost (*interconnectivity*) naprav, ki ga tvorijo. Večina vojaških omrežij se zanaša na civilno kibernetsko infrastrukturo, kot so podmorski kabli in sateliti. In obratno, civilna tehnologija se zanaša na vojaško. Nadzor ladijskega in zračnega prometa je tako denimo odvisen od vojaških satelitov. Medsebojna povezanost zato predstavlja nevarnost, da kibernetski napadi prizadenejo ključno civilno infrastrukturo (Droege, 2012, str. 538–539). Prepletenost vojaške in civilne sfere je tipična tudi za udeležence v kibernetskem vojskovanju,[1] za katerega je v primerjavi z drugimi domenami značilna večja vključenost nedržavnih in zasebnih akterjev.

V luči pomena kibernetskih operacij v sodobnem vojskovanju (Microsoft, 2022, str. 35), ter posledic, ki jih lahko povzročijo civilnemu prebivalstvu, je treba biti pozoren na njihovo pravno ureditev. Vsaka civilizacija je namreč poznala nekatere najbolj temeljne omejitve za zaščito civilnega prebivalstva v vojni, ki so veljale, še preden je mednarodno pravo dobilo celovito podobo. V sodobnem mednarodnem humanitarnem pravu (MHP) je za zaščito civilistov primarno pomembno načelo razlikovanja, ki je zasnovano na temelju mednarodnih pogodb, običajnega prava in splošnih pravnih načel (Sancin idr., 2009, str. 49, 57), predstavlja pa tudi običajno mednarodno pravo v obeh vrstah oboroženega spopada (ICJ, 1996, odst. 78).[2] Najnatančneje je opredeljeno v Prvem dopolnilnem protokolu k Ženevskim konvencijam (DP-I), določa pa, da morajo vpleteni v oboroženi spopad vselej razlikovati med civilnimi objekti in vojaškimi cilji, ter civilisti in borci. Temu ustrezno morajo usmerjati svoje

---

[1] *Univerzalno sprejete definicije kibernetskega vojskovanja ni, Mednarodni odbor Rdečega križa (MORK) pa ga definira kot izvajanje kibernetskih operacij, ki kot sredstva ali metode vojskovanja dosežejo prag oboroženega spopada, ali se odvijajo v njegovem okviru (ICRC, 2013, str. 1). ZDA definirajo kibernetske operacije kot uporabo kibernetskih zmogljivosti, katerih glavni namen je doseganje ciljev bodisi v kibernetskem prostoru, ali z uporabo kibernetskega prostora (DoD, 2021, str. 55). Rusi in Kitajci z izjemo prevodov iz tujih besedil pojma kibernetsko vojskovanje ne uporabljajo, govorijo pa o informacijskem vojskovanju, ki je širši pojem od definicije MORK in ZDA (Connell in Vogler, 2016, str. 3). Podobno definicijo uporablja tudi Šanghajska organizacija za sodelovanje (Shanghai Cooperation Organisation, 2009, str. 9).*

[2] *Oborožen spopad obstaja, ko pride do uporabe oborožene sile med državami oz. v primeru dolgotrajnega oboroženega nasilja med vladnimi oblastmi in organiziranimi oboroženimi skupinami ali med takšnimi skupinami znotraj države (ICTY, 1995, odst. 70).*

akcije zgolj zoper objekte, ki so vojaški cilji, ter borce in tiste civiliste, ki neposredno sodelujejo v sovražnostih. Namen članka je preučiti, ali načelo razlikovanja nudi zadostno zaščito tudi v kibernetski domeni. To stori z analizo uporabe načela razlikovanja pri objektih in osebah in izpostavitvijo najbolj perečih problemov, ter sprotno obravnavo predlogov stroke za njihovo rešitev.

1 RAZLIKOVANJE MED CIVILNIMI OBJEKTI IN VOJAŠKIMI CILJI V KIBERNETSKEM PROSTORU

1.1 Prispevek k vojaškemu delovanju

Vojaški cilji so skladno z 52. členom DP-I definirani kot objekti,[3] ki zaradi svoje narave, lokacije, namena ali uporabe pomembno prispevajo k vojaškemu delovanju in katerih popolno ali delno uničenje, zavzetje ali nevtralizacija daje v danih okoliščinah jasno vojaško prednost. Civilni objekti so vsi objekti, ki ne zadostijo definiciji vojaških ciljev.[4] Identificiranje vojaških ciljev po kriterijih narave in lokacije se v kibernetskem vojskovanju v bistvenem ne razlikuje od kinetičnega, razlike pa se pojavijo pri kriterijih uporabe in namena.

Večino kibernetskega prostora sestavljajo objekti, ki so v osnovi civilni, npr. podmorski kabli. Velika odvisnost vojska od civilne kibernetske infrastrukture je znatno razširila nabor objektov, ki so lahko napadeni, vključujoč sisteme, na katere se zanašajo ključne civilne dejavnosti. Legitimni vojaški cilji denimo postane civilni satelitski sistem za navigacijo ali pridobivanje slike v realnem času, če ga nasprotnik uporablja za pridobivanje posnetkov ali informacij o lokaciji vojaških objektov. Legitimne tarče predstavljajo tudi objekti, ki zaradi svoje prihodnje uporabe izpolnijo kriterij namena. Če stran v spopadu razpolaga z zanesljivimi informacijami, da bo nasprotnik pridobil računalniško opremo, ki bo prispevala k njegovemu vojaškemu delovanju, se taka oprema šteje za legitimni vojaški cilj (Schmitt, 2017, str. 440, 447).

Način izbiranja tarč je v kibernetski domeni specifičen, saj se pri izbiri tarč bolj kot na same podatke, ki potujejo po kibernetskem prostoru, osredotoča na njihovo pot - zlonamerno kodo je namreč zaradi minimalnih razlik v primerjavi z običajno kodo, ter visoke hitrosti prenosa, med njeno potjo praktično nemogoče najti. Zato se v kibernetskem vojskovanju napada fizična kibernetska infrastruktura.[5] Ker je že na začetku oboroženega spopada jasno, da se bo za izvajanje kibernetskih operacij uporabljala civilna kibernetska infrastruktura, praktično nemogoče pa je predvideti, katero milisekundo bo pri izvajanju neke vojaške operacije uporabljen

[3] *Objekt je nekaj vidnega in oprijemljivega, v čemer se razlikuje od pojmovanja v računalniški znanosti, kjer je termin definiran širše (Schmitt, 2017, str. 437).*

[4] *Definicija se pojavlja v več virih, ki veljajo v obeh tipih oboroženih spopadov, npr. v tretjem in četrtem odst. 1. člena Protokola o prepovedih ali omejitvah uporabe zažigalnih orožij.*

[5] *Geiss in Lahmann navedeno ponazorita s primerjavo vojskovanja v zračnem in kibernetskem prostoru. Pri prvem se ne cilja zraka, temveč zrakoplove, pri drugem pa je tarča medij, po katerem potuje zlonamerna koda (Geiss in Lahmann, 2012, str. 389).*

njen določen segment (Geiss in Lahmann, 2012, str. 386), tako vojaški cilji denimo postanejo vsi komunikacijski kanali, usmerjevalniki in strežniki, preko katerih bodo potovali, ali se na njih nahajali vojaški podatki (Schmitt, 2015, str. 19). Zlasti zaradi izpolnitve kriterijev uporabe in namena, bi tako vojaški cilj postala popolnoma vsa kibernetska infrastruktura (Pascucci, 2017, str. 438). Idealna rešitev te praktično nevzdržne situacije bi bila dosledna fizična delitev kibernetske infrastrukture na vojaško in civilno, za kar si trenutno prizadeva Mednarodni odbor Rdečega križa (MORK) (ICRC, 2023, OP 10). V hladni vojni je bila denimo ločitev na MILNET in ARPANET, ki sta se kasneje razvila v omrežje za vojaške komunikacije in internet (Šarf, 2017, str. 84), še izvedljiva, danes pa zaradi vseprisotne soodvisnosti vojaške in civilne kibernetske infrastrukture, ni uresničljiva. Bolj realistična bi bila zgolj ločitev objektov, ki so v MHP posebej zaščiteni, oziroma morebitna širitev njihovega nabora na druge objekte kritične infrastrukture.

1.2 Jasna vojaška prednost

Na videz odprto definicijo vojaškega cilja utegne zamejiti njen drugi del, ki v drugem odstavku 52. člena DP-I poleg prispevka k vojaškemu delovanju zahteva, da njegovo popolno ali delno uničenje, zavzetje ali nevtralizacija v danih okoliščinah daje jasno vojaško prednost. Tok podatkov je namreč odporen na motnje - če so nekateri komunikacijski kanali uničeni, lahko podatki do svojega cilja samodejno najdejo pot po preostalih kanalih. Tako je možno zagovarjati stališče, da civilna kibernetska infrastruktura, kljub svojemu pomembnemu prispevku k vojaškemu delovanju, ne more postati vojaški cilj, saj njeno uničenje, zavzetje ali nevtralizacija, resneje ne ogrožajo nasprotnikove zmožnosti izvajanja operacij in zato ne dajejo jasne vojaške prednosti. Jasna vojaška prednost bi bila podana kvečjemu z uničenjem vseh, ali vsaj večjih komunikacijskih poti (Mavropoulou, 2015, str. 44).[6] V praksi je ta dilema razvidna iz analize bombardiranja stavbe Radiotelevizije Srbije (RTS), pri katerem se je Nato zavedal, da bo bombni napad prekinil oddajanje zgolj za nekaj ur, kar je v Končnem poročilu tožilcu s strani odbora, ustanovljenega za pregled bombardiranja Zvezne republike Jugoslavije (ZRJ), s strani Nato sprožilo vprašanje o jasni vojaški prednosti takšnega napada. Strateška tarča (omrežje poveljevanja nadzora in komunikacij ZRJ) je bila namreč kompleksna mreža, ki je ni bilo možno onesposobiti v enem napadu. Nato je doseganje jasne vojaške prednosti opravičeval s trditvijo, da je bil napad na RTS zgolj del večje operacije zoper več podobnih objektov (poleg stavbe RTS tudi električno omrežje, radijske in televizijske relejne postaje v Novem Pazarju, Novem Sadu in Kruševcu) (ICTY, 2000, odst. 78).

Kibernetska infrastruktura torej ne more postati vojaški cilj, razen v primeru, da se uniči njen večinski del. Iz povedanega denimo sledi, da bi se zaradi inherentne odpornosti interneta, pogosto uporabljenega v vojaške namene, katere posledica

[6] *Talinski priročnik omrežje dvojne rabe, pri katerem se ne ve, katere njegove dele bodo prečkale vojaške komunikacije, ponazori z analogijo s cestnim omrežjem, pri katerem se ne ve natančno, kateri obvoz bodo ubrala vojaška vozila v primeru cestne blokade - v tem primeru celotno cestno omrežje šteje za vojaški cilj, oz. vsaj tisti njegov del, po katerem je pot vojaških vozil visoko verjetna (Schmitt, 2017, str. 446).*

je možnost pridobitve jasne vojaške prednosti zgolj z oviranjem večjega dela komunikacijskih poti, lahko kot vojaški cilj kvalificiral tudi internet v celoti (Mavropoulou, 2015, str. 54).[7] Takšen sklep, ki ne dopušča vmesnih nians, se zdi neživljenjski.

2 RAZLIKOVANJE MED CIVILISTI IN BORCI V KIBERNETSKEM PROSTORU

Poleg vojsk in vladnih agencij, kibernetske operacije pogosto izvajajo tudi zasebne institucije in posamezniki.[8] Nekateri nedržavni akterji so že pokazali kibernetske zmogljivosti, do nedavnega dostopne le državam (Generalna skupščina Združenih narodov, 2021, odst. 16), njihova vloga pa se bo v prihodnosti verjetno še povečevala in še bolj zameglila ločnico med vojaškimi in civilnimi osebami (ICRC, 2020, str. 34). Štrucl opaža, da je tudi rusko-ukrajinska vojna pokazala, da dejanske kibernetske zmogljivosti držav poleg vojska in državnih organov ležijo tudi v zasebnem sektorju (Štrucl, 2022, str. 117). Skladno s 3. členom Zakona o obrambi vojaško obrambo v Republiki Sloveniji (RS) izvaja Slovenska vojska (SV), civilno obrambo pa državljani, samoupravne lokalne skupnosti, državni organi, gospodarske družbe, zavodi in druge organizacije. Kibernetsko obrambo skladno s 24. členom Zakona o informacijski varnosti (ZInfV) izvajajo Urad Vlade RS za informacijsko varnost, skupine za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij, Ministrstvo za obrambo in drugi nacionalni organi, torej je moč podobno trditi tudi za RS. Velja opomniti, da se borce, ter zgoraj omenjene civiliste, ki so neposredno udeleženi v sovražnostih, lahko napade tako kibernetsko, kot tudi kinetično.[9]

2.1 Borci

Splošno sprejeta definicija borca izhaja iz 1. člena Haaškega pravilnika, za potrebe upravičenosti do statusa vojnega ujetnika jo je prevzel tudi 4. člen Ženevske konvencije o ravnanju z vojnimi ujetniki (ŽK-III). Skladno z obema pravnima viroma, so borci pripadniki oboroženih sil ene od strani v spopadu, ter pripadniki drugih milic in drugih prostovoljnih enot, vključno s tistimi pripadniki organiziranih odporniških gibanj, ki pripadajo eni od strani v spopadu,[10] ob izpolnjevanju naslednjih pogojev: poveljuje jim poveljnik, ki je odgovoren za svoje podrejene, imajo na

---

[7] *Skupina strokovnjakov za Talinski priročnik se je tega problema sicer zavedala in takšno rešitev v teoriji dopustila, vendar je menila, da okoliščine, ki bi napravile celoten internet vojaški cilj, zaenkrat še ne obstajajo. Nasprotno, vsak napad na internet kot tak, bi moral biti omejen le na njegove manjše segmente (Schmitt, 2017, op. cit. 14, str. 446).*

[8] *Eden izmed udeležencev srečanja strokovnjakov MORK je postavil tezo, da države s ciljem izogibanja nekaterim obveznostim in zaradi nepoznavanja MHP s strani obveščevalnih agencij, izvajanje kibernetskih operacij morda namenoma premikajo izven delokroga oboroženih sil (ICRC, 2020, str. 14).*

[9] *To se je denimo zgodilo v NMOS med Izraelom in Hamasom, v katerem se je Izrael na kibernetski napad Hamasa odzval z zračnim napadom na stavbo izvora napada (Doffman, 2019).*

[10] *Patriotski hekerji, ki izvajajo kibernetske operacije iz osebnih simpatij do strani v spopadu, zaradi prešibke povezave s stranjo v spopadu statusa borca ne uživajo.*

daljavo viden razpoznavni znak, odkrito nosijo orožje in izvajajo svoje operacije v skladu z zakoni in običaji vojne. V RS tej definiciji denimo zadostijo pripadniki Enote za komunikacijske in informacijske sisteme SV, ki je namenjena zagotavljanju delovanja komunikacijskih in informacijskih sistemov ter podpori poveljevanja in kontrole na strateškem in operativnem nivoju SV.

Stroka glede pogojev za status borca sicer ni enotna. Stališče MORK je, da je običajnopravna definicija borca zapisana v DP-I, namen definicij iz Haaškega pravilnika in ŽK-III pa naj bi bil zgolj določiti pogoje za status vojnega ujetnika, ki pa ne sovpada nujno s statusom pripadnika oboroženih sil (Henckaerts in Doswald-Beck, 2005, str. 15). Borec skladno z DP-I zaradi narave sovražnosti, ki včasih ne omogoča razlikovanja od civilnega prebivalstva, obdrži svoj status, če odkrito nosi orožje med vsako vojaško akcijo in dokler ga nasprotnik lahko vidi med vojaško pripravo pred napadom, v katerem bo sodeloval. DP-I tako v svojem 44. členu črta zahtevan pogoj nošenja na daljavo vidnega razpoznavnega znaka za status borca. V kontekstu kibernetskega vojskovanja je tak pristop smotrnejši, saj se borci pri kibernetskem vojskovanju fizično niti ne soočijo (Döge, 2010, str. 495). Čeprav Talinski priročnik[11] priznava obstoj kibernetskih orožij,[12] je strokovna skupina ugotovila, da zahteva po odkritem nošenju orožja v kibernetski domeni ni realna (Schmitt, 2017, str. 406). Opozoriti velja, da zgolj neuporaba konvencionalnega orožja s strani kibernetskih borcev še ne spreminja pravne ureditve, ki je v tem primeru popolnoma jasna. Kibernetski napadalci se v bistvenem ne razlikujejo od ostalih pripadnikov oboroženih sil, katerih primarna naloga ni boj z nasprotnikom (inženirji, kuharji, pravniki, ipd.). Našteti so prav tako oboroženi z lahko osebno oborožitvijo, s čimer zadostijo zahtevi po odkritem nošenju orožja.

Status borca pripada tudi pripadnikom *levée en masse* (množični odpor), ki so definirani kot prebivalci neokupiranega območja, ki se z oboroženo silo spontano uprejo bližajočemu nasprotniku, ne da bi se imeli čas organizirati v redne oborožene sile. Skladno z 2. členom Haaškega pravilnika štejejo za borce če odkrito nosijo orožje, ter spoštujejo zakone in običaje vojne, niso pa podvrženi zahtevi po nošenju razlikovalnega znaka ali druge razlikovalne oprave. Kibernetski *levée en masse* bi tako lahko sestavljali t. i. »hacktivisti« oz. »patriotski hekerji,« saj niso pripadniki oboroženih sil in na lastno iniciativo izvajajo kibernetske napade zoper nasprotnika. Čeprav to počno brez avtorizacije ali nadzora njihovih držav, zasledujejo iste politične cilje (Turns, 2012, str. 293). Zgoraj omenjeni pogoj odkritega nošenja orožja je v primeru *levée en masse* posebnega pomena zaradi odsotnosti zahteve po uporabi razlikovalnega znaka (ICRC, 2021, odst. 1021–1023).

---

[11] *Talinski priročnik je trenutno najbolj celovit dokument, ki med drugim obravnava uporabo MHP v kibernetski domeni. Lahko ga štejemo za nauk uglednih strokovnjakov za mednarodno pravo, torej služi kot pomožno sredstvo pri ugotavljanju in razlagi pravnih pravil.*

[12] *Za potrebe Talinskega priročnika so kibernetska orožja sredstva bojevanja, ki so uporabljena, dizajnirana ali namenjena povzročitvi smrti ali poškodb ljudem, oziroma uničenja ali poškodb objektom (Schmitt, 2017, str. 452).*

Čeprav Talinski priročnik priznava, da pogoj nošenja orožja v kibernetski domeni nima realne uporabe, pa brez vidnega orožja ni jasnega načina ločitve teoretičnega kibernetskega *levée en masse* od civilnega prebivalstva (Wallace in Reeves, 2013, str. 659). Prenosni računalniki in mobilni telefoni se lahko sicer nosijo odkrito, vendar je vprašljivo, če zaradi njihove vseprisotnosti med civilnim prebivalstvom zadostijo potrebi po razlikovanju (Turns, 2012, str. 293). Argument glede nošenja orožja pri *levée en masse* je v kibernetski domeni sicer enak tistemu v zvezi s pripadniki oboroženih sil, predstavljenim zgoraj. V Talinskem priročniku obstaja tudi dilema glede globine ozemlja pod sovražnim nadzorom, v katero *levée en masse* še sme izvajati kibernetske operacije (Schmitt, 2017, str. 409).

Zgodovinsko gledano *levée en masse* namreč ni izvajal operacij globoko v sovražno ozemlje, temveč je bil njegov namen zaustaviti nasprotnika na frontni liniji. Zato so nekateri avtorji mnenja, da se kibernetske operacije ukrajinske »IT armade,« katerih tarče se nahajajo na različnih koncih Rusije, ne morejo šteti kot akcije *levée en masse* (Buchan in Tsagourias, 2022). Zgodovinsko *levée en masse* sicer niti ni bil sposoben izvajanja napadov v globino sovražnega ozemlja, danes pa kibernetska orodja omogočajo povzročanje škode v nasprotnikovemu zaledju, ki lahko pripomore tudi k njegovi zaustavitvi na frontni liniji. Zaradi opisanih nejasnosti pri globini ozemlja pod sovražnim nadzorom, v katero se še smejo izvajati kibernetske operacije, ter vsebini pojma odkrite nošnje orožja v kibernetski domeni, kot konstitutivnih pogojev *levée en masse*, je zaslediti predloge popolne ukinitve te kategorije borcev za kibernetsko vojskovanje. Namesto nje naj bi se od vseh kibernetskih borcev zahtevalo upoštevanje štirih kriterijev iz Haaškega pravilnika in ŽK-III (Wallace in Reeves, 2013, str. 664). Omenjeni predlog spregleda kriterija spontanosti in neorganiziranosti, ki sta bistvena elementa *levée en masse*, nekatere kibernetske borce pa prikrajša statusa borca, saj bi se v tem primeru kvalificirali kvečjemu kot civilisti, ki se neposredno udeležujejo sovražnosti.

2.2 Civilisti

Za civiliste se skladno s 50. členom DP-I štejejo vsi, ki niso pripadniki oboroženih sil ali *levée en masse.* Njihova uporaba je v kibernetskem kontekstu mamljiva zaradi oteževanja pripisljivosti, njihovega tehničnega znanja in razpolaganja s kibernetskimi orodji, ki niso predmet tipičnega vojaškega inventarja (Hathaway idr., 2011, str. 854). Zgoraj omenjen opis kibernetske obrambe po ZInfV, ki jo izvajajo številni nacionalni organi, nakazuje, da je tudi pri kibernetski obrambi v oboroženem spopadu, katerega stran bi bila RS, pričakovati poudarjeno vlogo civilistov. Civilisti skladno z 51. členom DP-I postanejo legitimne vojaške tarče, kadar so neposredno udeleženi v sovražnostih. Zaradi vseprisotne uporabe civilistov (van Benthem, 2023), so v kibernetski domeni pravila o neposredni udeležbi v sovražnostih nadvse pomembna. Mednarodno pogodbeno pravo definicije neposredne udeležbe ne ponuja, obstaja pa dovolj strinjanja glede osnovnih parametrov Interpretativnih smernic o pojmu neposredne udeležbe v sovražnostih v MHP (*Interpretive Guidance on the Notion of Direct participation in Hostilities under International Humanitarian Law* – Interpretativne smernice), da te lahko služijo kot temelj za razpravo o neposredni

udeležbi v sovražnostih. V tem smislu so Interpretativne smernice avtoritativne (Turns, 2012, str. 286).

Same sovražnosti so v Interpretativnih smernicah definirane kot kolektivna uporaba sredstev in metod vojskovanja strani v spopadu. Ne zahteva se nujno uporaba oborožene sile zoper nasprotnika, ali povzročitev smrti, poškodb ali uničenja (Melzner, 2009, str. 47), kar pomeni, da pojem sovražnosti pokriva velik spekter kibernetskih operacij. Eden izmed zadržkov glede Interpretativnih smernic, ki je zaradi zamegljene ločnice med civilisti in borci v kibernetski domeni še toliko bolj utemeljen, je, da definirajo neposredno udeležbo preširoko (Goodman in Jinks, 2010, str. 639). V nadaljevanju bo predstavljeno, da temu ni nujno tako.

V Interpretativnih smernicah so identificirani trije konstitutivni elementi neposredne udeležbe v sovražnostih - nastanek škode, neposredna vzročna zveza, ter povezava s sovražnostmi.

2.2.1 Nastanek škode

Da se ravnanje kvalificira kot neposredna udeležba v sovražnostih, mora biti take narave, da lahko specifično škoduje vojaškim operacijam ali vojaškim zmogljivostim nasprotne strani v oboroženem spopadu, ali alternativno, povzroči smrt, poškodbo, ali uničenje. Zgolj nevšečnosti, kot je manipulacija civilnega računalniškega ali električnega omrežja, čeprav lahko resno vplivajo na javno zdravje, varnost, ali trgovino, ne dosežejo nivoja zahtevane škode (Melzner, 2009, str. 50). Motnja računalniškega sistema za nadzor železniškega omrežja, bi lahko omrežje torej ohromila in onemogočila potovanja v ciljni državi, ne bi pa dosegla zahtevanega nivoja škode.[13] Če bi enaka motnja ohromila transport moštva, oborožitve ali opreme, bi bil zaradi škodovanja vojaškim operacijam ali vojaškim zmogljivostim rezultat drugačen. Kibernetski napad v Estoniji leta 2007, ki je povzročil motnje vitalnih računalniških sistemov v administraciji, finančnem, ter socialnem sistemu, tako ni dosegel zahtevanega nivoja škode, saj ni prišlo do poškodb na objektih ali ljudeh. Napad z virusom Stuxnet pa bi zaradi nastanka fizične škode na centrifugah v Natanzu, kriteriju škode zadostil.[14]

2.2.2 Neposredna vzročna zveza

Interpretativne smernice neposredno vzročno zvezo pogojujejo z enim korakom med ravnanjem in nastankom škode. Tako kot delavec v tovarni orožja, za katerega so bili avtorji Interpretativnih smernic soglasni, da v sovražnostih ne sodeluje neposredno, naj neposredno ne bi sodeloval niti razvijalec kibernetskih orožij (Melzner, 2009, str. 53). Kibernetska orožja so v tem smislu lahko specifična – zaradi nasprotnikove nepričakovane ali spreminjajoče-se aktivne kibernetske

[13] *To se je denimo zgodilo v Nemčiji v oktobru 2022 (Thurau, 2022).*

[14] *Opomniti velja, da niti v Estoniji, niti v Iranu, ni potekal oboroženi spopad. Obenem tudi ni povsem jasno, kdo stoji za napadoma.*

obrambe, lahko obstaja neprestana potreba po nadgradnji kibernetskih orožij tekom samega napada. Takšne nadgradnje zahtevajo globlje sodelovanje med napadalcem in razvijalcem kibernetskega orožja, kar poveča intenzivnost razvijalčeve udeležbe v samem napadu. Nekatera ravnanja razvijalcev programske opreme tako lahko dosežejo prag neposredne vzročne zveze, saj so od škode oddaljena zgolj en korak (Matheson, 2019, str. 39). Interpretativne smernice v takšnem scenariju torej dajejo zelo življenjski rezultat.

2.2.3 Povezava s sovražnostmi

Pogoj povezave s sovražnostmi (*belligerent nexus*) zahteva, da dejanje v svoji zasnovi podpira eno stran v spopadu v škodo nasprotne strani (Melzner, 2009, str. 59). V kibernetski domeni pomaga razlikovati med patriotskimi hekerji, ki želijo pomagati svoji državi, ter skupinami, kot je recimo *Anonymous*. Oboji izvajajo podobne akcije, vendar zadnji tega ne počno s ciljem pomoči strani v spopadu. Pogoj povezave s sovražnostmi v izjemnih primerih vzame v obzir subjektivne lastnosti napadalca, kot je naklep,[15] kar se v kibernetskem scenariju zgodi v primeru »botneta«, specifično načrtovanega za izvajanje napadov porazdeljene zavrnitve storitve (*distributed denial of service* – DDoS) preko ugrabljenih civilnih računalnikov. Lastniki teh računalnikov se ne zavedajo njihove zlorabe, torej obdržijo svojo zaščito, čeprav njihovi računalniki postanejo vojaški cilji. Gre za še eno kibernetsko situacijo, ki s strani avtorjev Interpretativnih smernic morda ni bila predvidena, a zanjo Interpretativne smernice ponujajo praktično rešitev.

2,2,4 Ugotovitve o udeležbi civilistov v kibernetskem vojskovanju

Nabor aktivnosti, ki se štejejo za neposredno udeležbo v sovražnostih, je v kibernetski domeni širok, zaradi česar je v sodobnih oboroženih spopadih delež civilistov, ki predstavljajo legitimne tarče, večji, kot smo vajeni v klasičnih vojnah.[16] Ker pa operacije, ki sicer resno vplivajo na javno zdravje, varnost ali trgovino, ne dosežejo nujno nivoja zahtevane škode, razen če rezultirajo v uničenju civilne infrastrukture ali civilnih poškodbah, in ker Interpretativne smernice neposredno vzročno zvezo pogojujejo tudi z enim korakom med ravnanjem in nastankom škode, kar pri kibernetskih operacijah ni tipično, tvorijo visok prag za neposredno udeležbo

---

[15] *Te so vzete v račun le v izrednih okoliščinah, ko se civilist niti malo ne zaveda svoje vloge v izvajanju sovražnosti (voznik, ki nevede prevaža daljinsko vodeno bombo), ali pa, ko fizično niti ne ravna (mu je povsem odvzeta fizična svoboda - neprostovoljni človeški ščiti) (Melzner, 2009, str. 60).*

[16] *Skupina strokovnjakov za Priročnik iz Osla o izbranih temah prava oboroženih spopadov (Oslo Manual Manual on Select Topics of the Law of Armed Conflict) je bila soglasna, da se za neposredno udeležbo v sovražnostih štejejo: kibernetske aktivnosti, zasnovane za neposredno povzročitev poškodb ali uničenja nasprotni strani v spopadu, kibernetska obramba vojaških ciljev, prispevanje k postopkom izbire ciljev, udeležba v načrtovanju kibernetskih napadov, ter zagotavljanje oz. prenos taktično pomembnih informacij s ciljem pomagati bojnim operacijam. Zgolj pridobivanje vojaško pomembnih informacij še ne šteje za neposredno udeležbo, avtorji pa niso mogli določiti jasne meje med zbiranjem in procesiranjem pridobljenih informacij, ki pa že šteje kot neposredna udeležba v sovražnostih (Dinstein in Willy, 2020, pravilo 28).*

v sovražnostih.[17] Civilisti torej lahko izvajajo kibernetske operacije z znatnimi posledicami za civilno prebivalstvo, ne da bi postali vojaške tarče. Interpretativne smernice časovno okno neposredne udeležbe v sovražnostih poleg izvajanja sovražnosti omejijo še na pripravljalna dejanja in vrnitev z aktivnosti (Melzner, 2009, str. 65).

V kibernetskem vojskovanju je to nepraktičen standard, saj z izjemo operacij bližnjega dostopa, ni prihoda ali odhoda z operacije. Sama izvedba kibernetske operacije tipično poteka hitro, tako da pred njenim zaključkom napadalca običajno niti ni mogoče identificirati (Dinniss, 2013, str. 270). Obstoječa ureditev zaradi manjše verjetnosti zajetja, ki sicer izvotli pomen borčevskega privilegija, tako predstavlja iniciativo za neupoštevanje načela razlikovanja (Padmanabhan, 2013, str. 301).

2.3 Posebej zaščitene osebe

Zdravstveno osebje, pripadniki civilne zaščite, versko osebje, in druge posebej zaščitene osebe, uživajo svojo zaščito tudi v kibernetski domeni. Kot dodatna kategorija posebej zaščitenih oseb, bi se v tej domeni lahko šteli tudi pripadniki skupin za odzivanje na elektronske grožnje (*computer emergency response teams* – CERT). Skladno z ZInfV so v RS to skupine za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij. Po Pravilih odgovornega obnašanja v kibernetskem prostoru (*UN Norms of Responsible State Behaviour in Cyberspace*), naj takšne skupine ne bi bile vojaške tarče.[18] Sodelujoči na srečanju strokovnjakov o izogibanju civilni škodi v vojaških kibernetskih operacijah v oboroženih spopadih (*Avoiding Civilian Harm from Military Cyber Operations During Armed Conflicts*) so o potrebi, da se CERT v kibernetskem prostoru zaščiti podobno kot bolnišnično osebje, ki v kinetičnem vojskovanju nudi prvo pomoč, razpravljali leta 2020. Več strokovnjakov je izpostavilo, da je takšno analogijo težko vzpostaviti, saj sta vlogi prvih poleg saniranja škode tudi identifikacija vira napada in zaustavitev samega napada (ICRC, 2020, str. 28). Pravila odgovornega obnašanja v kibernetskem prostoru vsekakor predstavljajo dober nastavek za nadaljnje delo na področju ustanavljanja ekvivalentov bolničarjem, gasilcem, ali pripadnikom civilne zaščite v kibernetski domeni, pod pogojem da se njihove naloge zameji zgolj na zmanjševanje škode. V primeru izvajanja protinapada bi, podobno kot preostale zaščitene osebe, svojo zaščito začasno izgubili.

---

[17] *Turns na primeru desetih hipotetičnih kibernetskih operacij ugotavlja, da zgolj tri dosežejo prag neposredne udeležbe v sovražnostih. Najlažje je vzpostaviti pogoj povezave s sovražnostmi, najtežje pa neposredno vzročno zvezo (Turns, 2012).*

[18] *UN GGE je to predlagala v svojem poročilu GS OZN št. A/70/174, odst. 13(k), kasneje je GS OZN poročilo soglasno podprla v resoluciji št. 70/237. Pravila odgovornega obnašanja v kibernetskem prostoru sicer niso zavezujoča, državam pa služijo kot smernice pri ravnanju z IKT (Generalna skupščina Združenih narodov, 2021, odst. 25).*

Zaključek

Spoštovanje načela razlikovanja je v kibernetskem vojskovanju zahtevnejše kot v ostalih domenah vojskovanja. Naletimo namreč na več ovir, tako pri ločevanju civilnih objektov od vojaških ciljev, kot civilistov od borcev.

Zaradi velike odvisnosti vojska od kibernetskega prostora bi ob upoštevanju zlasti kriterijev uporabe in namena, lahko bil nabor civilnih objektov, ki se v kibernetskem vojskovanju spremenijo v vojaške cilje, izjemno širok in bi vključeval sisteme, na katere se zanašajo ključne civilne dejavnosti. Idealna rešitev je dosledna fizična delitev kibernetske infrastrukture na vojaško in civilno, ki pa zaradi njune vseprisotne soodvisnosti ni uresničljiva. Bolj realistična je zgolj ločitev objektov, ki so v MHP posebej zaščiteni, oziroma širitev njihovega nabora na druge objekte kritične infrastrukture. Odprto definicijo vojaškega cilja zamejuje zahteva po jasni vojaški prednosti, ki pa v zvezi s kibernetskimi omrežji ponuja neživljenjski zaključek, da bi bila jasna vojaška prednost podana zgolj z uničenjem vseh, ali vsaj večjega dela komunikacijskih poti.

Problemi pri ločevanju civilistov od borcev se pojavijo že pri konstitutivnih pogojih vizualnega razlikovanja za določene skupine oseb, tako ali drugače udeleženih v kibernetskem vojskovanju. Ker se borci pri kibernetskem vojskovanju fizično ne soočijo, je zahteva po nošenju na daljavo vidnega razpoznavnega znaka, po mnenju nekaterih avtorjev, utemeljeno, odveč. Del stroke meni tudi, da v kibernetski domeni nima realne uporabe zahteva po odkritem nošenju orožja. A zgolj neuporaba konvencionalnega orožja s strani kibernetskih borcev še ne spreminja popolnoma nedvoumne pravne ureditve. Če se odkrito nošenje orožja pri trenutni ureditvi še lahko zanemari pri večini borcev, se tega ne da storiti pri kibernetskem *levée en masse*, pri katerem je pogoj odkritega nošenja orožja edini element razlikovanja od civilistov. Obenem pa trenutno ni jasno, kaj se v kibernetski domeni sploh lahko šteje kot odkrito nošenje orožja.

V kibernetskem vojskovanju je delež civilistov, neposredno udeleženih v sovražnostih, večji, kot smo vajeni v klasičnih vojnah, kar je skladno z našo zakonodajo pričakovati tudi v RS, saj kibernetsko obrambo izvajajo Urad Vlade RS za informacijsko varnost, skupine za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij in drugi nacionalni organi. Uslužbenci teh organov lahko pod pogoji, identificiranimi v članku, postanejo legitimne vojaške tarče, v primeru zajetja s strani nasprotnika, pa so lahko zaradi odsotnosti njihovega borčevskega statusa tudi kazensko preganjani po nasprotnikovi zakonodaji.

Obenem pa tipične kibernetske operacije, katerih tarča je civilno prebivalstvo in lahko resno vplivajo na javno zdravje, varnost ali gospodarstvo, ne dosežejo nivoja zahtevane škode, razen če rezultirajo v uničenju civilne infrastrukture ali civilnih poškodbah. Civilisti torej lahko izvajajo kibernetske operacije z znatnimi posledicami za nasprotnikovo civilno prebivalstvo, brez nevarnosti, da bodo postali vojaški cilji. Obstoječa ureditev je do takšnih civilistov torej preveč prizanesljiva, saj jim nudi večjo zaščito kot osebam z borčevskim privilegijem.

V odsotnosti mednarodne jurisprudence na temo kibernetskega vojskovanja, je razjasnitev v članku identificiranih problemov zaenkrat odvisna od akademikov in bodoče prakse držav. Zaradi izpostavljenih pomanjkljivosti uporabe načela razlikovanja pri kibernetskem vojskovanju, ki posegajo v njegovo bistvo do te mere, da v nekaterih primerih ostane praktično brez zaščitne vrednosti, načelo razlikovanja osebam in objektom, zaščitenim v kinetičnem vojskovanju, v kibernetski domeni ne nudi zadostne zaščite. Kljub temu zaščita civilistov in civilnih objektov ni nujno nezadostna. Ugotovitev se namreč nanaša zgolj na načelo razlikovanja, ki pa podobno kot v drugih domenah vojskovanja, vselej deluje v kombinaciji z drugimi načeli MHP, zlasti načeloma previdnosti in sorazmernosti.[19]

Obstaja tudi nekaj dobrih predlogov dopolnitve obstoječe pravne ureditve, med katerimi velja poleg že omenjene ločitve v MHP posebej zaščitenih objektov, ter širitve njihovega nabora, izpostaviti tudi možnosti zaščite CERT z nekaterimi omejitvami pri izvajanju protinapadov, na podoben način, kot je zaščiteno zdravstveno in versko osebje, kar bi v RS lahko omogočalo zaščiten status skupinam za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij.

Literatura

1. *Buchan, R., in Tsagourias, N., 2022. ‚Ukrainian 'IT Army': A Cyber Levée en Masse or Civilians Directly Participating in Hostilities?'. https://www.ejiltalk.org/ukranian-it-army-a-cyber-levee-en-masse-or-civilians-directly-participating-in-hostilities/ (26. 2. 2024).*
2. *Connell, M., in Vogler, S., 2016. Russia's Approach to Cyber Warfare, CNA's Occasional Paper series, https://apps.dtic.mil/sti/pdfs/AD1019062.pdf (28. 2. 2024).*
3. *Department of Defense, 2021. Dictionary of Military and Associated Terms, https://www.supremecourt.gov/opinions/URLs_Cited/OT2021/21A477/21A477-1.pdf (28. 2. 2024).*
4. *Dinstein, Y., in Willy, D. A., 2020. Oslo Manual on Select Topics of the Law of Armed Conflict: Rules and Commentary. Springer.*
5. *Doffman, Z., 2019. Israel Responds to Cyber Attack with an Air Strike on Cyber Attackers in World First. Forbes, 6. maj, https://www.forbes.com/sites/zakdoffman/2019/05/06/israeli-military-strikes-and-destroys-hamas-cyber-hq-in-world-first/?sh=50d4edacafb5 (26. 2. 2024).*
6. *Döge, J., 2010. Cyber Warfare Challenges for the Applicability of the Traditional Laws of War Regime. Archiv des Völkerrechts, 48(4), str. 486-501.*
7. *Droege, C., 2012. Get off my Cloud: cyber warfare, international humanitarian law, and the protection of civilians. International Review of the Red Cross, 94(886), str. 533–578.*
8. *Geiß, R., in Lahmann, H., 2012. Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space. Israel Law Review, 45(3), str. 381–399.*
9. *Generalna skupščina Združenih narodov, (2015). The United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Report 2015 (A/70/174). Z dne 22. julija 2015.*
10. *Generalna skupščina Združenih narodov, (2021). OEWG Final Substantive Report (A/AC.290/2021/CRP.2). Z dne 10. marca 2021.*

[19] *Kibernetske operacije lahko s svojo nesmrtonosno naravo omogočijo napadanje vojaških ciljev z manjšo postransko škodo, kot jo povzročijo njihove kinetične alternative, zato so lahko ob odgovorni uporabi primernejše od kinetičnih. Glej npr stališče Združenega Kraljestva (UK, 2020, točka B).*

11. *Goodman, R., in Jinks, D. P., 2010. The ICRC Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law: An Introduction to the Forum, New York University International Law and Politics, 42, str. 637–640.*
12. *Harrison Dinniss, H., 2013. Participants in Conflict: Cyber warriors, patriotic hackers and the laws of war. V: D. Saxon, ur. International Humanitarian Law and the Changing Technology of War, str. 251–278. Leiden: Boston: Martinus Nijhoff Publishers.*
13. *Hathaway, O. idr., 2011. The Law of Cyber-Attack. California Law Review, 100, str. 817–886.*
14. *Henckaerts, J., in Doswald-Beck, L., 2009. Customary International Humanitarian Law, Vol. 1 – Rules. Cambridge: Cambridge University Press.*
15. *Human Rights Watch, 2003. International Humanitarian Law Issues in a Potential War in Iraq. Human Rights Watch Briefing Paper. Washington DC.*
16. *ICRC, 2013. Cyberwarfare and international humanitarian law: the ICRC's position, https://www.icrc.org/en/doc/assets/files/2013/130621-cyberwarfare-q-and-a-eng.pdf (28. 2. 2024).*
17. *ICRC, 2020. Avoiding Civilian Harm from Military Cyber Operations During Armed Conflicts: ICRC Expert Meeting, 21–22 January 2020, Geneva, https://shop.icrc.org/avoiding-civilian-harm-from-military-cyber-operations-during-armed-conflicts-icrc-expert-meeting-21-22-january-2020-geneva-pdf-en (27. 2. 2024).*
18. *ICRC, 2021. Commentary on the Third Geneva Convention: Convention (III) relative to the Treatment of Prisoners of War. Cambridge: Cambridge University Press.*
19. *ICRC, 2022. Digitalizing the Red Cross, Red Crescent and Red Crystal Emblems: Benefits, Risks, and Possible Solutions. ICRC, Ženeva.*
20. *ICRC, 2023. Preventing and minimizing digital threats to people affected by armed conflict, Draft Elements of Resolution, November 2023. ICRC, Ženeva.*
21. *International Court of Justice (ICJ), 1996. Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion). I.C.J. Reports, 226.*
22. *International Criminal Tribunal for the Former Yugoslavia (ICTY), 1995. The Prosecutor v. Dusko Tadić, IT-94-1-AR72 (Appeals Chamber, Decision).*
23. *International Criminal Tribunal for the Former Yugoslavia (ICTY), 2000. Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia. International Legal Materials, 39(5), str. 1257–1283.*
24. *Matheson, C., 2019. From Munitions to Malware: A Comparative Analysis of Civilian Targetability in Cyber Conflict. Journal of Law & Cyber Warfare, 7(2), str. 29–66.*
25. *Mavropoulou, E., 2015. Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks. Journal of Law & Cyber Warfare, 4(2), str. 23–93.*
26. *Melzer, N., 2009. Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law. International Committee of the Red Cross (ICRC), Ženeva.*
27. *Microsoft, 2022. Microsoft Digital Defense Report 2022. https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022 (27. 2. 2024).*
28. *Nash, K. S., Castellanos, S., in Janofsky, A., 2018. One Year After NotPetya Cyberattack, Firms Wrestle with Recovery Costs. The Wall Street Journal, https://www.wsj.com/articles/one-year-after-notpetya-companies-still-wrestle-with-financial-impacts-1530095906 (27. 2. 2024).*
29. *Padmanabhan, V. M., 2013. Cyber Warriors in the Jus in Bello. International law studies, 288(89), str. 288-308.*
30. *Pascucci, C., 2017. Distinction and Proportionality in Cyber War: Virtual Problems with a Real Solution. Minnesota Journal of International Law, 26(1), str. 419–460.*

31. *Protokol o prepovedih ali omejitvah uporabe zažigalnih orožij, Uradni list Socialistične Federativne Republike Jugoslavije, Mednarodne pogodbe, št. 3/82.*
32. *Sancin, V., Švarc, D., in Ambrož, M., 2009. Mednarodno pravo oboroženih spopadov. Ljubljana: Poveljstvo za doktrino, razvoj, izobraževanje in usposabljanje.*
33. *Schmitt, M. N., 2015. The Law of Cyber Targeting. Naval War College Review, 68(2), Article 3, str. 1–20.*
34. *Schmitt, M. N., 2017. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2. izd. Cambridge: Cambridge University Press.*
35. *Second International Peace Conference, The Hague, 1907. Hague Convention (IV) Respecting the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land. International Conferences (Haag), z dne 18. oktobra 1907.*
36. *Shanghai Cooperation Organisation, 2009. Agreement on Cooperation in Ensuring International Information Security. Jekaterinburg, 16. junija.*
37. *Šarf, P., 2017. Legality of Low-Intensity Cyber Operations Under International Law. Sodobni vojaški izzivi, 19(3), str. 81–93.*
38. *Štrucl, D., 2022. Russian Aggression on Ukraine: Cyber Operations and the Influence of Cyberspace on Modern Warfare. Sodobni vojaški izzivi, 24(2), str. 103–123.*
39. *Thurau, J., 2022. Germany's Critical Infrastructure Is Poorly Protected. DW, https://www.dw.com/en/germanys-critical-infrastructure-is-poorly-protected/a-63505983 (26. 2. 2024).*
40. *Turns, D., 2012. Cyber Warfare and the Notion of Direct Participation in Hostilities. Journal of Conflict and Security Law, 17, str. 279–297.*
41. *Ur. l. SFRJ, 1978. Dopolnilni protokol k ženevskim konvencijam z dne 12. avgusta 1949 o zaščiti žrtev mednarodnih oboroženih spopadov, z dne 8. junija 1977 (DP-I), mednarodne pogodbe, št. 16/78.*
42. *van Benthem, T. J., 2023. Privatized Frontlines: Private-Sector Contributions in Armed Conflict. 15th International Conference on Cyber Conflict: Meeting Reality (CyCon), Talin, Estonija, str 55–69. DOI: 10.23919/CyCon58705.2023.10182177.*
43. *Wallace, D. A., in Reeves, S., 2013. The Law of Armed Conflict's ‚Wicked' Problem: Levée En Masse in Cyber Warfare. International Law Studies, 89, str. 646–668.*
44. *Združeno kraljestvo, 2020. Response to Chair's Initial 'Pre-draft' of the Report of the OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security, April 2020.*
45. *Ženevska konvencija o ravnanju z vojnimi ujetniki, z dne 12. avgusta 1949. (1950). Ur.l. Prezidijuma LS FLRJ, št. 6/50.*

email: urban.praprotnik@mors.si