

**SLOVENSKI  
POGLED  
NA POMEN  
MEDNARODNEGA PRAVA  
V KIBERNETSKEM  
PROSTORU**



REPUBLIKA SLOVENIJA  
MINISTRSTVO ZA ZUNANJE  
IN EVROPSKE ZADEVE



## Seznam kratic

ARSIWA	Členi o odgovornosti držav za mednarodno protipravna dejanja
EKČP	Evropska konvencija o varstvu človekovih pravic
ESČP	Evropsko sodišče za človekove pravice
SVS	Skupina vladnih strokovnjakov
MKS	Mednarodno kazensko sodišče
ICJ	Meddržavno sodišče
IKT	Informacijsko-komunikacijske tehnologije
KMP	Komisija za mednarodno pravo
MHP	Mednarodno humanitarno pravo
ZN	Združeni narodi
GS ZN	Generalna skupščina Združenih narodov

## I. DEL

### I. SPLOŠNO

V tem dokumentu je predstavljen slovenski pogled na pomen mednarodnega prava v kibernetnem prostoru. Za kibernetne dejavnosti se štejejo dejanja držav in nedržavnih akterjev, ki vključujejo uporabo informacijsko-komunikacijskih tehnologij (IKT) ter s tem povezanih fizičnih sredstev, ki neposredno ali posredno vplivajo na digitalni ali fizični prostor. V tem pogledu izraz *kibernetna dejavnost* zajema vsako uporabo ali izkoriščanje kibernetnih zmogljivosti, da bi v kibernetnem prostoru ali prek njega dosegli neke cilje. V posebnih primerih, ki vključujejo strukturirane ukrepe z možnostjo kinetičnih učinkov, kot je uporaba sile ali mednarodnega humanitarnega prava (MHP), se zaradi natančnosti uporablja izraz *kibernetne operacije*.

Kibernetne dejavnosti se nanašajo na fizično (strojna oprema in druga infrastruktura IKT, vključno s fizičnimi omrežnimi elementi in logičnimi komponentami (podatki, programska oprema, protokoli itn.)) in socialno razsežnost (resnična in virtualna osebnost), ki sta neodvisni, a tesno medsebojno povezani.

Zaradi nenehnega razvoja znanosti in tehnologije bo ta pogled v prihodnje revidiran in posodobljen.

### II. Uvod

Slovenija je v celoti zavezana spodbujanju spoštovanja mednarodnega prava, tudi v povezavi z vsemi kibernetnimi dejavnostmi. Slovenija priznava vse večji pomen in vpliv dejavnosti v kibernetnem prostoru na ozemljih držav in zunaj njih ter potrebo po zagotavljanju učinkovite rabe mednarodnega prava na tem področju.<sup>1</sup>

Slovenija ugotavlja, da sta skupina vladnih strokovnjakov ZN (SVS ZN) za razvoj na področju informatike in telekomunikacij v povezavi z mednarodno varnostjo in odprta delovna skupina ZN ponovno potrdili možnost uporabe mednarodnega prava v primerih, ko kibernetni prostor uporabljajo države.<sup>2</sup> Slovenija meni, da veljavno mednarodno pravo vključuje vse veje mednarodnega prava, med drugim pravo o uporabi sile, mednarodno humanitarno pravo (MHP), mednarodno pravo človekovih pravic (MPČP) in mednarodna pravila o odgovornosti držav.

---

<sup>1</sup> Resolucija GS ZN A/RES/79/1 (2024): »Pakt za prihodnost«, 33. odstavek.

<sup>2</sup> Poročilo skupine vladnih strokovnjakov o razvoju na področju informatike in telekomunikacij v povezavi z mednarodno varnostjo, dokument ZN A/68/98 (2013), sprejeto z Resolucijo GS ZN A/RES/68/243; poročilo skupine vladnih strokovnjakov o razvoju na področju informatike in telekomunikacij v povezavi z mednarodno varnostjo, dokument ZN A/70/174 (2015), sprejeto z Resolucijo GS ZN A/RES/70/237; poročilo odprte delovne skupine za razvoj na področju informatike in telekomunikacij v povezavi z mednarodno varnostjo, dokument ZN A/75/816 (2021); poročilo skupine vladnih strokovnjakov o spodbujanju odgovornega ravnanja držav v kibernetnem prostoru v povezavi z mednarodno varnostjo, dokument ZN A/76/135 (2021); poročilo odprte delovne skupine o varnosti informacijsko-komunikacijskih tehnologij in njihove uporabe 2021–2025, dokument ZN A/77/275 (2022); poročilo odprte delovne skupine o varnosti informacijsko-komunikacijskih tehnologij in njihove uporabe 2021–2025, dokument ZN A/79/214 (2024); Res. GS ZN A/RES/75/240 (2021); Res. GS ZN A/RES/78/265 (2024); Res. GS ZN A/RES/79/237 (2024).

Dodatno pojasnilo je potrebno predvsem v zvezi s tem, kako se mednarodno pravo uporablja v kibernetickem prostoru. Slovenija meni, da pri kibernetickem prostoru ne gre za novo pravno področje, temveč nekaj, kar vpliva na predmete in osebe na obstoječih področjih (kopno, morje, zrak in vesolje). Zato je treba načela in pravila mednarodnega prava, ki se nanašajo na slednje, uporabljati v povezavi s kibernetickim prostorom.

Slovenija želi z objavo nacionalnega pogleda prispevati k razpravi o uporabi mednarodnega prava v kibernetickem prostoru.

### III. Suverenost

Za dejavnosti držav v kibernetickem prostoru<sup>3</sup> se uporablja temeljno pravno načelo državne suverenosti, ki je uveljavljeno načelo mednarodnega običajnega prava.<sup>4</sup> Države izvajajo ozemeljsko suverenost nad kiberneticko infrastrukturo in posamezniki, ki se ukvarjajo s kibernetickimi dejavnostmi na njihovem ozemlju, kar obsega pravice do reguliranja, uveljavljanja in jurisdikcije. Slovenija zagovarja stališče, da ta suverenost zajema vso kiberneticko infrastrukturo in dejavnosti, ne glede na to, ali je ta infrastruktura javna ali zasebna last. Slovenija je tudi mnenja, da je od narave in učinka kibernetiske dejavnosti odvisno, ali ta krši suverenost, kar je treba oceniti za vsak primer posebej.

Na splošno se kršitev suverenosti, ki ima za posledico fizično škodo ali poškodbo, začasno ali trajno izgubo funkcionalnosti ali motnjo ali uzurpacijo inherentno vladnih funkcij države, z namenom povzročiti tako škodo, da šteje za mednarodno protipravno dejanje<sup>5</sup>, za katerega je odgovorna tista država, ki ji je mogoče pripisati tako kiberneticko dejanje. Na primer, kiberneticka dejavnost, ki povzroči škodo ali izgubo funkcionalnosti državne infrastrukture, se šteje za kršitev ozemeljske suverenosti. Za kršitev suverenosti se lahko šteje tudi nepooblaščen vdor, ki vpliva na podatke ali storitve, nujne za delovanje vlade.<sup>6</sup>

### IV. Načelo nevmešavanja

Načelo nevmešavanja kot temeljno načelo mednarodnega prava, ki je trdno zasidrano v mednarodnem običajnem pravu<sup>7</sup>, velja le za odnose med državami ali med državami in mednarodnimi organizacijami, ne pa za odnose med nedežavnimi akterji in državo.

Prepoved vmešavanja obsega dvoje: poseganje v suverene pristojnosti, tj. notranje ali zunanje zadeve ali zadeve, ki so po naravi vladne in o katerih lahko vsaka država odloča svobodno, ter prisila. Prepovedano vmešavanje torej pomeni neposredno ali posredno poseganje v notranje ali zunanje zadeve druge države z uporabo prisilnih sredstev, in sicer

<sup>3</sup> Poročilo SVS ZN A/68/98 (2013), 20. odstavek; Poročilo SVS ZN A/70/174 (2015), 27.–28. odstavek, potrjeno z Res. GS ZN A/RES/70/237 (2015); poročilo Odprte delovne skupine ZN A/79/214 (2024), 37. odstavek.

<sup>4</sup> Res. GS ZN 2625 (XXV) *Deklaracija o načelih mednarodnega prava o prijateljskih odnosih in sodelovanju med državami* (1970); Vojaške in paravojaške dejavnosti v Nikaragvi in proti njej (Nikaragva proti Združenim državam Amerike). [1986] Poročilo ICJ 14, 202. in 205. odstavek; Oborožene dejavnosti na območju Konga (Demokratska republika Kongo proti Ugandi). [2005] Poročilo ICJ 168, 164. odstavek.

<sup>5</sup> Kot je opredeljeno v ARSIWA, 20.–27. člen.

<sup>6</sup> Talinski priročnik 2.0, Cambridge University Press, 2017, pravilo 4, 15. odstavek.

<sup>7</sup> ICJ Nikaragva, 191.–192., 205. odstavek; ICJ Oborožene dejavnosti DR Kongo proti Ugandi (2005), 162.–163. odstavek.

tudi v njen gospodarski, politični, kulturni in socialni sistem ter zunanjo politiko. Za prepovedano vmešavanje se šteje vsako dejanje, katerega namen je onemogočiti ali omejiti pristojnosti tarčne (oškodovane) države.

Kibernetske dejavnosti se po mednarodnem pravu štejejo za prepovedano vmešavanje, če so po obsegu in učinku primerljive z vmešavanjem zunaj kibernetskega okolja. Prisilna sredstva so tista, s katerimi se državi namerno odvzame zmožnost nadzora, odločanja ali upravljanja zadev, ki so sicer izrecno v pristojnosti vlade. Namen vmešavanja kot takega bi torej bil spremeniti ravnanje tarčne države. Na primer, z uporabo kibernetskih sredstev bi spodkopali zmožnost države, da zagotavlja kritične storitve, ali manipulirali njene notranje postopke.

V kibernetskem prostoru se poseganje ne šteje vedno za vmešavanje. Kibernetsko dejanje poseganja se lahko šteje za prepovedano vmešavanje, samo če vsebuje element prisile. Prisilo je treba razlikovati od drugih dejanj, ki jih ni mogoče opredeliti kot prisilo, kot so na primer kritika, uvedba omejevalnih ukrepov, sankcije ali drugi načini vplivanja z miroljubnimi ali diplomatskimi sredstvi. Ali gre v kibernetskem prostoru za prisilo, je treba presoditi v vsakem primeru posebej in pri tem upoštevati dane okoliščine.

## **V. Prepoved grožnje s silo ali uporabe sile**

Četrty odstavek 2. člena Ustanovne listine ZN in mednarodno običajno pravo državam prepovedujeta uporabo groženj s silo ali uporabo sile zoper ozemeljsko celovitost ali politično neodvisnost katere koli države ali drugega tovrstnega ravnanja, ki ni skladno s cilji ZN. Ta prepoved ima status peremptorne norme (*jus cogens*).<sup>8</sup> Stvarno področje uporabe prepovedi ni omejeno na manj hude kršitve, npr. kršitev suverenosti ali prepovedano vmešavanje, ali na nekatere hude kršitve, npr. oborožen napad. Ta prepoved velja za uporabo sile v kakšni koli obliki, ne glede na uporabljeno orožje ali sredstva,<sup>9</sup> zato vključuje tudi kibernetske operacije.

Slovenija meni, da sta v kibernetskem prostoru za presojo, ali kibernetska operacija pomeni prepovedano uporabo sile, ki presega kršitev suverenosti, ali prepovedano nevmešavanje, merodajna obseg in učinek kibernetske operacije in ne uporabljena sredstva. Pri presoji, ali kibernetska operacija pomeni kršitev prepovedi uporabe sile, je zato treba v vsakem posameznem primeru oceniti njen obseg in učinek v danih okoliščinah, med drugim težo takega dejanja ali dejanj glede na obseg in učinek, ne pa glede na uporabljena sredstva.<sup>10</sup> Kibernetsko dejavnost bi lahko opredelili kot uporabo sile, če bi bila po obsegu in učinku primerljiva z uporabo sile v dejavnostih zunaj kibernetskega prostora.<sup>11</sup> V skladu s tem se kibernetska operacija ali kibernetska grožnja

<sup>8</sup> ICJ Nikaragva (1986), 175.–176., 188.–190. odstavek; ICJ Oborožene dejavnosti DR Kongo proti Ugandi (2005), 164.–165. odstavek.

<sup>9</sup> Legalnost grožnje z jedrskim orožjem ali njegove uporabe (svetovalno mnenje), [1996] Poročilo ICJ 226, 39. odstavek.

<sup>10</sup> Resolucija GS ZN 3314 (XXIX) *Opredelitev agresije* (1974), 2. odstavek; ICJ Nikaragva (1986), 195. odstavek; ICJ Oborožene dejavnosti DR Kongo proti Ugandi (2005), 163.–164. odstavek.

<sup>11</sup> V skladu s Talinskim priročnikom 2.0 (pravilo 69 in spremni komentar) je pri oceni obsega in učinkov kibernetske operacije pomembnih več dejavnikov, med katerimi so tudi posledice kibernetske operacije, ali je operacija vojaške narave in ali jo izvaja država.

šteje za grožnjo s silo, kadar se kibernetična grožnja, če bi bila izvedena, izkaže za uporabo sile.

Manjša kibernetična motnja sama po sebi ne pomeni uporabe sile, kibernetične operacije, ki povzročijo fizično škodo ali poškodbe, pa bi običajno opredelili kot uporabo sile. Tudi kibernetične operacije z izključno nefizičnimi učinki lahko v nekaterih okoliščinah pomenijo uporabo sile.

Pomenljiv kazalnik, da je dosežen prag uporabe sile, je namerno ciljanje kritične infrastrukture.<sup>12</sup>

Slovenija bo v vsakem posameznem primeru preučila tiste kibernetične operacije, ki lahko pomenijo grožnjo s silo ali uporabo sile, in za vsak primer posebej ugotavljala, ali so 'obseg in učinki'<sup>13</sup> taki, da kibernetična operacija pomeni kršitev prepovedi uporabe sile ali da kibernetična grožnja pomeni grožnjo s silo.

## **VI. Mednarodno humanitarno pravo (MHP)**

Za uporabo številnih omejitev in prepovedi po MHP v povezavi s kibernetičnimi operacijami je ključna razlaga pojma »napad«, kot je opredeljen v MHP/pravu oboroženih spopadov. Kibernetični napad je ofenzivna ali defenzivna kibernetična operacija, za katero se lahko upravičeno pričakuje, da bo povzročila poškodbe ali smrt ljudi ali poškodovanje ali uničenje objektov. To vključuje vsako posledično škodo, uničenje, poškodbo ali smrt, ki jo je mogoče razumno predvideti. Slovenija meni, da se po MHP kot napad lahko opredeli tudi izguba funkcionalnosti, če je po učinku dovolj uničujoč. To stališče je skladno s splošno sprejetim izhodiščem, da se pri oceni, ali je bil dosežen prag napada, ne upošteva, katere vrste orožja in sredstva so bila uporabljena.

Pravila in načela, ki urejajo izvajanje sovražnosti, je treba spoštovati tudi v kibernetičnem prostoru.<sup>14</sup> MHP in njegova temeljna načela – vključno s humanostjo, vojaško nujnostjo, razlikovanjem, sorazmernostjo in previdnostnimi ukrepi – se uporabljajo za kibernetične operacije med oboroženimi spopadi ali okupacijo, če se te operacije izvajajo v okviru takšnega spopada ali okupacije ali če same po sebi izzovejo uporabo MHP.<sup>15</sup> MHP zagotavlja tudi posebno zaščito za osebe ali objekti, med katerimi so tudi zdravstvene službe in prevozna sredstva, kulturna dediščina, naravno okolje, zgradbe in naprave, ki vsebujejo nevarne sile, ter objekti, ki so nujni za preživetje civilnega prebivalstva. Slovenija meni, da priznanje uporabe MHP za kibernetične operacije nikakor ne upravičuje kibernetičnega vojskovanja in ne spodbuja militarizacije kibernetičnega prostora.

Ker so v kibernetičnem prostoru drugačni predmeti kot v fizičnem prostoru, se uporaba MHP nanaša na vse sestavine kibernetičnega prostora, tudi na podatke. Slovenija meni,

---

<sup>12</sup> Trenutno ni mednarodno priznane opredelitve kritične infrastrukture. Zato bi bilo v pomoč, če bi opredelili obseg in učinke kibernetične dejavnosti.

<sup>13</sup>[C] Nikaragva (1986), 195. odstavek.

<sup>14</sup> Na podoben način veljajo človekove pravice tako v fizičnem kot v virtualnem svetu. Za več informacij glej besedilo spodaj.

<sup>15</sup> Vendar je treba opozoriti, da večina kibernetičnih dejavnosti ni povezana z oboroženim spopadom, kar izključuje uporabo MHP.

da se podatki ne štejejo za predmete, saj predmet razumemo kot nekaj vidnega in otipljivega. Nekatere kibernetске operacije zoper podatke so kljub temu prepovedane. Civilni podatki so zaščiteni pred kibernetскими napadi v primerih, ko se upravičeno lahko pričakuje, da bi ponarejanje, poškodovanje ali izbris takih podatkov povzročil poškodbe ali smrt oseb ali poškodovanje ali uničenje predmetov. Prepovedano je tudi manipuliranje s podatki, ki bi ogrozilo delovanje zdravstvenih služb ali nepristranskih humanitarnih organizacij.

Načelo razlikovanja narekuje razlikovanje med civilnimi objekti in vojaškimi cilji ter med civilisti in borci. Slednji vključujejo tudi *levée en masse*, torej prebivalce nezasedenega ozemlja, ki ob približevanju sovražnika spontano poprimejo za orožje in se uprejo okupatorju, nimajo pa časa, da bi se organizirali v redne oborožene sile. Zaradi možnosti, ki so na voljo v kibernetickem vojskovanju, lahko odpor proti okupatorju vključuje tudi vojaške operacije proti ciljem, ki so globoko na sovražnikovem ozemlju.

Če civilisti sodelujejo pri kibernetickih dejanjih, ki se štejejo za neposredno sodelovanje v sovražnostih, izgubijo zaščiteni status po MHP. To se lahko zgodi, kadar civilisti izvajajo napadalne kibernetické operacije, da bi vplivali na vojaške dejavnosti ali zmogljivosti, ali obrambne operacije, namenjene zaščiti lastnih vojaških ciljev. Civilisti, ki sodelujejo v takšnih akcijah, morajo biti seznanjeni s pravnimi posledicami svojega sodelovanja ter s pravili in načeli MHP, ki jih morajo upoštevati. Otrokom se ne sme dovoliti, da neposredno sodelujejo v kibernetickih sovražnostih.<sup>16</sup>

Slovenija je prepričana, da bi moralo nadaljnje delo na področju uporabe MHP v kibernetickem prostoru temeljiti na obstoječem pravnem okviru ter ga krepiti in spodbujati ob zavedanju, kakšni so izzivi v kibernetickem prostoru.

## **VII. Mednarodno pravo človekovih pravic (MPČP)**

Slovenija je v celoti zavezana uresničevanju človekovih pravic. MPČP velja tudi za kibernetické dejavnosti.

Države so dolžne v enaki meri v fizičnem in virtualnem svetu spoštovati in varovati človekove pravice posameznikov ter izpolnjevati prevzete obveznosti na področju človekovih pravic, kot je določeno v veljavnih mednarodnih pogodbah o človekovih pravicah in nacionalnem pravu.<sup>17</sup>

Kibernetické dejavnosti lahko vplivajo na vse človekove pravice. Med pravicami in svoboščinami, ki so lahko še posebej izpostavljene, so svoboda izražanja, svoboda vesti, pravica do zasebnosti, komunikacijska zasebnost, varstvo osebnih podatkov, pravica do zbiranja in združevanja ter enakost pred zakonom. Kot potrjuje mednarodna sodna

---

<sup>16</sup> Konvencija ZN o otrokovih pravicah (1989) Izbirni protokol (2000) 1. in 5. člen.

<sup>17</sup> Pravica do zasebnosti v digitalni dobi, Resolucija Generalne skupščine 68/167, 3. odstavek, dokument ZN A/RES/68/167 (december 2013).

praksa, morajo države ob upoštevanju zakonitih izjem in omejitev tudi v kibernetnem prostoru zagotoviti uživanje teh pravic brez razlikovanja.<sup>18</sup>

Če kibernetna dejavnost povzroči kršitev človekovih pravic in jo je mogoče pripisati neki državi, morajo biti žrtvi na voljo pritožbeni mehanizmi, ki jih ob taki kršitvi zagotavljajo veljavno nacionalno pravo in mednarodne pogodbe, katerih pogodbenica je država. Slovenija podpira delo mednarodnih organov in mehanizmov za področje človekovih pravic, ki razvijajo ustrezne pristope glede spoštovanja in zaščite ter izpolnjevanja obveznosti držav na področju človekovih pravic v kibernetnem prostoru.

Kibernetne dejavnosti lahko zajamejo kibernetno infrastrukturo več držav, zato se lahko ob posegu v človekove pravice pojavijo spori glede pristojnosti. Slovenija ponovno poudarja stališče Odbora ZN za človekove pravice<sup>19</sup> glede ekstrateritorialne uporabe človekovih pravic, kadar neka država izvaja oblast ali dejanski nadzor zunaj svojega ozemlja, vključno s funkcionalno pristojnostjo, kadar je to primerno, in sicer z nujnimi prilagoditvami za kibernetni prostor.

## **VIII. Kibernetna kriminaliteta**

Konvencija Sveta Evrope o kibernetni kriminaliteti (ETS 185) in njeni dodatni protokoli priznavajo pomembnost skupnih standardov pri opredelitvi kibernetne kriminalitete, pri urejanju postopkovnih pooblastil za preiskovanje in pregon ter pri omogočanju mednarodnega sodelovanja v zvezi s čezmejnimi primeri kibernetne kriminalitete in zbiranjem dokazov v elektronski obliki v tujini.

Konvencija je globalnega pomena, saj je prva vzpostavila jasne standarde na navedenem področju, njena uporaba pa ni omejena na države članice Sveta Evrope.

Konvencija ZN o kibernetni kriminaliteti (2024, še ne velja) obravnava vprašanje kibernetne kriminalitete na globalni ravni in zagotavlja okvir za meddržavno sodelovanje na področju kazenskega pravosodja in izvrševanje prava. Po vsebini v veliki meri izhaja iz opredelitev Konvencije Sveta Evrope in je z njo skladna, enako kot s Konvencijo ZN proti mednarodnemu organiziranemu kriminalu.

## **II. DEL**

### **I. Odgovornost držav**

---

<sup>18</sup> Tudi Evropsko sodišče za človekove pravice (ESČP) je razvilo svojo prakso v zvezi s kršitvami človekovih pravic v kibernetnem prostoru. ESČP je poudaril pomen pozitivne obveznosti države, da razišče spletne kršitve (kazniva dejanja) osebnostnih pravic žrtve. V več primerih vmešavanja države s tajnim nadzorom in množičnim prestrežanjem se je sodišče osredotočilo na pravico do zasebnosti in določilo pogoje, ki morajo biti izpolnjeni za zakonito poseganje in zaščitne ukrepe. V primeru *Wieder in Guarnieri* (2023) je na primer potrdilo veljavnost EKČP in njegovih ustreznih protokolov za vse ekstrateritorialne nadzorne dejavnosti, zato morajo evropske obveščevalne agencije opraviti test sorazmernosti/legitimnosti pri pridobivanju, obdelavi ali manipulaciji podatkov tujih posameznikov. ESČP je ugotovil, da so vsebine, ki jih na spletu ustvarjajo uporabniki, platforma brez primere za uresničevanje svobode izražanja, in izrazil mnenje, da je blokiranje dostopa do spleta lahko v neposrednem nasprotju s svobodo izražanja. V meddržavni zadevi *Ukrajina in Nizozemska proti Rusiji* (2022) je ta neuspešno zagovarjala stališče, da je kibernetne napade na odvetniško pisarno, ki jo je zastopala v postopku, mogoče pripisati tožečim državam, in s tem izrazila domnevo, da vloga ni pristna.

<sup>19</sup> Splošna komentarja 31 in 36 Odbora za človekove pravice.

Slovenija potrjuje, da se splošna pravila in načela, ki urejajo odgovornost držav za mednarodno protipravna dejanja – kot so zapisana v mednarodnem običajnem pravu in Členih Komisije za mednarodno pravo o odgovornosti držav za mednarodna protipravna dejanja (ARSIWA)<sup>20</sup> – uporabljajo tudi za ravnanje držav v kibernetskem prostoru.

Kibernetska dejavnost se lahko šteje za mednarodno protipravno dejanje, če se to ravnanje po ARSIWA lahko pripiše državi in če to ravnanje pomeni kršitev mednarodne obveznosti te države. V primeru ugotovitve teh dejstev odgovorna država nosi pravne posledice v skladu z ARSIWA – vključno s prenehanjem, zagotovili in jamstvi, da se to ne bo ponovilo, ter celotnim nadomestilom škode.<sup>21</sup> Če tako ravnanje pomeni hudo kršitev obveznosti, ki izhaja iz peremptorne norme splošnega mednarodnega prava, se upoštevajo tudi posebne posledice v skladu z ARSIWA.<sup>22</sup>

Slovenija opozarja tudi, da sekundarna pravila iz ARSIWA veljajo skupaj z ustreznimi primarnimi pravili mednarodnega prava (vključno z Ustanovno listino OZN) in da si je treba pri ocenjevanju odgovornosti držav na kibernetskem področju okoliščine, ki izključujejo možnost protipravnosti, pravila o pomoči ali podpori in o protiukrepih razlagati skupaj s pravili o pripisu odgovornosti in posledicah.

### **A) Pripis odgovornosti za kibernetske dejavnosti**

Slovenija priznava, da je pripis odgovornosti bistven za ugotavljanje odgovornosti držav po mednarodnem pravu in zato sestavni del širšega okvira mednarodne odgovornosti, ki se uporablja kot vodilo za pravna sredstva in skupen politični odziv.

Slovenija potrjuje, da obstoječe mednarodno pravo, vključno s Členi Komisije za mednarodno pravo o odgovornosti držav za mednarodno protipravna dejanja (ARSIWA)<sup>23</sup>, se uporablja v kibernetskem prostoru in zanj.<sup>24</sup> V skladu z ARSIWA se bo kibernetska dejavnost štela za mednarodno protipravno dejanje le, (1) če je tako ravnanje mogoče pripisati državi po pravilih o pripisu odgovornosti iz ARSIWA in (2) če tako ravnanje krši veljavno mednarodno obveznost.<sup>25</sup>

Slovenija ugotavlja, da je *pripis politične odgovornosti* javno-politična presoja, ki temelji na tehtanju razpoložljivih tehničnih, obveščevalnih in pravnih dokazov ter je podana kot ocena zaupanja, katere namen je omogočiti sankcije, diplomatske ukrepe in koalicijsko

<sup>20</sup> Besedilo Členov Komisije za mednarodno pravo o odgovornosti držav za mednarodna protipravna dejanja (ARSIWA) (2001), vključno z zgoraj navedenimi členi (2., 4.–11., 16.–18., 20.–31., 40.–41. člen).

<sup>21</sup> Vojaške in paravojaške dejavnosti (Nikaragva proti Združenim državam Amerike) – ICJ, meritorna odločitev (1986) (vodilna razlaga o pripisu odgovornosti/»učinkovitem nadzoru« in praksi državne odgovornosti).

<sup>22</sup> Uporaba Konvencije o preprečevanju in kaznovanju zločina genocida (Bosna in Hercegovina proti Srbiji in Črni gori) – ICJ, sodba (2007) (o pripisu odgovornosti, pomoči/sodelovanju in dokaznih standardih v primerih hudih mednarodnih nezakonitosti).

<sup>23</sup> Komisija za mednarodno pravo, *Členi Komisije za mednarodno pravo o odgovornosti držav za mednarodna protipravna dejanja s komentarji*, v poročilu *Komisije za mednarodno pravo*, 53. zasedanje, dokument ZN A/56/10 (2001), zbornik, zvezek II (drugi del).

<sup>24</sup> Glej tudi glavno analizo v *Talinskem priročniku 2.0* o mednarodnem pravu za kibernetske operacije, ki uporablja in razlaga ta načela v kibernetskem prostoru; Michael N Schmitt (ur.), *Talinski priročnik 2.0 o mednarodnem pravu za kibernetske operacije* (Cambridge University Press, 2017) (Talinski priročnik 2.0) pravilo 14 (o mednarodno protipravnih kibernetskih dejanjih) (84. stran) (nezavezujoč strokovni komentar).

<sup>25</sup> KMP, *Členi o odgovornosti držav za mednarodna protipravna dejanja* (ARSIWA) 2. člen; glej 4.–8., 11. člen.

delovanje. *Pripis tehnične odgovornosti* se opira na forenzično poreklo in vedenjske vzorce (zlonamerna programska oprema, indikatorji kompromitiranja (IOC), taktike, tehnike in postopki (TTP)).<sup>26</sup> *Pripis pravne odgovornosti* je jasna pravna ugotovitev, da dejstva kažejo na pravno povezavo, ki zadošča za pripis odgovornosti v skladu z ARSIWA, posledica tega pa so obveznosti in pravna sredstva po mednarodnem pravu.<sup>27</sup>

Slovenija meni, da lahko pripis odgovornosti po ARSIWA med drugim izhaja iz ravnanja državnih organov (4. člen), oseb ali subjektov, ki izvajajo državno oblast (5. člen), organov, ki so na razpolago drugi državi (6. člen), dejanj *ultra vires* organov, ki delujejo po uradni dolžnosti (7. člen), ravnanja, ki ga usmerja ali nadzoruje država (8. člen), ravnanje oseb, ki v odsotnosti ali ob neizpolnjevanju nalog uradnih oblasti izvršujejo elemente javne oblasti, ter v okoliščinah, ki zahtevajo izvrševanje teh elementov oblasti (9. člen), ali ravnanja, ki ga država priznava in sprejema za svoje (11. člen). Ko država zagotavlja infrastrukturo, pomoč ali navodila z vednostjo o protipravnih okoliščinah, se ji lahko pripiše tudi posredna odgovornost (16. in 17. člen).<sup>28</sup>

Slovenija ugotavlja, da različna sodišča in razsodišča uporabljajo različne preskuse nadzora (zlasti preskus *učinkovitega nadzora* ICJ v zadevi *Nikaragva*<sup>29</sup> in širša formulacija *skupnega nadzora* Mednarodnega kazenskega sodišča za nekdanjo Jugoslavijo (MKS) v zadevi *Tadić*<sup>30</sup>); tožnik mora opredeliti veljavni standard in dokazati zahtevano dejansko povezavo in vzročno zvezo med pripisanim ravnanjem in domnevno škodo (glej zadevo *Bosna in Hercegovina proti Srbiji in Črni gori*<sup>32</sup> o vzročni povezavi).

V kibernetnem prostoru se države zato zanašajo na večplastne dokaze, ki se medsebojno podpirajo – tehnično forenziko (dnevniki, analiza zlonamerne programske opreme,

---

<sup>26</sup> Z *zlonamerno programsko opremo* so mišljeni zlonamerna programska oprema, ki se uporablja za vdor, dolgotrajni napadi, iznos podatkov ali motnje (npr. binarne datoteke, skripti, koristni tovor). *Indikatorji kompromitiranja (IOC)* so zaznavni artefakti, ki razkrivajo kompromitiranje ali infrastrukturo napadalca (npr. naslovi IP, domene, zgoščene vrednosti datotek (hash), kazalniki omrežja ali končne točke C2). *Taktike, tehnike in postopki (TTP)* opisujejo značilne metode in vedenjske vzorce akterja (operativni priročnik, po katerem se izvajajo napadi). Pripis tehnične odgovornosti se opira na te kategorije, da se odkrije izvor in poveže incidente s kampanjami, toda taki tehnični kazalniki sami po sebi niso odločilni za pravno odgovornost, čeprav so dokazni. Glej Talinski priročnik 2.0 (Michael N Schmitt (ur.)), pravilo 15 in spremni komentar (87.–90. stran) (o vlogi in omejitvah forenzičnih kazalnikov pri pripisu odgovornosti) ter praktična navodila o predstavitvi dokazov (118.–121. stran).

<sup>27</sup> Glej *Talinski priročnik 2.0* o navodilih glede dokazov in pripisa odgovornosti v zvezi s kibernetnimi operacijami; Michael N Schmitt (ur.), *Talinski priročnik 2.0* (n 27) pravilo 15 (Pripis odgovornosti za kibernetne operacije državnim organom) in spremni komentar (87.–90. stran) (o forenzičnih kazalnikih, dokazni vrednosti tehničnih podatkov in omejitvah pri dokazovanju izvora za pripis pravne odgovornosti).

<sup>28</sup> Glej Diplomatsko in konzularno osebje ZDA v Teheranu (ZDA proti Iranu) [1980], Poročilo ICJ 3 (sodba z dne 24. maja 1980), 69.–75. odstavek (Sodišče zabeleži trditev Združenih držav o »sostoritstvu« in »odobritvi« Irana ter preuči dejansko podlago vpletenosti države). Iz tega gradiva je razvidno, da je odobritev ali potrditev države lahko pomembno dejstvo v preiskavi za ugotavljanje odgovornosti, vendar je od konkretnih dejstev in stopnje vpletenosti države odvisno, ali takšno ravnanje pomeni pravno »priznanje in sprejetje«; v nasprotju s tem so v skladu z ARSIWA potrebni nedvoumni dokazi, da je država dejanje »priznala in sprejela« kot svoje, poznejša sodna praksa pa je poudarila, da naknadna potrditev, napredovanje ali nagrada ne dosega nujno tega visokega praga (glej Makuchyan & Minasyan proti Azerbajdžanu in Madžarski, pritožba št. 17247/13 (ESČP, 26. maj 2020), 112.–18. odstavek).

<sup>29</sup> Sodišče pojasni prag »učinkovitega nadzora« in dejstvo, da samo financiranje/opremljanje ne zadostuje za pripis odgovornosti za dejanja, če ni dokazov, da je država »usmerjala ali izvrševala izvedbo« zadevnih operacij; *Vojaške in paravojaške dejavnosti v Nikaragvi in proti njej (Nikaragva proti Združenim državam Amerike)* (meritorna sodba) ICJ, 27. junij 1986, 115.–16. odstavek.

<sup>30</sup> Pritožbeni senat je opredelil preskus »skupnega nadzora« in razpravljal o tem, kako se lahko zaradi skupnega nadzora dejavnosti skupine pripišejo državi; *Tožilec proti Dušku Tadiću* (pritožbeni senat) zadeva št. IT-94-1-A (15. julij 1999), 120.–23. odstavek.

<sup>31</sup> *Talinski priročnik 2.0* obravnava te standarde nadzora in njihovo uporabo v kibernetnem prostoru. Je uporabna praktična referenca za primerjavo dejanskih vzorcev s pravnimi preskusi; Michael N Schmitt (ur.), *Talinski priročnik 2.0* (n 27) pravilo 17 in komentar (94.–97. stran) (o pripisu odgovornosti nedržavnim akterjem in razlikovanju med »dejanskim nadzorom« in »skupnim nadzorom« ter navodila za uporabo preskusov nadzora v kibernetnih primerih).

<sup>32</sup> Sodišče poudarja, da je pri ugotavljanju odgovornosti in odškodnin potrebna »dovolj neposredna in nedvoumna vzročna povezava med protipravnim dejanjem ... in povzročeno škodo«; *Uporaba Konvencije o preprečevanju in kaznovanju zločina genocida (Bosna in Hercegovina proti Srbiji in Črni gori)* (meritorna sodba) ICJ, 26. februar 2007, 462. odstavek.

indikatorji kompromitiranja (IOC), taktike, tehnike in postopki (TTP))<sup>33</sup>, ocene obveščevalnih služb, analizo vedenja in dokumentarne dokaze o usmerjanju, nadzoru ali pomoči – ter javno navedejo stopnjo zanesljivosti svoje ocene, hkrati pa zaščitijo zaupne vire in metode.<sup>34</sup>

## B) Kršitev mednarodnih obveznosti

O kršitvi govorimo, ko lahko neki državi v kibernetičnem prostoru pripišemo ravnanje, ki je v nasprotju z mednarodnopravnimi obveznostmi te države. V skladu z ARSIWA se za mednarodno protipravno dejanje šteje, (1) če je tako ravnanje mogoče pripisati tej državi in (2) če tako ravnanje pomeni kršitev obveznosti, ki velja za to državo. V kibernetičnem prostoru lahko ustrezna primarna pravila – odvisno od okoliščin – vključujejo prepoved uporabe sile<sup>35</sup>, načelo nevmešavanja<sup>36</sup>, dolžnost spoštovanja državne suverenosti<sup>37</sup>, obveznosti iz mednarodnih pogodb in veljavne obveznosti na področju človekovih pravic. Uporaba določenega primarnega pravila je odvisna od obsega, učinkov in okoliščin operacije. Za ugotovitev kršitve je zato treba pripisano ravnanje pravno opredeliti glede na ustrezno primarno pravilo oz. pravila, v primeru zahtevkov za odškodnino pa dokazati vzročno zvezo med pripisanim ravnanjem in domnevno škodo ali izgubo.<sup>38</sup>

Pri javni izjavi o pripisu odgovornosti se pravna ocena vlade opira na tehtanje razpoložljivih dokazov – ki vključujejo tehnične forenzične podatke (sistemski dnevnik in dnevnik aplikacij; analiza zlonamerne programske opreme), povezanost taktik, tehnik in postopkov (TTP), obveščevalna poročila (vključno s prestreženo komunikacijo in poročanjem človeških virov, kjer je to primerno), dokaze o državnem usmerjanju, nadzoru ali materialni podpori ter kakršno koli podprto javno ali odprtokodno gradivo – in ocene, da ti dokazi skupaj zadoščajo za ugotovitev obstoja kršitve navedenih mednarodnih obveznosti.<sup>39</sup>

<sup>33</sup> *Dnevnik* so sistemski in omrežni zapisi, ki se uporabljajo v forenzični rekonstrukciji (npr. dnevnik gostitelja/dogodkov, dnevnik požarnega zidu/posredniškega strežnika, zajeti paketi in drugi zapisi s časovnim žigom, ki razkrivajo povezave, procese in sistemske dogodke). *Analiza zlonamerne programske opreme* se nanaša na statično in dinamično preučevanje zlonamerne kode (povratno inženirstvo, peskovnik in analiza vedenja) za ugotavljanje zmogljivosti, artefaktov kodiranja in ponovne uporabe. *Indikatorji kompromitiranja (IOC)* so zaznavni artefakti, ki razkrivajo kompromitiranje ali infrastrukturo napadalca (npr. zgoščene vrednosti datotek (hash), naslovi IP, domenska imena, certifikati SSL, registrski ključi). *Taktike, tehnike in postopki (TTP)* pomenijo značilne vedenjske vzorce in metode delovanja akterja (»način« vtorov, ki povezuje incidente s kampanjami). Te tehnične kategorije dokazujejo izvor in povezave, toda, kot pojasnjuje Talinski priročnik 2.0, so bolj kazalniki, niso pa odločilne za pripis pravne odgovornosti; tehnične dokaze je treba predstaviti kot del večplastnega, podprtega zapisa skupaj z obveščevalnimi podatki in dokumentarnimi dokazi. Glej Talinski priročnik 2.0 (Michael N Schmitt (ur.), *Talinski priročnik 2.0 o mednarodnem pravu za kibernetične operacije* (Cambridge University Press, 2017), pravilo 15 (87.–90. stran) in praktična navodila o predstavitvi dokazov (118.–121. stran).

<sup>34</sup> Ti večplastni dokazni pristopi so skladni s praktičnimi smernicami iz *Talinskega priročnika 2.0* o zbiranju in predstavitvi dokazov za pripis odgovornosti v kibernetičnih incidentih; Michael N Schmitt (ur.), *Talinski priročnik 2.0* (n 27) (glej zlasti praktične smernice o dokazih in predstavitvi ocen v zvezi s pripisom odgovornosti, vključno s priporočenimi kategorijami za razkritje nezaupnih podatkov in obveščanje partnerjev) (118.–121. stran).

<sup>35</sup> Ustanovna listina OZN, 4. odstavek 2. člena (prepoved uporabe sile); glej tudi Michael N Schmitt (ur.), *Talinski priročnik 2.0 o mednarodnem pravu za kibernetične operacije* (Cambridge University Press, 2017) (nezavezujoč strokovni komentar) (o pristopu k uporabi sile v kibernetičnem prostoru z vidika obsega/učinkov).

<sup>36</sup> Glej sodbo v zadevi *Vojaške in paravojaške dejavnosti (Nikaragva proti ZDA)*, (meritorna sodba) ICJ, 27. junij 1986 (o načelu nevmešavanja in s tem povezanih obveznostih držav).

<sup>37</sup> Glej sodbo v zadevi *Krfski kanal (Združeno kraljestvo proti Albaniji)*, (meritorna sodba) ICJ, 9. april 1949 (o državni suverenosti in spoštovanju ozemeljske celovitosti); glej tudi razpravo o suverenosti in nevmešavanju v Talinskem priročniku 2.0 (n 49).

<sup>38</sup> *Uporaba Konvencije o preprečevanju in kaznovanju zločina genocida (Bosna in Hercegovina proti Srbiji in Črni gori)*, (meritorna sodba) ICJ, 26. februar 2007, 462. odstavek (o potrebi po dovolj neposredni in nedvoumni vzročni povezavi med protipravnim ravnanjem in škodo, ki jo je treba nadomestiti).

<sup>39</sup> Glede kategorij dokazov in praktične predstavitve dokazov za pripis odgovornosti v kibernetičnih incidentih glej Talinski priročnik 2.0 (n 2), pravilo 15 in spremni komentar (tehnični kazalniki, TTP in omejitve pri dokazovanju izvora kot dokončni dokaz), ter praktična

## C) Dolžna skrbnost

Države so dolžne zagotoviti, da z njihovo vednostjo nihče ne uporablja njihovega ozemlja ali objektov, dejavnosti in infrastrukture pod njihovo jurisdikcijo za dejanja, ki kršijo pravice drugih držav.

Načelo dolžne skrbnosti od države zahteva, da sprejme izvedljive ukrepe v zvezi s kibernetiskimi dejavnostmi, če je seznanjena ali bi morala biti seznanjena z dejanjem, ki krši pravice države žrtve in izvira iz njenega ozemlja ali prek njega poteka. Če države ne morejo ustaviti take kibernetiske dejavnosti, morajo storiti vse, kar lahko, da jih omejijo in opozorijo tarčno državo. Načelo dolžne skrbnosti ne vključuje obveznosti uvedbe preventivnih ukrepov, s katerimi bi se zagotovilo, da ozemlje neke države ne bo uporabljeno tako, da bi to negativno vplivalo na pravice drugih držav. Države morajo samo izkazati dolžno skrbnost, in sicer tako, da sprejmejo smiselne ukrepe za prenehanje ali omejitev kibernetiskih dejavnosti, ki bi lahko imele resne negativne posledice.

## D) Kdaj kibernetiska dejavnost ni protipravna

Slovenija meni, da med okoliščine, v katerih ni mogoče govoriti o protipravnosti kibernetiske dejavnosti, spadajo soglasje, samoobramba, protiukrepi, nujnost, višja sila in nevarnost.

### Samoobramba

Če se kibernetiska operacija šteje za *oborožen napad* – tj. kibernetiska operacija preraste v kibernetiski oborožen napad –, lahko tarčna država uveljavi svojo pravico do uporabe sile v samoobrambi, individualni ali kolektivni, kot določata 51. člen Ustanovne listine OZN in mednarodno običajno pravo.<sup>40</sup> Oborožen napad je treba razlikovati od drugih oblik uporabe sile. Doseženi prag je po obsegu in učinkih višji kot pri manj resnih oblikah uporabe sile, zato je stvarno področje uporabe ustrezne pravice do samoobrambe ožje.<sup>41</sup>

Kibernetiska operacija, v kateri je resno poškodovanih ali ubitih več oseb ali povzročena znatna škoda ali uničenje premoženja, kot je napad na sistem kontrole zračnega prometa, posledica katerega je nesreča, ali napad na kritično infrastrukturo, ki povzroči resno fizično škodo, bi se štela za oborožen napad, saj bi bila po obsegu in učinkih primerljiva z oboroženim napadom s konvencionalnim orožjem. Niz kibernetiskih dejavnosti, ki posamično ne dosežajo praga oboroženega napada, se lahko opredeli kot oborožen napad, če njihove posledice po obsegu in učinkih skupno dosežejo prag za tako opredelitev. V primeru tuje kibernetiske operacije, ki se pripiše neki državi, mednarodni

---

navodila za zbiranje in predstavitev dokazov (118.–121. stran); glej tudi KMP (n 26) 16.–17. člen (pomoč/podpora; usmerjanje in nadzor – seznanjenost in elementi nadzora).

<sup>40</sup> Talinski priročnik 2.0, pravila 71–76 in spremni komentar.

<sup>41</sup> ICJ Nikaragva (1986), 50., 74., 176.–181., 193.–201., 210.–211., 232.–234., 238. odstavek; ICJ Oborožene dejavnosti DR Kongo proti Ugandi (2005), 118., 128., 142.–143., 144.–146. odstavek.

organizaciji ali nedržavnemu akterju, vendar ne izpolnjuje merila oboroženega napada, napadena država ne more uveljavljati pravice do samoobrambe.

## Protiukrepi

Če je neka država žrtev zlonamerne kibernetične operacije, ki jo je mogoče pripisati državi storilki, lahko tarčna država pod pogoji, ki jih določa mednarodno običajno pravo, sprejme protiukrepe.<sup>42</sup> Protiukrepi proti državi storilki so lahko po naravi kibernetični ali alternativni, vedno pa morajo biti v skladu s standardi, določenimi v veljavnem mednarodnem pravu, kot je na primer začasna oprostitev nekaterih obveznosti iz dvostranskih pogodb za obdobje, ko država storilka ne izpolnjuje mednarodnih obveznosti, in sicer če se lahko s takimi ukrepi doseže, da država storilka začne izpolnjevati prekršene mednarodne obveznosti, če so taki ukrepi sorazmerni in če niso prepovedani po mednarodnem pravu. Protiukrepi v zvezi s kibernetičnimi operacijami ne smejo niti prerasti v uporabo sile niti kršiti temeljnih človekovih pravic, humanitarnih obveznosti, ki prepovedujejo povračilne ukrepe, ali peremptornih mednarodnih pravnih norm (*jus cogens*). Protiukrepi morajo biti usmerjeni proti odgovorni državi (tj. storilki) in sorazmerni s škodo, ki jo je utrpela tarčna država. Poleg tega morajo biti, kolikor je mogoče, reverzibilni, namenjeni spodbujanju države k izpolnjevanju njenih mednarodnih obveznosti in sprejeti tako, da jih ta lahko začne ponovno izpolnjevati.

Poleg tega mora oškodovana (tj. tarčna) država načeloma najprej pozvati odgovorno državo, naj izpolni svoje obveznosti, in jo uradno obvestiti o svoji odločitvi, da bo sprejela protiukrepe. V nekaterih okoliščinah in glede na posebnosti kibernetičnega prostora je lahko nujno in upravičeno, da oškodovana država zaradi zaščite svojih pravic sprejme nujne protiukrepe, ne da bi odgovorno državo vnaprej opozorila o taki nameri.

Preden se kot odgovor na zlonamerne kibernetične dejavnosti sprejmejo protiukrepi, je potrebna previdnost, zlasti kadar so vpleteni nedržavni akterji in še ni gotovo, komu se lahko pripiše odgovornost.

## Nujnost

Država lahko uveljavlja nujnost kot razlog, da se neko dejanje, ki sicer ni v skladu z mednarodno obveznostjo te države, ne šteje za protipravno, če je lahko le na ta način zaščitila bistven interes pred hudo in neposredno kibernetično ali drugo nevarnostjo. Zato lahko država začne izvajati kibernetično dejavnost, da zaščiti električno omrežje, preskrbo s hrano in vodo, železniški promet, izplačevanje socialnih prejemkov in zdravje prebivalstva, ali v podobnih primerih, ko je to neizogibno za delovanje države in družbe.<sup>43</sup> Država, ki se sklicuje na nujnost, pa ne sme resno ogroziti bistvenih interesov prizadete države ali držav ali celotne mednarodne skupnosti. Država se ne more sklicevati na nujnost kot razlog, da se neko dejanje ne šteje za protipravno, če zadevna mednarodna

---

<sup>42</sup> ICJ Nikaragva (1986), 210., 248.–249., 257.–268. odstavek; projekt Gabčíkovo-Nagymaros (*Madžarska proti Slovaški*) [1997], Poročilo ICJ 7, 83.–88. odstavek.

<sup>43</sup> Talinski priročnik 2.0, Cambridge University Press, 2017, pravilo 26, 5. odstavek.

obveznost izključuje možnost sklicevanja na nujnost ali če je država sama prispevala k stanju nujnosti.

### **E) Povrnitev škode**

Država lahko uveljavlja mednarodnopravno odgovornost odgovorne države in zahteva pravno zadoščenje, prenehanje mednarodno protipravnega dejanja in/ali povrnitev vse škode in izgub. Slovenija meni, da se pravila in načela odgovornosti držav, kot je navedeno zgoraj, lahko uporabljajo v kibernetnem prostoru. Slovenija prav tako meni, da lahko povrnitev škode vključuje nadomestilo za škodo, ki jo je mogoče finančno ovrednotiti, in zagotovila ali jamstva, da se tako dejanje ne bo ponovilo.

### **F) Retorzija**

Mednarodno pravo ne izključuje možnosti, da države sprejmejo ukrep retorzije – neprijaznih dejanj, ki niso v nasprotju z njihovimi mednarodnimi obveznostmi –, vključno z razglasitvijo diplomatov države storilke za *persona non grata*. Slovenija priznava, da ukrepi retorzije drugih držav ne smejo prikrajšati za njihove mednarodne pravice. Glede na zgoraj navedeno bi se omejevanje dostopa do strežnikov ali druge digitalne infrastrukture drugi državi na slovenskem ozemlju štelo za ukrep retorzije. Tudi zbirka orodij Evropske unije za kibernetno diplomacijo omogoča ukrepe, ki se lahko uporabijo kot odgovor na zlonamerne kibernetne dejavnosti, ki se štejejo za retorzijo.

## **II. Mirno reševanje sporov**

Slovenija meni, da so si države v skladu s 3. odstavkom 2. člena in VI. poglavjem Ustanovne listine OZN dolžne prizadevati za mirno reševanje sporov, katerih stranke so, vključno s spori v zvezi z ravnanjem držav v kibernetnem prostoru. To vključuje pogajanja, preiskave, mediacijo, spravo, arbitražo in sodno poravnavo.

Glede na posebno naravo in zapletenost sporov v zvezi s kibernetnimi dejavnostmi po mednarodnem pravu bi lahko razmislili o ustanovitvi posebnih strokovnih organov.

## **III. Individualna kazenska odgovornost po mednarodnem pravu**

Kibernetne dejavnosti se pod nekaterimi pogoji lahko štejejo za mednarodna kazniva dejanja, ki imajo za posledico individualno kazensko odgovornost, kot je na primer opredeljeno v Rimskem statutu Mednarodnega kazenskega sodišča (MKS) in mednarodnem običajnem pravu. Poudariti velja, da so določbe tehnološko nevtralne, saj pri nobenem kaznivem dejanju, opredeljenem v predhodno omenjenih instrumentih, ni treba uporabiti posebnega orodja ali sredstev, da bi se nekaj štelo za kaznivo dejanje, temveč se namesto tega osredotočajo na učinke storjenih dejanj. Zato je jasno, da je tudi s kibernetnimi dejavnostmi mogoče povzročiti mednarodna kazniva dejanja.

Vendar pa je ugotavljanje, ali so se taka kazniva dejanja povzročila s kibernetško dejavnostjo, poseben izziv, še zlasti s teh štirih vidikov: (1) resnost kaznivega dejanja, (2) pristojnost držav, (3) pripis odgovornosti za kaznivo dejavnost in (4) ugotavljanje naklepa.

Kibernetška dejavnost kot dejanje ali opustitev dejanja bi se morala šteti za mednarodno kaznivo dejanje, če po svoji naravi, obsegu, učinkih in posledicah dosega prag mednarodnega kaznivega dejanja (*actus reus*) in če je dokazan subjektivni element naklepa ali malomarnosti (*mens rea*).

Glede na dejstvo, da so kibernetške dejavnosti po svoji naravi čezmejne, se državna pristojnost za taka kazniva dejanja veliko težje določi. Med državo in kibernetško dejavnostjo, povezano z zadevnim kaznivim dejanjem, mora obstajati zadostna povezava.

Za pripis odgovornosti za kibernetško dejavnost osebam, ki naj bi izvršile mednarodno kaznivo dejanje, je treba upoštevati kazenskopravne standarde, zato mora biti izpolnjeno dokazno breme, kot narekuje kazenski postopek.

Podobno merilo bi moralo veljati tudi pri ugotavljanju naklepa oseb, izvajalk kibernetške dejavnosti v zvezi z domnevnim mednarodnim kaznivim dejanjem. Zato je priporočljiva previdnost, saj mora biti v kazenskih postopkih izpolnjen visok dokazni standard.

Slovenija odobrava in spodbuja nadaljnje oblikovanje dokumentov o politikah pregona kibernetških kaznivih dejanj, kot je npr. nedavna pobuda urada tožilca Mednarodnega kazenskega sodišča.<sup>44</sup>

## SKLEP

Slovenija kot močna zagovornica spoštovanja mednarodnega prava in vladavine prava pojasnjuje pomen veljavnih načel mednarodnega prava (načela suverenosti, nevmešavanja in prepoved grožnje s silo ali uporabo sile) in še posebej mednarodnega humanitarnega prava in prava človekovih pravic tudi v kibernetškem prostoru. Za ugotavljanje odgovornosti držav v zvezi s kibernetškimi dejavnosti je nepogrešljivo Besedilo členov Komisije za mednarodno pravo o odgovornosti držav za mednarodna protipravna dejanja, za ugotavljanje individualne kazenske odgovornosti glede teh dejavnosti pa Rimski statut Mednarodnega kazenskega sodišča. Slovenija meni, da oblikovanje novega pravno zavezujočega akta ni potrebno. Ne glede na to bo Slovenija spodbujala in krepila razprave o tej temi tako v slovenskem prostoru kot tudi na mednarodni ravni.

---

<sup>44</sup> Osnutek politike o kibernetški kriminaliteti v skladu z Rimskim statutom, 6. marec 2025. Dostopno na: <https://www.icc-cpi.int/sites/default/files/2025-03/250306-OTP-Policy-on-Cyber-Enabled-Crimes-for-public-consultation.pdf>.