

Posvet o nujnosti oblikovanja strategije za odpornost kritične infrastrukture

Pon, 20.04.2026 - 15:31

[Natisni](#)

Ljubljana, 20. april 2026 – [Komisija Državnega sveta za državno ureditev je v sodelovanju z Institutom za korporativne varnostne študije \(ICS\) in Slovenskim združenjem za korporativno varnost v dvorani Državnega sveta pripravila posvet z naslovom »Nujnost oblikovanja ustrezne strategije za zagotavljanje uinkovite odpornosti kritične infrastrukture v Republiki Sloveniji«.](#)

Uvodoma je zbrane nagovoril predsednik Državnega sveta Republike Slovenije **Marko Lotrič**, ki je poudaril, da na kritični infrastrukturi temeljijo osnovne funkcije države in družbe – od oskrbe z energijo, delovanja digitalnih in komunikacijskih omrežij do transportnih sistemov, zdravstvenih in drugih javnih storitev. Opozoril je, da lahko vsaka večja motnja ali prekinitev delovanja teh sistemov povzroči resne posledice za gospodarstvo, varnost države in kakovost življenja državljanov.

Spomnil je, da se sodobno varnostno okolje hitro spreminja, tveganja pa postajajo vse bolj kompleksna in medsebojno povezana. Naravne nesreče, podnebne spremembe, kibernetične grožnje, tehnološke ranljivosti in geopolitična nestabilnost po njegovih besedah zahtevajo celovit pristop krepitve odpornosti, pripravljenosti in sposobnosti hitrega odzivanja. Poudaril je tudi pomen upoštevanja najnovejših domačih in evropskih znanj ter dobrih praks pri oblikovanju nacionalnih strategij. Po njegovih besedah je pri vprašanih odpornosti kritične infrastrukture nujno tesno sodelovanje vseh deležnikov, saj le usklajeno delovanje omogoča oblikovanje dolgoročno vzdržnih rešitev.

Na posvetu sta bila predstavljena dva evropska projekta, ki se iz različnih vidikov ukvarjata z vprašanjem, kako v Evropi okrepi odpornost kritične infrastrukture. Projekt **ENDURANCE**, ki postavlja vseevropski strateški okvir za odpornost KI, ter projekt **ECHO**, ki nadgrajuje delo projekta ENDURANCE, pri čemer upošteva specifične in potrebe na lokalni in regionalni ravni.

Dr. **Jolanda Modic** (ICS Ljubljana) je med glavnimi izzivi, ugotovljenimi na podlagi obeh projektov, naštel razdrobljenost virov (oprema ni dovolj dostopna, znanje je razpršeno, tehnologije niso interoperabilne, podatki se premalo delijo); pomanjkanje operativnih formalnih okvirov; reaktivnost (še vedno je preveč poudarka na odzivu po dogodku in premalo na preventivnem, dolgoročnem upravljanju odpornosti) ter kadrovska in organizacijska preobremenjenost organizacij, ki skrbijo za odpornost in delovanje bistvenih storitev. Za izboljšanje odpornosti je po njenem mnenju treba slediti naslednjim prioritetam: operativno sodelovanje in enotno razumevanje; premik iz reaktivnega v proaktivno upravljanje odpornosti ter vlaganje v človeške vire. Nujen je tudi ustrezen pravni okvir, ki mora biti dovolj fleksibilen in dinamičen, da omogoča delovanje v različnih okoljih, na različnih ravneh in ob različnih vrstah groženj.

V nadaljevanju je potekala okrogla miza, na kateri so sodelovali dr. **Aida Kamišalič Latifič**, državna sekretarka na Ministrstvu za digitalno preobrazbo, **Boštjan Pavlin**, državni sekretar na Ministrstvu za obrambo, dr. **Uroš Svete**, direktor Urada vlade za informacijsko varnost, mag. **Aleksander Mervar**, direktor družbe ELES, mag. **Vesna Prodnik**, članica uprave Telekom Slovenije, in **Leon Behin**, generalni direktor Uprave RS za zaščito in reševanje. Okroglo mizo je moderiral dr. **Denis Čaleta**.

Državni sekretar na Ministrstvu za obrambo **Boštjan Pavlin** je izpostavil nujnost izvajanja ukrepov brez dolgih strateških dokumentov, temveč z operativnimi dokumenti. Ugotovitve zadnje vaje odpornosti po njegovem mnenju kažejo, da je nujno krepiti zaupanje državljanov. V Zakon o kritični infrastrukturi je bil s

tem namenom umeščen sistem zgodnjega opozarjanja. Proces obrambnega narotovanja so z državne ravni pomaknili nazaj na lokalno raven, s čimer so osnovni segment odpornosti ponovno približali ljudem. Gospodarske družbe javnega pomena se bodo morale zavedati, da informacije, s katerimi razpolagajo, niso zgolj njihova last, temveč imajo družbeni pomen in jih je treba deliti, je poudaril. Izpostavil je povezovanje kibernetičnih strokovnjakov iz javne uprave in zasebnega sektorja ter medsektorsko sodelovanje. Sodelovanje poteka npr. z Ministrstvom za zdravje pri vprašanju bolnišničnih kapacitet ter z Ministrstvom za kmetijstvo, gozdarstvo in prehrano pri ohranjanju lokalnih prehranskih verig. Odpornost je po njegovem prepričanju treba sistematično umestiti tako v procese izobraževanja v šolah kot tudi v delovne procese.

Dr. **Aida Kamišali Latifi**, državna sekretarka na Ministrstvu za digitalno preobrazbo, je pojasnila, da se ministrstvo vključuje v vse pobude, s katerimi želijo tudi s finančnimi sredstvi prispevati k skupni zgodbi, zgraditi močnejši sistem in razmišljati o krepitvi nacionalne varnosti. Ob tem je izpostavila, da se pri digitalizaciji na državni ravni vsako ministrstvo samostojno sooča z vprašanjem, katere izzive bo naslovlilo in kako jih bo financiralo, medtem ko lahko Ministrstvo za digitalno preobrazbo drugim ministrstvom predvsem svetuje. Poudarila je tudi pomembno vlogo umetne inteligence ter opozorila, da imamo veliko strokovnjakov, ki delujejo silosno. Kot velik uspeh je navedla razpis za Kompetenčni center za umetno inteligenco, s katerim so uspeli povezati ključne deležnike iz gospodarstva ter raziskovalnih in izobraževalnih institucij.

Dr. **Uroš Svete**, direktor Urada Vlade za informacijsko varnost, je poudaril, da je premagovanje razkoraka na področju kibernetične varnosti tek na dolge proge. Spomnil je, da smo šele pred približno desetimi leti začeli resno razmišljati o celovitem sistemu kibernetične varnosti, medtem ko je bil nemški pristojni urad ustanovljen že leta 1994. Zakonodaja je po njegovem mnenju prilagojena trenutnemu stanju tveganj, Slovenija pa je tudi edina država v EU, ki je v zakon zapisala obvezno usposabljanje odgovornih oseb vseh zavezancev na področju kibernetične varnosti. Poudaril je, da specifična tega področja zahteva nenehno prilagajanje ter da so jasni načrti in protokoli ključni za pravočasno odzivanje na incidente in krize ter tudi za njihovo preprečevanje. Izpostavil je tudi pomen vzpostavitve nacionalnega kibernetičnega vozlišča, ki bi deloval kot povezovalni hub med javnim in zasebnim sektorjem ter bi omogočala sistemsko in tehnično usmerjeno delovanje ter deljenje informacij v realnem času.

Mag. **Aleksander Mervar**, direktor družbe ELES, je povedal, da ELES spada med tri najbolj napredne elektrooperaterje v EU ter da tehnično obvladovanje elektroenergetskega sistema ni problematično - večji izziv predstavljajo razpršeni elektroenergetski viri ter vplivi, ki prihajajo iz tujinskega prostora. Tudi glede odpornosti elektroenergetskega sistema smo od žledoloma leta 2014 napredovali. Izpostavil je, da je večkrat predsednikom vlad predlagal, naj se lastniško upravljanje družbe ELES prenese iz okvira Slovenskega državnega holdinga na resorno ministrstvo, saj gre za infrastrukturo strateškega pomena, povezano z nacionalno varnostjo in odpornostjo. Med ključnimi izzivi distribucijskega omrežja je navedel zadostnost rezervnih delov ter digitalizacijo kart distribucijskega omrežja, saj je npr. ob obilnem snegu težko natančno ugotoviti mesto prekinitve. Pomemben izziv ostaja nadzor nad razpršenimi viri, pri čemer je predlagal večjo centralizacijo.

Mag. **Vesna Prodnik**, članica uprave družbe Telekom Slovenije, je izpostavila potrebo po jasni delitvi odgovornosti. Država mora po njenem mnenju jasno določiti, kateri subjekti so specializirani za kaj in jih krepiti, predvsem pa je nujno, da vemo, kdo je za kaj odgovoren. Izpostavila je tudi strateško vlogo Telekoma Slovenije, ki ima po njenih besedah več inženirjev kot vsi ostali operaterji skupaj, ter dodala, da bi morala država sistem usmerjati bolj koordinirano – podobno kot trener vodi športno ekipo – z jasno razmejenimi vlogami in odgovornostmi.

Leon Behin, generalni direktor Uprave Republike Slovenije za zaščito in reševanje, je poudaril, da so prav pripadniki sistema zaščite in reševanja prvi, ki v kriznih razmerah upravljajo in posredujejo – tako ob naravnih nesrečah kot drugih kriznih dogodkih – ter na terenu odpravljajo njihove posledice. Opozoril je, da je sistem zaščite in reševanja širši od same zaščitne kritične infrastrukture, saj vključuje tudi pripravljenost družbe kot celote. Po njegovem mnenju pripravljenost presega pojem odpornosti, ker zajema tudi ozavešenost in usposobljenost prebivalstva. Kot prednost sistema je izpostavil številko 112, ki je analogna in zato ni

izpostavljena kibernetским napadom. Kot ključni izziv je navedel kadre, nujnost profesionalizacije in krepitve strokovnosti. »Če sistemu zaščite in reševanja ne bomo priznali samostojnosti, bomo imeli v prihodnosti težave,« je poudaril.

Direktor Agencija za komunikacijska omrežja in storitve Republike Slovenije mag. **Marko Mišmaš** je pojasnil, da so mobilna omrežja del kritične infrastrukture, saj si sodobne družbe brez zanesljivih komunikacij ni mogoče predstavljati. »Prav so omrežja kakovostna, ostajajo ranljiva predvsem v primeru naravnih nesreč. Izpostavil je, da na agenciji proaktivno sodelujejo z vsemi deležniki pri pripravi tehničnih rešitev še pred sprejetjem evropske regulative, zlasti na področju odpornosti mobilnih omrežij za zagotavljanje osnovnih storitev, kot sta sistem SI-ALARM in klic na 112. Med konkretnimi ukrepi je navedel tudi naštovani dvig zmogljivosti baterijskih sistemov v baznih postajah na 12 ur, saj trenutna zmogljivost ob izpadu električne energije znaša približno 4 ure.

Posvet je ponudil pregled stanja na področju upravljanja kritične infrastrukture, pri čemer so bile izpostavljene vrzeli v obstoječih politikah, zakonodaji (med drugim prenormiranost na EU ravni), pristojnostih in operativnih zmogljivostih. Omogočil je tudi razpravo o vzpostavitvi sodobnega modela upravljanja odpornosti kritične infrastrukture, izboljšani koordinaciji med deležniki (vključno s povezovanjem javnega in zasebnega sektorja), krepitvi nacionalnih zmogljivosti, uvajanju novih tehnologij, kadrovske okrepitvi ter zagotavljanju trajnostnega financiranja. Sodelujoči so poudarili pomen celostnega pristopa k upravljanju odpornosti kritične infrastrukture ter potrebo po jasnih strateških usmeritvah, ki bodo prispevale k večji varnosti, stabilnosti in odpornosti države.

Dogodek sta povezovala državni svetnik, predsednik Komisije za državno ureditev **Rajko Fajt** in predsednik sveta ICS dr. **Denis Žaleta**.

Dr. **Denis Žaleta** je pojasnil, da je bil med drugim namen posveta, da se ob nastopu nove vlade pripravi nabor predlogov za nadaljnji razvoj tega področja. Izpostavil je, da je odpornost tek na dolge proge – pretekli koraki so ključni, da je mogoče »maraton priteči do konca«. Izrazil je željo, da bi naslednja vlada nadaljevala začetne aktivnosti in dobre rešitve nadgrajevala. Opozoril je tudi, da se sistem izobraževanja in usposabljanja še vedno prepočasno prilagaja, kar predstavlja pomemben izziv tudi na področju zagotavljanja odpornosti.

Na podlagi razprave bo pristojna komisija Državnega sveta pripravila zaključke, ki jih bo nato na eni izmed prihodnjih sej obravnaval Državni svet Republike Slovenije. Zaključki bodo podlaga za nadaljnje razprave o krepitvi odpornosti kritične infrastrukture ter oblikovanju ustreznih strateških usmeritev na tem področju.

