

PRILOGA 1 (spremni dopis – 1. del):

 REPUBLIKA SLOVENIJA MINISTRSTVO ZA OBRAMBO Vojkova cesta 55, 1000 Ljubljana T: 01 471 23 73 F: 01 471 29 78 E: gp.mo@gov.si E: glavna.pisarna@mors.si www.gov.si	
Številka: 870-25/2026-24	
Ljubljana, dne 19. 10. 2026	
GENERALNI SEKRETARIAT VLADE REPUBLIKE SLOVENIJE gp.gs@gov.si	
ZADEVA: Sklep o sodelovanju Republike Slovenije na Natovi vaji kibernetске obrambe »Cyber Coalition 2026 – CC26« – predlog za obravnavo	
1. Predlog sklepov vlade:	
Na podlagi šestega odstavka 21. člena Zakona o Vladi Republike Slovenije (Uradni list RS, št. 24/05 – uradno prečiščeno besedilo, 109/08, 38/10 – ZUKN, 8/12, 21/13, 47/13 – ZDU-1G, 65/14, 55/17, 163/22, 57/25 – ZF in 555/26) in v zvezi s prvim odstavkom 6. člena Pravilnika o vajah v obrambnem sistemu (Uradni list Republike Slovenije, št. 100/13 in 44/21) je Vlada Republike Slovenije na ___ redni seji dne _____ pod ___ točko dnevnega reda sprejela naslednji S K L E P Vlada Republike Slovenije je sprejela Sklep o sodelovanju Republike Slovenije na Natovi vaji kibernetске obrambe »Cyber Coalition 2026 – CC26«. Mag. Janja Garvas generalna sekretarka Priloga: – Sklep o sodelovanju Republike Slovenije na Natovi vaji kibernetске obrambe »Cyber Coalition 2026 – CC26«. Prejmejo: – Generalni sekretariat Vlade Republike Slovenije, – Ministrstvo za finance, – Ministrstvo za notranje zadeve in javno upravo, – Ministrstvo za obrambo, – Ministrstvo za zunanje in evropske zadeve, – Urad Vlade Republike Slovenije za informacijsko varnost, – Služba Vlade Republike Slovenije za zakonodajo, – Akademsko in raziskovalna mreža Slovenije, SI-CERT, – Univerzitetni klinični center Ljubljana.	

2. Osebe, odgovorne za strokovno pripravo in usklajenost gradiva:		
mag. Marko Doblekar, vršilec dolžnosti generalnega direktorja Direktorata za obrambne zadeve		
3. Zunanji strokovnjaki, ki so sodelovali pri pripravi dela ali celotnega gradiva:		
/		
4. Predstavniki vlade, ki bodo sodelovali pri delu državnega zbora:		
/		
5. Kratek povzetek gradiva:		
Od 26. novembra do 3. decembra 2026 bo Republika Slovenija (RS) sodelovala na Natovi vaji kibernetске obrambe »Cyber Coalition 2026 – CC26« (v nadaljevanju: vaja). Vaja je umeščena v Načrt vaj v obrambnem sistemu in sistemu varstva pred naravnimi in drugimi nesrečami v letu 2026 (Sklep Vlade RS, št. 84300-2/2026/6 z dne 14. 5. 2026, št. 84300-2/2026/2 z dne 5. 2. 2026 in št. 84300-10/2026/3 z dne 1. 10. 2026), zato Vlada Republike Slovenije skladno s prvim odstavkom 6. člena Pravilnika o vajah v obrambnem sistemu (Uradni list RS, št. 100/13 in 44/21) sprejme sklep o sodelovanju na vaji. Aktivnosti za načrtovanje in izvedbo vaje bodo v RS sledile aktivnostim, načrtovanim v Natu. Incidenti se bodo prožili na kibernetškem vadišču (ang. Cyber Range), do katerega bodo imeli dostop vsi aktivni vadbenci Natovega scenarija. Težišče vaje bo predstavljalo odzivanje na kibernetске incidente pri delovanju elektronskih komunikacijskih omrežij in sistemov, ki podpirajo delovanje nacionalno-varnostnega sistema, sektorja zdravstvene oskrbe ter vesoljskih storitev, s posebnim poudarkom na zagotavljanju kibernetске varnosti nacionalnih informacijsko-komunikacijskih omrežij in sistemov, ki izvajajo podporo pri logistični oskrbi slovenskega kontingenta na mednarodni misiji. Skladno z dokumenti Nata, specifikacijami vaje ter s Pravilnikom o vajah v obrambnem sistemu (Uradni list RS, št. 100/13 in 44/21), je Ministrstvo za obrambo pripravilo predlog sklepa o sodelovanju RS na Natovi vaji kibernetске obrambe »Cyber Coalition 2026 – CC26«, s katerim se določa cilje vaje in vadbence ter zagotavlja pravočasne priprave na izvedbo vaje. Ministrstvo za obrambo bo zagotovilo tudi pripravo vseh ostalih dokumentov za načrtovanje in izvedbo vaje v RS.		
6. Presoja posledic za:		
a)	javnofinančna sredstva nad 40.000 EUR v tekočem in naslednjih treh letih	NE
b)	usklajenost slovenskega pravnega reda s pravnim redom Evropske unije	NE
c)	administrativne posledice	NE
č)	gospodarstvo, zlasti mala in srednja podjetja ter konkurenčnost podjetij	NE
d)	okolje, vključno s prostorskimi in varstvenimi vidiki	NE
e)	socialno področje	NE
f)	dokumente razvojnega načrtovanja: – nacionalne dokumente razvojnega načrtovanja – razvojne politike na ravni programov po strukturi razvojne klasifikacije programskega proračuna – razvojne dokumente Evropske unije in mednarodnih organizacij	NE
7.a Predstavitev ocene finančnih posledic nad 40.000 EUR:		
/		

I. Ocena finančnih posledic, ki niso načrtovane v sprejetem proračunu				
	Tekoče leto (t)	t + 1	t + 2	t + 3
Predvideno povečanje (+) ali zmanjšanje (–) prihodkov državnega proračuna				
Predvideno povečanje (+) ali zmanjšanje (–) prihodkov občinskih proračunov				
Predvideno povečanje (+) ali zmanjšanje (–) odhodkov državnega proračuna				
Predvideno povečanje (+) ali zmanjšanje (–) odhodkov občinskih proračunov				
Predvideno povečanje (+) ali zmanjšanje (–) obveznosti za druga javnofinančna sredstva				
II. Finančne posledice za državni proračun				
II.a Pravice porabe za izvedbo predlaganih rešitev so zagotovljene:				
Ime proračunskega uporabnika	Šifra in naziv ukrepa, projekta	Šifra in naziv proračunske postavke	Znesek za tekoče leto (t)	Znesek za t + 1
SKUPAJ				
II.b Manjkajoče pravice porabe bodo zagotovljene s prerazporeditvijo:				
Ime proračunskega uporabnika	Šifra in naziv ukrepa, projekta	Šifra in naziv proračunske postavke	Znesek za tekoče leto (t)	Znesek za t + 1
SKUPAJ				
II.c Načrtovana nadomestitev zmanjšanih prihodkov in povečanih odhodkov proračuna:				
Novi prihodki		Znesek za tekoče leto (t)	Znesek za t + 1	
SKUPAJ				
7.b Predstavitev ocene finančnih posledic pod 40.000 EUR:				
Skladno z Načrtom vaj v obrambnem sistemu in sistemu varstva pred naravnimi in drugimi nesrečami v letu 2026 (Vlada RS, št. 84300-3/2026/2 z dne 5. 2. 2026, št. 84300-2/2026/6 z dne 14. 5. 2026 in št. 84300-10/2026/3 z dne 1. 10. 2026) bodo za izvedbo vaje nastale finančne posledice v višini do 10.000 evrov. Finančna sredstva so zagotovljena pri proračunskem uporabniku 1911 - MORS, na proračunski postavki 130011 in bodo namenjena kritju stroškov usposabljanja pred vajo, stroškov tehničnih storitev, prehrane in drugih osnovnih storitev med izvajanjem vaje. Ostala finančna sredstva, namenjena kritju rednih stroškov, kot so izplačilo nadur, zagotovitev tehnične podpore in zagotovitev prehrane in drugih osnovnih storitev, ki nastanejo tekom priprav in izvedbe vaje na sedežih vadbencev, zagotavljajo vadbenci sami.				
8. Predstavitev sodelovanja z združenji občin:				
Vsebina predloženega gradiva (predpisa) vpliva na:			NE	
- pristojnosti občin,				

- delovanje občin, - financiranje občin.	
9. Predstavitev sodelovanja javnosti:	
Gradivo je bilo predhodno objavljeno na spletni strani predlagatelja:	NE
Skladno s sedmim odstavkom 9. člena Poslovnika Vlade RS (Uradni list RS, št. 43/01, 23/02 – popr., 54/03, 103/03, 114/04, 26/06, 21/07, 32/10, 73/10, 95/11, 64/12, 80/13, 10/14, 164/20, 35/21, 51/21 in 114/21) javnost ni bila povabljena k sodelovanju, ker gre za predlog sklepa Vlade.	
Mag. Valentin Hajdinjak MINISTER	

Poslano:

- naslovníkom,
- DOZ,
- OVS,
- SGS,
- SSK,
- GŠSV.

Številka:

V Ljubljani, dne _____

Na podlagi šestega odstavka 21. člena Zakona o Vladi Republike Slovenije (Uradni list RS, št. 24/05 – uradno prečiščeno besedilo, 109/08, 38/10 – ZUKN, 8/12, 21/13, 47/13 – ZDU-1G, 65/14, 55/17, 163/22, 57/25 – ZF in 555/26) in v zvezi s prvim odstavkom 6. člena Pravilnika o vajah v obrambnem sistemu (Uradni list Republike Slovenije, št. 100/13 in 44/21) je Vlada Republike Slovenije na ____ redni seji dne _____ pod ____ točko dnevnega reda sprejela naslednji

S K L E P

o sodelovanju Republike Slovenije na Natovi vaji kibernetске obrambe »Cyber Coalition 2026 - CC26«

1. člen (vsebina)

Republika Slovenija (v nadaljevanju: RS) bo od četrтка, 26. 11. 2026, do četrтка, 3. 12. 2026, sodelovala na Natovi vaji kibernetске obrambe »Cyber Coalition 2026 – CC26« (v nadaljevanju: vaja).

2. člen (namen)

(1) Namen vaje je izboljšati sodelovanje in okrepiti sposobnost Nata in zaveznic pri zaščiti in obrambi kibernetskega prostora.

(2) Namen vaje v RS je vaditi nacionalne postopke zaščite in obrambe kibernetskega prostora ter postopke ob pojavu resne motnje v delovanju elektronskih komunikacijskih omrežij in sistemov, ki podpirajo delovanje nacionalno-varnostnega sistema ter neprekinjeno zagotavljanje storitev.

(3) Vaja zagotavlja pogoje za razvoj in testiranje tehničnih in operativnih postopkov za izvajanje kolektivne obrambe pred kibernetскими grožnjami.

(4) Sodelovanje na vaji vključuje vadbo Natovih in nacionalnih postopkov, vključujoč dobre prakse na področju izmenjave podatkov, vzpostavitev situacijskega zavedanja v kibernetskem prostoru ter svetovanje in sprejemanje odločitev, skladno s pravili in pristojnostmi.

3. člen (cilji vaje)

(1) Skladno s scenarijem Nata, opredeljenim v Natovem dokumentu Navodilo o vaji CC26 (EXERCISE CYBER COALITION 2026 - EXERCISE SPECIFICATION - dok. št. ACT/CAPDEV/MDC/TT-2050/SER:NU:790, z dne 22. 4. 2026), so cilji Natove vaje, v katero bo vključen širši strateški in operativni nivo, naslednji:

- doseči zaželeni nivo procesov, kapacitet in delovanja skupnosti v kibernetnem prostoru z namenom okrepitve zavezniške sposobnosti načrtovanja in izvajanja operacij v kibernetnem prostoru ter odzivanja na kibernetne incidente, vključujoč civilne in vojaške subjekte;
- izvajati delovanje obstoječih mehanizmov, izmenjavo podatkov in ostale postopke za interakcijo teles Nata, zaveznic in partnerskih držav ter organizacij z namenom izboljšanja sodelovanja, skupnega delovanja in koordinacije vojaških in civilnih aktivnosti v kibernetnem prostoru;
- identificirati vrzeli v kapacitetah, zadovoljiti vadbemim zahtevam, preizkusiti nove postopke operacij v kibernetnem prostoru in omogočiti operacionalizacijo novih kapacitet v podporo delovanju v kibernetnem prostoru;
- vaditi delovanje Natovega integriranega centra za kibernetno obrambo (ang. NATO Integrated Cyber Defence Centre - NICC) in njegovo interakcijo z zaveznicami, telesi Nata in industrijo v podporo zavezniškim mednarodnim operacijam in misijam (MOM).

(2) Cilji vaje v RS so:

- i. preveriti odziv nacionalno-varnostnega sistema RS na posredna ali neposredna ogrožanja in varnostna tveganja v primeru kibernetne grožnje ali incidenta v nacionalnem kibernetnem prostoru;
- ii. dvigniti zavedanje o kibernetni varnosti in obrambi kot politični in strateški prioriteti;
- iii. vaditi procese in postopke zaščite in obrambe kibernetnega prostora;
- iv. vaditi postopke koordiniranja upravljanja kibernetnih incidentov na nacionalnem nivoju;
- v. vaditi sodelovanje in izmenjavo informacij v zvezi s kibernetnimi incidenti na mednarodnem nivoju;
- vi. preveriti nacionalne in mednarodne normativne podlage ter procese za usklajevanje in izvajanje postopkov kibernetne obrambe;
- vii. preveriti sodelovanje, izmenjavo informacij in funkcionalnost odzivanja na kibernetne incidente v sodelovanju z gospodarskim sektorjem;
- viii. vaditi sodelovanje s pravnimi strokovnjaki tekom odzivanja na kibernetne incidente;
- ix. vaditi odzivanje na kibernetne incidente na področju kritične infrastrukture, v sektorju digitalne infrastrukture, ki vplivajo na sodelovanje Slovenske vojske na mednarodni mirovni misiji;
- x. vaditi operativne postopke in postopke poročanja Slovenske vojske ob kibernetnih incidentih;
- xi. preizkusiti odpornost informacijsko-komunikacijske tehnologije sistema državne uprave na kibernetne napade;
- xii. vaditi postopke poročanja vadbencev ob zaznavi kibernetnega incidenta s ciljem zmanjševanja njihovih negativnih učinkov in zagotavljanjem celovite situacijske slike kibernetne varnosti v državi;
- xiii. vaditi zbiranje obveščevalnih podatkov o kibernetnih grožnjah z namenom usmerjanja operacij v kibernetnem prostoru;
- xiv. ohranjanje situacijskega zavedanja v kibernetnem prostoru vseh vadbencev prek procesov pridobivanja informacij;
- xv. vaditi procese zaprosila, koordinacije ter odobritve bilateralne pomoči v podporo operacijam v kibernetnem prostoru;
- xvi. zbirati, analizirati ter ovrednotiti informacije o hibridnih grožnjah v podporo odločanju;
- xvii. preveriti odziv na medijski pritisk ter usklajeno komuniciranje z javnostjo v primeru kibernetnih incidentov;
- xviii. preveriti odzivanje enot Slovenske vojske, ki sodelujejo na vaji na kibernetne incidente na mednarodni mirovni misiji ter preveriti procese štabnega dela in sodelovanja z organi kibernetne obrambe znotraj Ministrstva za obrambo;
- xix. vaditi postopke odzivanja na kibernetne incidente v omrežjih na terenu v skladu s SOP SV št. 16-0014: Odzivanje na računalniške in omrežne incidente;
- xx. preveriti izmenjavo podatkov in odločitev na obstoječih komunikacijsko informacijskih sistemih med posameznimi deležniki vaje skladno z obstoječo dokumentacijo ter preveriti SOP za odzivanje na incidente (SOP SV št. 16-0014: Odzivanje na računalniške in omrežne incidente);

xxi. preveriti izvajanje postopkov zaščite lastnih sil, ter postopkov za zaščito stacionarnih in premičnih omrežij v upravljanju in uporabi Slovenske vojske med povečanimi aktivnostmi v kibernetnem prostoru.

4. člen (osnovna zamisel za izvedbo)

(1) Na vaji bo ključna sprememba v samem scenariju vaje. Dolgoletni scenarij na namišljenem otoku Icebergen (državi Andvarija in Harbardus) se je zaključil s trajnim mirom v državi Andvarija. Zaradi navedenega se dosedanja NATO CNDF misija zaključuje, glavna vaje oziroma scenarija pa se preusmeri na vzhodno krilo Nata na prednje kopenske sile (v ang. *Forward Land Forces*; v nadaljevanju:FLF), kjer sodeluje tudi Slovenija. Iz preteklega scenarija bo glavno grožnjo Natu predstavljala država Murinus.

(2) Scenarij vaje je vezan na delovanje kontingentov držav članic Nata na vzhodnem krilu zavezništva (FLF). Kontingenti se soočajo z različnimi načini kibernetnega delovanja nasprotnika, ki se odražajo skozi vnaprej pripravljena medijska sporočila in zgodbe (storyline) s tehničnimi izzivi. Kibernetno delovanje ni omejeno samo na območje delovanja kontingenta, ampak ima tudi posledice na kritično infrastrukturo posamezne države oziroma vadbence in kibernetno obrambo v logističnih procesih, ki podpirajo kontingent. Incidenti ne povzročijo kaskadnih učinkov odpovedi delovanja sistemov in vplivanja na druge sektorje.

(4) Cilj nasprotnikov je, da s kibernetnimi napadi in hibridnim delovanjem oslabijo učinkovitost ter ugled kontingenta. Kibernetni incidenti ter odzivanje nanje vodijo do sodelovanja med vojaškimi ter civilnimi centri za obravnavo kibernetnih incidentov in organi Nata. Sodelovanje med vadbenci v okviru vadbe postopkov in dobrih praks svetovanja ter sprejemanja odločitev je ključnega pomena za situacijsko zavedanje v kibernetnem prostoru.

(5) Za potrebe vaje bo Nato vzpostavil ločeno komunikacijsko-informacijsko omrežje oziroma kibernetno vadblišče (ang. *Cyber Range*), na katerem bo potekala vaja ter simulacija kibernetnih incidentov. Za izmenjavo podatkov in odločitev bodo uporabljene storitve na obstoječih komunikacijsko-informacijskih sistemih.

5. člen (nacionalni scenarij)

(1) Osnovni scenarij vaje je zastavljen na način, da se lahko ta prilagodi nacionalnim željam in potrebam. Osnova nacionalnega scenarija je kibernetno delovanje zoper kontingent Slovenske vojske (v nadaljevanju: SVNKON) v FLF v Latviji. Sodelovanje SVNKON prinaša posledice, in sicer napade na kritično infrastrukturo RS. Vlogo SVNKON bo igrala Logistična brigada Slovenske vojske. V vajo bosta vključena tudi gospodarski sektor s področja zdravstva ter vesoljskih storitev, s poudarkom na zagotavljanju varnosti informacijsko-komunikacijskih omrežij in sistemov kritične infrastrukture RS, tudi v povezavi z delovanjem SVNKON, zagotavljanjem satelitskih storitev in preprečevanjem vdora v satelitske sisteme, preprečevanjem manipulacije vojaške in civilne logistike (v podporo SVNKON) ter zoperstavljanju kibernetnim incidentom na misijskem omrežju FLF. Nacionalni scenarij vsebuje tudi scenarij o hibridnih grožnjah, ki ga bo preigravala hibridna celica Ministrstva za obrambo.

(2) Izhajajoč iz nacionalnega scenarija, bodo vadbenci v RS vadili postopke odzivanja na kibernetne incidente, ki ne povzročajo kaskadnega učinka in vpliva na ostale sektorje.

6. člen
(kraj in čas izvajanja)

(1) Vodstvo vaje Nata in predstavnike udeleženi držav bo v simulacijskem centru v Talinu, Estonija, gostilo Ministrstvo za obrambo Estonije. RS bo za čas izvedbe vaje v Talin napotila dva nacionalna predstavnika, in sicer predstavnika v vlogi nacionalnega koordinatorja (EXCON) ter njegovega namestnika.

(2) Vadbenci v RS bodo za čas vaje delovali na njihovih sedežih.

(2) V RS bodo skupino na področju prava (LEGAD) sestavljali predstavniki vadbencev in drugih sodelujočih subjektov na vaji, delovala pa bo v prostorih Ministrstva za obrambo.

(3) Vaja se bo izvajala med 26. 11. 2026 in 3. 12. 2026, v okviru rednega delovnega časa do 17.30 ure, kot tudi v soboto in nedeljo. Za potrebe izvedbe posameznih aktivnosti, se čas izvajanja vaje uskladi z odločitvami vodstva vaje, ki bodo podane v navodilu za vajo.

7. člen
(tehnične in varnostne zahteve)

Vadbenci, ki bodo komunicirali z Natovimi poveljstvi in z Natovo misijo na vzhodnem krilu Nata (FLF), za izvajanje delovnih nalog v okviru vaje potrebujejo dostop do sistema NATO SECRET oziroma BICES.

8. člen
(priprava, načrtovanje in izvedba)

(1) Vaja bo izvedena skladno s specifikacijami Nata za izvedbo vaje – Navodila o vaji CC26 (EXERCISE CYBER COALITION 2026 - EXERCISE SPECIFICATION - dok. št. ACT/CAPDEV/MDC/TT-2050/SER:NU:790, z dne 22. 4. 2026) ter Navodilom za organizacijo in izvedbo Natove vaje kibernetске obrambe Cyber Coalition 2026 - CC26 v RS, ki ga sprejme vodja vaje.

(2) Ministrstvo za obrambo organizira in usklajuje priprave na vajo in zagotovi izdelavo dokumentov, potrebnih za izvedbo vaje v RS. Vsi vadbenci so dolžni sodelovati v pripravi na vajo, pri njeni izvedbi in uresničitvi zastavljenih ciljev.

(3) Usposabljanje za vse vadbence glede scenarija, zgodb, postopkov in poročanja EXCON-a iz končne koordinacijske konference bo, s strani Ministrstva za obrambo in lokalnih trenerjev, izvedeno v drugi polovici novembra, pred samo vajo.

(4) Določeni dokumenti v zvezi z scenarijem vaje se bodo vadbencem posredovali predhodno.

(5) Za čas vaje bo po potrebi sklicana Koordinacijska skupina za kibernetско varnost, ki jo vodi Urad Vlade Republike Slovenije za informacijsko varnost. Koordinacijska skupina za kibernetско varnost bo sklicana ob določeni količini in stopnji incidentov ter zgolj s člani subjektov, ki sodelujejo na vaji.

(6) Za strateško komuniciranje z javnostmi na vaji poskrbi Služba za strateško komuniciranje Ministrstva za obrambo.

(7) Ministrstvo za obrambo zagotovi skupni portal, kjer imajo vsi vadbenci in ostali sodelujoči na vaji dostop do gradiv vaje.

(8) Vadbenci pri določitvi števila sodelujočih na vaji ter delovnega časa upoštevajo predpise, ki urejajo delovna razmerja in delovni čas.

9. člen (vodja in vodstvo vaje)

(1) Vodstvo vaje v RS sestavljajo:

- mag. Marko Doblekar, Ministrstvo za obrambo, vodja vaje;
- Gregor Majcen, Ministrstvo za obrambo, namestnik vodje vaje;
- pk. Samo Flisek, Ministrstvo za obrambo, član;
- mag. Viktor Sterle, Ministrstvo za obrambo, član;
- dr. Niko Gamulin, Urad Vlade Republike Slovenije za informacijsko varnost, član;
- mag. Anton Ujčič, Ministrstvo za notranje zadeve in javno upravo, član;
- Irena Utroša, Ministrstvo za notranje zadeve in javno upravo, članica;
- Rok Zagorski, Ministrstvo za zunanje in evropske zadeve, član;
- Tilen Sotler, Dewesoft d.o.o., član;
- Andrej Dočinski, Univerzitetni klinični center Ljubljana, član.

(2) Vodstvo vaje zagotovi ustrezne priprave in izvedbo vaje ter sodelovanje vadbencev pri uresničitvi zastavljenih ciljev.

(3) Vodja vaje s sklepom imenuje člane Skupine za pripravo in izvedbo vaje, ki je odgovorna za priprave, organizacijo in izvedbo vaje, nacionalnega koordinatorja vaje (EXCON) in njegovega namestnika ter lokalne trenerje.

(4) Vodstvo vaje po končani vaji potrdi poročilo o vaji. Ministrstvo za obrambo poročilo o vaji pošlje v sprejem oziroma potrditev Vladi RS v roku treh mesecev.

10. člen (vadbenci)

(1) Vadbenci na vaji v RS so:

- Ministrstvo za obrambo;
- Slovenska vojska;
- Urad Vlade RS za informacijsko varnost;
- Akademsko in raziskovalna mreža Slovenije, SI-CERT;
- Ministrstvo za zunanje in evropske zadeve;
- Ministrstvo za notranje zadeve in javno upravo;
- Univerzitetni klinični center Ljubljana;
- Dewesoft d. o. o..

(2) Vsak vadbenec, ki razpolaga s tehnično ekipo, je dolžan zagotoviti tudi procesni del za namen poročanja ter imenovati osebo, ki bo zadolžena za odločanje in procese, tako v pripravi, kot v sami izvedbi vaje.

(3) Glede na razvoj scenarija vaje in skladno z odločitvijo vodstva vaje, se kot vadbenci v vajo lahko vključijo tudi drugi subjekti, ki v RS opravljajo naloge s področja nacionalnih komunikacijskih omrežij ali ostale naloge, vezane na kibernetško obrambo.

11. člen
(stroški priprav in izvedbe)

Stroške, ki nastanejo v zvezi z izvedbo usposabljanja za vadbence ter stroške, kot so tehnične storitve, prehrana in ostale osnovne storitve, ki nastanejo v času priprav in izvedbe vaje v prostorih Ministrstva za obrambo, v višini do 10.000 EUR, krije Ministrstvo za obrambo. Redne stroške, ki vključujejo kritje nadur, prehrano in ostale osnovne in tehnične storitve, ki nastanejo tekom priprav in izvajanja vaje na sedežih vadbencev, krijejo vadbenci sami.

12. člen
(varnostni ukrepi)

Pri pripravi in izvedbi vaje se izvajajo predpisani varnostni ukrepi za varovanje nacionalnih tajnih podatkov in tajnih podatkov Nata.

13. člen
(seznanitev vadbencev)

Ministrstvo za obrambo s tem sklepom seznani vadbence. Osebe, odgovorne za informacijsko varnost pri organih državne uprave, seznani Urad Vlade RS za informacijsko varnost.

14. člen
(končna določba)

Ta sklep začne veljati naslednji dan po sprejetju.

mag. Janja Garvas
generalna sekretarka

OBRAZLOŽITEV

Od 26. novembra do 3. decembra 2026 bo Republika Slovenija (v nadaljevanju: RS) sodelovala na Natovi vaji kibernetске obrambe »Cyber Coalition 2025 – CC26« (v nadaljevanju: vaja). Vaja je načrtovana v Načrtu vaj v obrambnem sistemu in sistemu varstva pred naravnimi in drugimi nesrečami v letu 2026 (Sklep Vlade RS, št. 84300-2/2026/6 z dne 14. 5. 2026, št. 84300-2/2026/2 z dne 5. 2. 2026 in št. 84300-10/2026/3 z dne 1. 10. 2026) pod zaporedno številko 11, v točki 2.1.1. – Celovite vaje obrambnega sistema.

Na vaji bo ključna sprememba v samem scenariju vaje. Dolgoletni scenarij na namišljenem otoku Icebergen (državi Andvarija in Harbardus) se je zaključil s trajnim mirom v državi Andvarija. Zaradi navedenega se dosedanja NATO CNDF misija zaključuje, glavčina vaje oziroma scenarija pa se preusmeri na vzhodno krilo Nata na prednje kopenske sile (v ang. Forward Land Forces (FLF)), kjer sodeluje tudi RS. Iz preteklega scenarija bo glavno grožnjo Natu predstavljala država Murinus. Scenarij vaje je vezan na mednarodno misijo pod vodstvom Nata, v kateri v posameznih vojaških poveljstvih sodelujejo vse države udeleženke vaje.

Osnovni scenarij vaje bo v RS nadgrajen z namenom doseganja ciljev iz 3. člena Sklepa o sodelovanju Republike Slovenije na Natovi vaji kibernetске obrambe »Cyber Coalition 2026 - CC26«. V vajo bosta poleg organov državne uprave, vključena še zdravstveni sektor ter tehnološko podjetje, poudarek pa bo na zagotavljanju varnosti informacijsko-komunikacijskih omrežij in sistemov kritične infrastrukture RS, varnosti civilnih in vojaških sistemov za obveščevalno dejavnost, nadzor in izvidovanje ter kibernetски incident na Natovi misiji.

Pomemben element vaje bo tudi preigravanje različnih možnosti nudenja in sprejemanja vzajemne pomoči ob kibernetских napadih, tako na nacionalnem nivoju kot v mednarodnem okolju. Pravna vprašanja glede nudenja pomoči postajajo vedno bolj aktualna zaradi hitrega in učinkovitega odzivanja na kibernetские incidente, zato je nujno, da RS v okviru vaje preigra tudi pravni vidik omenjenega izziva.

Aktivnosti za načrtovanje vaje in sama izvedba vaje bodo v RS sledile aktivnostim v Natu. Skladno z dokumenti Nata in s specifikacijo vaje, je Ministrstvo za obrambo pripravilo Sklep o sodelovanju Republike Slovenije na Natovi vaji kibernetске obrambe »Cyber Coalition 2026 - CC26«, s katerim se zagotovijo pravočasne priprave in določitev vadbencev. Ministrstvo za obrambo bo zagotovilo tudi pripravo vseh ostalih dokumentov za načrtovanje in izvedbo vaje v državi. Zaradi pravočasnih nadaljnjih priprav in določitve udeležencev vaje se, skladno s Pravilnikom o vajah v obrambnem sistemu, predlog sklepa pošlje Vladi Republike Slovenije v sprejem najmanj trideset dni pred začetkom vaje.

MINISTRSTVO ZA OBRAMBO