PREDLOGI SPREMEMB 001-001
vlagatelj: Odbor za industrijo, raziskave in energijo

Poročilo
Lina Gálvez Muñoz **A9-0426/2023**
Akt o kibernetski solidarnosti

Predlog uredbe (COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

Predlog spremembe 1

PREDLOGI SPREMEMB EVROPSKEGA PARLAMENTA*

k predlogu Komisije

2023/0109(COD)

Predlog

UREDBA EVROPSKEGA PARLAMENTA IN SVETA

o določitvi ukrepov za okrepitev solidarnosti in zmogljivosti v Uniji za odkrivanje kibernetskovarnostnih groženj in incidentov ter pripravo in odzivanje nanje *ter o spremembi Uredbe (EU) 2021/694*

EVROPSKI PARLAMENT IN SVET EVROPSKE UNIJE STA –

ob upoštevanju Pogodbe o delovanju Evropske unije ter zlasti člena 173(3) in člena 322(1), točka (a), Pogodbe,

* Spremembe: krepki ležeči tisk označuje novo ali spremenjeno besedilo, simbol ▌ pa tiste dele besedila, ki so bili črtani.

ob upoštevanju predloga Evropske komisije,

po posredovanju osnutka zakonodajnega akta nacionalnim parlamentom,

ob upoštevanju mnenja Računskega sodišča[1],

ob upoštevanju mnenja Evropskega ekonomsko-socialnega odbora[2],

ob upoštevanju mnenja Odbora regij[3],

v skladu z rednim zakonodajnim postopkom,

ob upoštevanju naslednjega:

(1) Uporaba informacijskih in komunikacijskih tehnologij ter odvisnost od njih sta postali ključna vidika***, hkrati pa tudi vir morebitnih ranljivosti*** v vseh sektorjih gospodarske dejavnosti ***in področjih demokracije***, saj so naše javne uprave, podjetja in državljani v različnih sektorjih in prek meja tesneje medsebojno povezani in bolj odvisni drug od drugega kot kdaj koli prej.

(2) Obseg, pogostost in posledice kibernetskovarnostnih incidentov se ***po vsej Uniji in tudi na svetovni ravni*** povečujejo ***tako z vidika njihovih metod kot z vidika posledic***, vključno z napadi na oskrbovalno verigo, katerih cilj je kibernetsko vohunjenje, izsiljevalsko programje ali povzročanje motenj. Ti predstavljajo veliko grožnjo za delovanje omrežja in informacijskih sistemov. Glede na hitro razvijajočo se krajino groženj je treba zaradi nevarnosti morebitnih incidentov velikih razsežnosti, ki ***bi po vsej Uniji povzročili*** velike motnje ali škodo na kritičnih infrastrukturah ***gospodarstva in demokracije***, povečati pripravljenost na vseh ravneh okvira Unije za kibernetsko varnost. Ta nevarnost presega rusko vojaško agresijo na Ukrajino in bo – glede na to, da so v trenutne geopolitične napetosti vpleteni številni akterji, ki so povezani z oblastmi, in kriminalni ▌akterji – verjetno še naprej obstajala. Taki incidenti lahko ovirajo zagotavljanje javnih storitev in opravljanje gospodarskih dejavnosti, tudi v kritičnih ali visoko kritičnih sektorjih, povzročijo znatne finančne izgube, spodkopljejo zaupanje uporabnikov, povzročijo veliko škodo gospodarstvu Unije in imajo lahko celo zdravstvene ali življenjsko nevarne posledice. Poleg tega so kibernetskovarnostni incidenti nepredvidljivi, saj pogosto nastanejo in se razvijejo v zelo kratkem času, niso omejeni na določeno geografsko območje in se zgodijo hkrati ali se takoj razširijo po številnih državah. ***Zato morajo javni in zasebni sektor, akademski svet, civilna družba in mediji med seboj tesno in usklajeno sodelovati. Poleg tega mora biti odziv Unije usklajen z mednarodnimi institucijami ter z zaupanja vrednimi in podobno mislečimi mednarodnimi partnerji. Zaupanja vredni in podobno misleči mednarodni partnerji so države, ki imajo enake vrednote kot Unija, tj. demokracijo, zavezanost človekovim pravicam, učinkovit multilateralizem in ureditev, ki temelji na pravilih, v skladu z okviri in sporazumi za mednarodno sodelovanje. Da bi zagotovili sodelovanje z zaupanja vrednimi in podobno mislečimi mednarodnimi partnerji ter zaščito pred sistemskimi tekmeci, subjektom s sedežem v tretjih državah, ki niso pogodbenice Sporazuma o javnih naročilih, po tej uredbi ne bi smelo biti dovoljeno sodelovati pri javnem naročanju.***

(3) Okrepiti je treba konkurenčni položaj industrijskega in storitvenega sektorja v Uniji v celotnem spletnem gospodarstvu ter podpreti njuno digitalno preobrazbo, in sicer z

---

1 UL C […], […], str. […].
2 UL C , , str. .
3 UL C , , str. .

okrepitvijo ravni kibernetske varnosti na enotnem digitalnem trgu. Kot je priporočeno v treh različnih predlogih Konference o prihodnosti Evrope[1], je treba povečati odpornost državljanov, podjetij***, zlasti mikro-, malih in srednjih podjetij (v nadaljnjem besedilu: MSP), vključno z zagonskimi podjetji,*** in subjektov, ki upravljajo kritične infrastrukture, ***vključno z lokalnimi ali regionalnimi organi,*** proti vse večjim kibernetskovarnostnim grožnjam, ki lahko imajo uničujoče družbene in gospodarske posledice. Zato so potrebne naložbe v infrastrukture in storitve ***ter krepitev zmogljivosti za razvoj kibernetskovarnostnih veščin***, ki bodo podpirale hitrejše odkrivanje kibernetskovarnostnih groženj in incidentov ter odzivanje nanje, države članice pa potrebujejo pomoč pri boljši pripravi na pomembne kibernetskovarnostne incidente in take incidente velikih razsežnosti ter odzivanju nanje. Unija bi tudi morala povečati svoje zmogljivosti na teh področjih, zlasti kar zadeva zbiranje in analizo podatkov o kibernetskovarnostnih grožnjah in incidentih.

(3a) Kibernetski napadi so pogosto usmerjeni v lokalne, regionalne ali nacionalne javne storitve in infrastrukture. Med najranljivejšimi tarčami kibernetskih napadov so lokalni organi, saj jim primanjkuje finančnih in človeških virov. Zato je zlasti pomembno, da se odločevalce na lokalni ravni seznani s tem, da je treba povečati digitalno odpornost in njihovo zmogljivost za zmanjšanje posledic kibernetskih napadov ter izkoristiti priložnosti, ki jih ponuja ta uredba.

(4) Unija je že sprejela več ukrepov za zmanjšanje ranljivosti in povečanje odpornosti kritičnih infrastruktur in subjektov proti tveganjem za kibernetsko varnost, zlasti Direktivo (EU) 2022/2555 Evropskega parlamenta in Sveta[2], Priporočilo Komisije (EU) 2017/1584[3], Direktivo 2013/40/EU Evropskega parlamenta in Sveta[4] ter Uredbo (EU) 2019/881 Evropskega parlamenta in Sveta[5]. Poleg tega so države članice v priporočilu Sveta o usklajenem vseevropskem pristopu za krepitev odpornosti kritične infrastrukture pozvane, naj sprejmejo nujne in učinkovite ukrepe ter zvesto, učinkovito, solidarno in usklajeno sodelujejo med seboj, s Komisijo in drugimi ustreznimi javnimi organi ter zadevnimi subjekti, da bi se okrepila odpornost kritične infrastrukture, ki se uporablja za zagotavljanje bistvenih storitev na notranjem trgu.

(5) Zaradi vse večjih tveganj za kibernetsko varnost in na splošno zapletene krajine groženj, pa tudi zaradi jasnega tveganja hitrega prelivanja kibernetskih incidentov iz ene države

---

1 https://futureu.europa.eu/sl/

2 Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (UL L 333, 27.12.2022).

3 Priporočilo Komisije (EU) 2017/1584 z dne 13. septembra 2017 o usklajenem odzivu na velike kibernetske incidente in krize (UL L 239, 19.9.2017, str. 36).

4 Direktiva 2013/40/EU Evropskega parlamenta in Sveta z dne 12. avgusta 2013 o napadih na informacijske sisteme in nadomestitvi Okvirnega sklepa Sveta 2005/222/PNZ (UL L 218, 14.8.2013, str. 8).

5 Uredba (EU) 2019/881 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti ter razveljavitvi Uredbe (EU) št. 526/2013 (Akt o kibernetski varnosti) (UL L 151, 7.6.2019, str. 15).

članice v druge in iz tretje države v Unijo je potrebna okrepljena solidarnost na ravni Unije za boljše odkrivanje kibernetskovarnostnih groženj in incidentov ter pripravo in odzivanje nanje ***in boljšo obnovitev po njih***. Države članice so Komisijo v sklepih Sveta o kibernetski drži EU pozvale tudi, naj predstavi predlog o novem skladu za odzivanje na izredne kibernetskovarnostne razmere[1].

(6) V skupnem sporočilu o politiki EU za kibernetsko obrambo[2], sprejetem 10. novembra 2022, je bila napovedana pobuda EU za kibernetsko solidarnost z naslednjimi cilji: okrepitev skupnih zmogljivosti EU za odkrivanje, situacijsko zavedanje in odzivanje s spodbujanjem uvedbe ***unijske mreže*** centrov za varnostne operacije ▌, podpiranje postopne vzpostavitve kibernetskovarnostne rezerve na ravni EU s storitvami zaupanja vrednih zasebnih ponudnikov in preskušanje kritičnih subjektov glede morebitnih ranljivosti na podlagi ocen tveganja EU.

(7) Po vsej Uniji je treba izboljšati odkrivanje kibernetskih groženj in incidentov ter situacijsko zavedanje o njih, hkrati pa je treba okrepiti solidarnost s povečanjem pripravljenosti in zmogljivosti držav članic in Unije za odzivanje na pomembne kibernetskovarnostne incidente in take incidente velikih razsežnosti ***ter za njihovo preprečevanje***. Zato bi bilo treba vzpostaviti vseevropsko ***mrežo*** centrov za varnostne operacije (evropski kibernetski ščit), da bi se oblikovale in okrepile skupne zmogljivosti za odkrivanje in situacijsko zavedanje ***in tako okrepile zmogljivosti Unije za odkrivanje groženj in izmenjavo informacij***; vzpostaviti bi bilo treba mehanizem za izredne kibernetskovarnostne razmere, da bi države članice podprli pri pripravi na pomembne kibernetskovarnostne incidente in take incidente velikih razsežnosti, odzivanju nanje in takojšnji obnovitvi po njih; vzpostaviti bi bilo treba mehanizem za pregledovanje kibernetskovarnostnih incidentov za pregledovanje in ocenjevanje posameznih pomembnih kibernetskovarnostnih incidentov ali incidentov velikih razsežnosti. Ti ukrepi ne posegajo v člena 107 in 108 Pogodbe o delovanju Evropske unije (PDEU).

(8) Za dosego teh ciljev je treba tudi spremeniti nekatere dele Uredbe (EU) 2021/694 Evropskega parlamenta in Sveta[3]. Zlasti bi bilo treba s to uredbo spremeniti Uredbo (EU) 2021/694, kar zadeva dodajanje novih operativnih ciljev v zvezi z evropskim kibernetskim ščitom in mehanizmom za izredne ***kibernetskovarnostne*** razmere v okviru specifičnega cilja 3 programa Digitalna Evropa, katerega cilj je zagotoviti odpornost, celovitost in zanesljivost enotnega digitalnega trga, okrepiti zmogljivosti za spremljanje kibernetskih napadov in groženj in odzivanje nanje ter izboljšati čezmejno sodelovanje na področju kibernetske varnosti. To bo dopolnjeno s posebnimi pogoji, pod katerimi se lahko za te ukrepe dodeli finančna podpora, pri čemer bi bilo treba opredeliti mehanizme upravljanja in usklajevanja, ki so potrebni za doseganje zastavljenih ciljev. Druge spremembe Uredbe (EU) 2021/694 bi morale vključevati opise predlaganih ukrepov v okviru novih operativnih ciljev in merljive kazalnike za spremljanje izvajanja teh novih operativnih ciljev.

---

1 Sklepi Sveta o oblikovanju kibernetske drže Evropske unije, ki jih je Svet odobril na seji 23. maja 2022 (9364/22).

2 Skupno sporočilo Evropskemu parlamentu in Svetu: Politika EU za kibernetsko obrambo, JOIN(2022)0049.

3 Uredba (EU) 2021/694 Evropskega parlamenta in Sveta z dne 29. aprila 2021 o vzpostavitvi programa Digitalna Evropa in razveljavitvi Sklepa (EU) 2015/2240 (UL L 166, 11.5.2021, str. 1).

(9) Financiranje ukrepov na podlagi te uredbe bi bilo treba določiti v Uredbi (EU) 2021/694, ki bi morala biti še naprej ustrezen temeljni akt za te ukrepe, določene v okviru specifičnega cilja 3 programa Digitalna Evropa. V skladu z veljavno določbo Uredbe (EU) 2021/694 bodo v zvezi z vsakim ukrepom v ustreznih delovnih programih določeni posebni pogoji za sodelovanje.

(9a) Glede na geopolitični razvoj dogodkov in krajino z vse več kibernetskimi grožnjami (PPE 52), pa tudi za zagotovitev, da se bodo ukrepi iz te uredbe, zlasti evropski ščit za kibernetsko varnost in mehanizem za izredne kibernetskovarnostne razmere, izvajali in nadalje razvijali tudi po letu 2027, je treba poskrbeti, da bo v večletnem finančnem okviru za obdobje 2028–2034 v ta namen predvidena posebna proračunska vrstica. Države članice bi se morale skušati zavezati, da bodo podprle vse ukrepe, potrebne za zmanjšanje kibernetskih groženj in incidentov po vsej Uniji ter za okrepitev solidarnosti.

(10) Za to uredbo se uporabljajo horizontalna finančna pravila, ki sta jih Evropski parlament in Svet sprejela na podlagi člena 322 PDEU. Ta pravila so navedena v Uredbi ***(EU, Euratom) 2018/1046 Evropskega parlamenta in Sveta***[1] in določajo zlasti postopek za določitev in izvrševanje proračuna Unije ter urejajo nadzor nad odgovornostmi finančnih udeležencev. Pravila, sprejeta na podlagi člena 322 PDEU, vključujejo tudi splošni režim pogojenosti za zaščito proračuna Unije, kot je določen v Uredbi (EU, Euratom) 2020/2092 Evropskega parlamenta in Sveta[2].

(11) Za dobro finančno poslovodenje bi bilo treba določiti posebna pravila za prenos neporabljenih odobritev za prevzem obveznosti in odobritev plačil. Ob upoštevanju načela, da se proračun Unije določi vsako leto, bi bilo treba s to uredbo zaradi nepredvidljive, izjemne in posebne narave kibernetskovarnostne krajine zagotoviti možnosti za prenos neporabljenih sredstev, ki presegajo tiste iz Uredbe ***(EU, Euratom) 2018/1046***, s čimer bi se čim bolj povečala zmogljivost mehanizma za izredne kibernetskovarnostne razmere za podporo državam članicam pri učinkovitem boju proti kibernetskim grožnjam.

(11a) Mehanizem za izredne kibernetskovarnostne razmere in kibernetskovarnostna rezerva EU, vzpostavljena s to uredbo, sta novi pobudi in pri pripravi večletnega finančnega okvira za obdobje 2021–2027 še nista bila predvidena, pri čemer bi moralo biti zmanjšanje financiranja drugih prednostnih nalog programa Digitalna Evropa kot posledica financiranja teh dveh pobud čim bolj omejeno. Znesek finančnih sredstev, namenjenih kibernetskovarnostni rezervi EU, bi bilo zato treba zmanjšati in črpati predvsem iz nedodeljenih razlik do zgornjih mej večletnega finančnega okvira ali mobilizirati prek netematskih posebnih instrumentov večletnega finančnega okvira. Če se sredstva dodelijo ali prerazporedijo iz obstoječih

---

1 ***Uredba (EU, Euratom) 2018/1046 Evropskega parlamenta in Sveta z dne 18. julija 2018 o finančnih pravilih, ki se uporabljajo za splošni proračun Unije, spremembi uredb (EU) št. 1296/2013, (EU) št. 1301/2013, (EU) št. 1303/2013, (EU) št. 1304/2013, (EU) št. 1309/2013, (EU) št. 1316/2013, (EU) št. 223/2014, (EU) št. 283/2014 in Sklepa št. 541/2014/EU ter razveljavitvi Uredbe (EU, Euratom) št. 966/2012 (UL L 193, 30.7.2018, str. 1), ELI: http://data.europa.eu/eli/reg/2018/1046/oj).***

2 ***Uredba (EU, Euratom) 2020/2092 Evropskega parlamenta in Sveta z dne 16. decembra 2020 o splošnem režimu pogojenosti za zaščito proračuna Unije (UL L 433 I, 22.12.2020, str. 1), ELI: http://data.europa.eu/eli/reg/2020/2092/oj).***

programov, bi morala biti ta sredstva omejena na absolutni minimum, da to ne bi negativno vplivalo na obstoječe programe, zlasti Erasmus+, in da bi zagotovili, da bodo lahko ti programi dosegli svoje zastavljene cilje.

(12) Za učinkovitejše preprečevanje in ocenjevanje kibernetskih groženj in incidentov ter odzivanje nanje ***in obnovitev po njih*** je treba razviti celovitejše znanje o grožnjah za kritična sredstva in infrastrukture na ozemlju Unije, vključno z njihovo geografsko porazdelitvijo, medsebojno povezanostjo in morebitnimi učinki v primeru kibernetskih napadov na te infrastrukture. ***Proaktiven pristop k prepoznavanju, blaženju in preprečevanju morebitnih kibernetskih groženj zajema večje zmogljivosti za boljše odkrivanje teh groženj, kar je potrebno, da se lahko napredne vztrajne grožnje končajo. Obveščevalni podatki o grožnjah so informacije, ki se zbirajo, analizirajo in razlagajo, da bi razumeli morebitne grožnje in tveganja. S tem, ko se analizirajo ogromne količine podatkov in preučijo povezave med njimi, se razodenejo vzorci, trendi in kazalniki ogroženosti, na podlagi kateri se lahko razkrijejo zlonamerne dejavnosti ali ranljivosti.*** Vzpostaviti bi bilo treba ***mrežo*** centrov za varnostne operacije (v nadaljnjem besedilu: evropski kibernetski ščit), ki bi jo sestavljalo več interoperabilnih čezmejnih platform, od katerih bi vsaka združevala več nacionalnih centrov za varnostne operacije. Ta infrastruktura bi morala služiti interesom in potrebam držav in Unije na področju kibernetske varnosti, spodbujati najsodobnejšo tehnologijo za napredno zbiranje podatkov in analitična orodja, okrepiti zmogljivosti kibernetskega odkrivanja in upravljanja ter zagotavljati situacijsko zavedanje v realnem času. ***Nacionalni center za varnostne operacije je centralizirana zmogljivost, pristojna za to, da ves čas zbira obveščevalne podatke o grožnjah in izboljšuje kibernetsko držo subjektov v nacionalni pristojnosti na področju kibernetske varnosti, tako da preprečuje, odkriva in analizira kibernetske grožnje.*** Namenjena bi morala biti boljšemu odkrivanju kibernetskovarnostnih groženj in incidentov ter tako dopolnjevati in podpirati subjekte in omrežja Unije, pristojne za krizno upravljanje v Uniji, zlasti organizacijsko mrežo EU za povezovanje v kibernetski krizi (v nadaljnjem besedilu: mreža EU-CyCLONe), kot je opredeljena v Direktivi (EU) 2022/2555 Evropskega parlamenta in Sveta[1].

(13) ***Za sodelovanje v kibernetskem ščitu bi morala*** vsaka država članica imenovati javni organ na nacionalni ravni, ki bi bil zadolžen za usklajevanje dejavnosti odkrivanja kibernetskih groženj v tej državi članici. ***Države članice se spodbuja, naj zmogljivosti nacionalnih centrov za varnostne operacije vključijo v svojo že obstoječo kibernetsko strukturo in upravljanje, da ne bi ustvarile dodatnih ravni upravljanja in da bi to uredbo uskladile z že obstoječo zakonodajo, vključno z Direktivo 2022/2555.*** Ti nacionalni centri za varnostne operacije bi morali delovati kot referenčna točka in točka dostopa na nacionalni ravni za sodelovanje ***zasebnih in javnih subjektov, zlasti njihovih nacionalnih centrov za varnostne operacije,*** v evropskem kibernetskem ščitu ter zagotoviti, da se informacije o kibernetskih grožnjah, ki jih predložijo javni in zasebni subjekti, na nacionalni ravni izmenjujejo in zbirajo na učinkovit in poenostavljen način. ***Nacionalni centri za varnostne operacije bi morali okrepiti sodelovanje in izmenjavo informacij med javnimi in zasebnimi subjekti, da bi odpravili sedanje komunikacijske ovire. Na ta način bi lahko podprli razvoj modelov za izmenjavo podatkov ter bi morali***

[1] Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (direktiva NIS 2) (UL L 333, 27.12.2022, str. 80).

olajšati in spodbujati izmenjavo informacij v zaupanja vrednem in varnem okolju. Za krepitev odpornosti Unije na področju kibernetske varnosti je osrednjega pomena, da javni in zasebni subjekti tesno in usklajeno sodelujejo med seboj.

(14) V okviru evropskega kibernetskega ščita bi bilo treba ustanoviti več čezmejnih centrov za varnostne operacije na področju kibernetske varnosti. Ti bi morali združevati nacionalne centre za varnostne operacije iz vsaj treh držav članic, da bi lahko v celoti izkoristili prednosti čezmejnega odkrivanja groženj ter izmenjave in upravljanja informacij. Splošna cilja čezmejnih centrov za varnostne operacije bi morala biti okrepitev zmogljivosti za analizo, preprečevanje in odkrivanje kibernetskovarnostnih groženj ter podpora pripravi visokokakovostnih obveščevalnih podatkov, ***vključno z zbiranjem in izmenjavo podatkov in informacij o morebitnih vdorih v računalniški sistem, novonastalih zlonamernih grožnjah in ukanah za izkoriščanje ranljivosti, ki še nikoli prej niso bile uporabljene v kibernetskih incidentih, ter dejavnostmi analize*** kibernetskovarnostnih ***groženj,*** zlasti z izmenjavo podatkov iz različnih virov, javnih ali zasebnih, pa tudi izmenjavo in skupno uporabo najsodobnejših orodij ter skupnim razvojem zmogljivosti za odkrivanje, analizo in preprečevanje v zaupanja vrednem ***in varnem*** okolju ***in ob podpori agencije ENISA, in sicer v zvezi z zadevami, povezanimi z operativnim sodelovanjem med državami članicami***. ***Čezmejni centri za varnostne operacije bi morali olajšati in spodbujati izmenjavo informacij v zaupanja vrednem in varnem okolju ter*** zagotoviti nove dodatne zmogljivosti, ki bi temeljile na obstoječih centrih za varnostne operacije in skupinah za odzivanje na incidente na področju računalniške varnosti (v nadaljnjem besedilu: skupine CSIRT) ter drugih ustreznih akterjih in jih dopolnjevale.

(15) Spremljanje, odkrivanje in analizo kibernetskih groženj na nacionalni ravni običajno zagotavljajo centri za varnostne operacije, ki jih sestavljajo javni in zasebni subjekti, v povezavi s skupinami CSIRT. Poleg tega si skupine CSIRT informacije izmenjujejo v okviru mreže skupin CSIRT v skladu z Direktivo (EU) 2022/2555. Čezmejni centri za varnostne operacije bi morali predstavljati novo zmogljivost***, vključeno v obstoječo infrastrukturo za kibernetsko varnost, zlasti*** v mrežo skupin CSIRT, in sicer z zbiranjem in izmenjavo podatkov javnih in zasebnih subjektov, ***zlasti njihovih centrov za varnostne operacije,*** o kibernetskovarnostnih grožnjah, s povečevanjem vrednosti takih podatkov s strokovno analizo ter skupno pridobljenimi infrastrukturami in najsodobnejšimi orodji ter s prispevanjem ***k tehnološki suverenosti, odprti strateški avtonomiji, konkurenčnosti in odpornosti Unije ter k razvoju pomembnega ekosistema kibernetske varnosti, tudi v sodelovanju z zaupanja vrednimi in podobno mislečimi mednarodnimi partnerji***. .

(16) Čezmejni centri za varnostne operacije bi morali delovati kot osrednja točka, ki bi omogočala obsežno zbiranje ustreznih podatkov in obveščevalnih podatkov o kibernetskih grožnjah ter širjenje informacij o grožnjah med velikim in raznolikim naborom akterjev (npr. skupinami za odzivanje na računalniške grožnje (v nadaljnjem besedilu: skupine CERT), skupinami CSIRT, centri za izmenjavo in analizo informacij, upravljavci kritičnih infrastruktur***), da bi omogočili lažjo odpravo sedanjih komunikacijskih ovir***. ***Na ta način bi lahko čezmejni centri za varnostne operacije tudi podprli razvoj modelov za izmenjavo podatkov po vsej Uniji.*** Informacije, ki si jih izmenjujejo sodelujoči v čezmejnem centru za varnostne operacije, bi lahko vključevale podatke iz omrežij in senzorjev, obveščevalne podatke o grožnjah, kazalnike ogroženosti ter kontekstualizirane informacije o incidentih, grožnjah in ranljivostih***, vključno z zbiranjem in izmenjavo podatkov in informacij o morebitnih vdorih v***

računalniški sistem, novonastalih zlonamernih grožnjah in ukanah za izkoriščanje ranljivosti, ki še nikoli prej niso bile uporabljene v kibernetskih incidentih, ter dejavnostmi analize. Poleg tega bi morali čezmejni centri za varnostne operacije skleniti tudi sporazume o sodelovanju z drugimi čezmejnimi centri za varnostne operacije.

(17) Skupno situacijsko zavedanje med ustreznimi organi je nujen osnovni pogoj za pripravljenost in usklajevanje na ravni Unije v zvezi s pomembnimi kibernetskovarnostnimi incidenti in takimi incidenti velikih razsežnosti. Z Direktivo (EU) 2022/2555 je ustanovljena mreža EU-CyCLONe za podporo usklajenemu obvladovanju kibernetskovarnostnih incidentov velikih razsežnosti in kriz na operativni ravni ter zagotovitev redne izmenjave ustreznih informacij med državami članicami ter institucijami, organi in agencijami Unije. V Priporočilu (EU) 2017/1584 o usklajenem odzivu na velike kibernetske incidente in krize je obravnavana vloga vseh ustreznih akterjev. V Direktivi (EU) 2022/2555 je tudi opozorjeno na odgovornosti Komisije v okviru mehanizma Unije na področju civilne zaščite, vzpostavljenega s Sklepom 1313/2013/EU Evropskega parlamenta in Sveta[1], ter za pripravo analitičnih poročil o enotni ureditvi za politično odzivanje na krize (IPCR) v skladu z Izvedbenim sklepom ***Sveta*** (EU) 2018/1993[2]. Zato bi morali čezmejni centri za varnostne operacije v primerih, ko pridobijo informacije v zvezi z morebitnim ali tekočim kibernetskovarnostnim incidentom velikih razsežnosti, mreži EU-CyCLONe, mreži skupin CSIRT in Komisiji ***v skladu z Direktivo (EU) 2022/2555*** zagotoviti ustrezne informacije. Glede na okoliščine bi lahko informacije, ki jih je treba izmenjati, vključevale zlasti tehnične informacije, informacije o naravi in motivih napadalca ali morebitnega napadalca ter netehnične informacije na višji ravni o morebitnem ali tekočem kibernetskovarnostnem incidentu velikih razsežnosti. V zvezi s tem bi bilo treba ustrezno upoštevati načelo potrebe po seznanitvi in morda občutljivo naravo izmenjanih informacij.

(18) Subjekti, ki sodelujejo v evropskem kibernetskem ščitu, bi morali zagotoviti visoko raven medsebojne interoperabilnosti, po potrebi tudi, kar zadeva formate podatkov, taksonomijo ter orodja za obravnavanje in analizo podatkov, pa tudi varne komunikacijske kanale, minimalno raven varnosti aplikacijske plasti, pregled situacijskega zavedanja in kazalnike. Pri sprejetju skupne taksonomije in oblikovanju predloge za poročila o razmerah za opis tehničnega vzroka in posledic kibernetskovarnostnih incidentov bi bilo treba upoštevati tekoče delo v zvezi s priglasitvijo incidentov v okviru izvajanja Direktive (EU) 2022/2555.

(19) Da bi omogočili obsežno izmenjavo podatkov o kibernetskovarnostnih grožnjah iz različnih virov v zaupanja vrednem ***in varnem*** okolju, bi morali biti subjekti, ki sodelujejo v evropskem kibernetskem ščitu, opremljeni z najsodobnejšimi in izjemno varnimi orodji, opremo in infrastrukturami ***ter usposobljenim osebjem***. To bi moralo omogočiti izboljšanje skupnih zmogljivosti za odkrivanje in pravočasno opozarjanje organov in ustreznih subjektov, zlasti z uporabo najnovejših tehnologij umetne inteligence in podatkovne analitike.

---

1 ***Sklep št. 1313/2013/EU Evropskega parlamenta in Sveta z dne 17. decembra 2013 o mehanizmu Unije na področju civilne zaščite (Besedilo velja za EGP) (***UL L 347, 20.12.2013, str. 924, ***ELI:*** http://data.europa.eu/eli/dec/2013/1313/oj***).***

2 ***Izvedbeni sklep Sveta (EU) 2018/1993 z dne 11. decembra 2018 o enotni ureditvi EU za politično odzivanje na krize (UL L 320, 17.12.2018, str. 28, ELI: http://data.europa.eu/eli/dec_impl/2018/1993/oj).***

(20) Evropski kibernetski ščit bi moral z zbiranjem, deljenjem in izmenjavanjem podatkov okrepiti tehnološko suverenost***, odprto strateško avtonomijo, konkurenčnost in odpornost*** Unije***, pa tudi pomemben kibernetskovarnostni ekosistem EU***. Zbiranje visokokakovostnih pripravljenih podatkov bi moralo prispevati tudi k razvoju naprednih tehnologij umetne inteligence in podatkovne analitike. ***Umetna inteligenca deluje najbolj učinkovito v kombinaciji s človeško analizo. Zato ima usposobljena delovna sila še vedno ključno vlogo pri zbiranju visokokakovostnih podatkov.*** Olajšati bi ga bilo treba tako, da se evropski kibernetski ščit poveže z infrastrukturo vseevropskega visokozmogljivostnega računalništva, vzpostavljenega z Uredbo Sveta (EU) 2021/1173[1].

(21) Čeprav je evropski kibernetski ščit civilni projekt, bi lahko imela skupnost za kibernetsko obrambo koristi od okrepljenih zmogljivosti civilnega odkrivanja in situacijskega zavedanja, ki so bile razvite za zaščito kritične infrastrukture. Čezmejni centri za varnostne operacije bi morali ob podpori Komisije in Evropskega kompetenčnega centra za kibernetsko varnost (v nadaljnjem besedilu: ECCC) ter v sodelovanju z visokim predstavnikom Unije za zunanje zadeve in varnostno politiko (v nadaljnjem besedilu: visoki predstavnik) postopoma razviti namenske ***pogoje dostopa*** ter protokole in standarde ***zaščitnih ukrepov***, da se omogoči sodelovanje s skupnostjo za kibernetsko obrambo, vključno s pogoji preverjanja in varnostnimi pogoji***, pri čemer morajo upoštevati civilni značaj institucij in namembnost financiranja, posledično pa uporabljati sredstva, ki so na voljo obrambni skupnosti***. Razvoj evropskega kibernetskega ščita bi moral spremljati razmislek, na podlagi katerega bi bilo v tesnem sodelovanju z visokim predstavnikom omogočeno prihodnje sodelovanje z mrežami in platformami, odgovornimi za izmenjavo informacij v skupnosti za kibernetsko obrambo***, pri čemer morajo biti v celoti spoštovane pravice in svoboščine***.

(22) Izmenjava informacij med sodelujočimi v evropskem kibernetskem ščitu bi morala biti skladna z obstoječimi pravnimi zahtevami, zlasti s pravom Unije in nacionalnim pravom o varstvu podatkov, ter pravili Unije o konkurenci, ki urejajo izmenjavo informacij. Če je potrebna obdelava osebnih podatkov, bi moral prejemnik informacij izvajati tehnične in organizacijske ukrepe, s katerimi se varujejo pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, in podatke uničiti takoj, ko niso več potrebni za navedeni namen, ter organ, ki daje podatke na voljo, obvestiti, da so bili podatki uničeni.

(23) Brez poseganja v člen 346 PDEU bi morala biti izmenjava informacij, ki so zaupne v skladu s ***pravom*** Unije ali ***nacionalnim pravom***, omejena na to, kar je ustrezno za namen te izmenjave in sorazmerno z njim. Pri izmenjavi takih informacij bi bilo treba ohraniti njihovo zaupnost ter zaščititi varnostne in poslovne interese zadevnih subjektov ob polnem spoštovanju trgovinskih in poslovnih skrivnosti.

(24) Glede na vse večja tveganja in število kibernetskovarnostnih incidentov, ki prizadenejo države članice, je treba vzpostaviti instrument podpore ob krizi, da se izboljša odpornost Unije proti pomembnim kibernetskovarnostnim incidentom in takim incidentom velikih razsežnosti ter da se ukrepi držav članic dopolnijo z nujno finančno podporo za pripravljenost, odzivanje in takojšnjo obnovitev bistvenih storitev. Ta instrument bi moral omogočiti hitro ***in učinkovito*** zagotavljanje pomoči v določenih okoliščinah in pod jasnimi pogoji ter skrbno spremljanje in ocenjevanje porabe sredstev. Čeprav so za

[1] Uredba Sveta (EU) 2021/1173 z dne 13. julija 2021 o ustanovitvi Skupnega podjetja za evropsko visokozmogljivostno računalništvo in razveljavitvi Uredbe (EU) 2018/1488 (UL L 256, 19.7.2021, str. 3, ***ELI: http://data.europa.eu/eli/reg/2021/1173/oj***).

preprečevanje kibernetskovarnostnih incidentov in kriz ter pripravo in odzivanje nanje v prvi vrsti odgovorne države članice, mehanizem za izredne ***kibernetskovarnostne*** razmere spodbuja solidarnost med državami članicami v skladu s členom 3(3) Pogodbe o Evropski uniji (PEU).

(25) Mehanizem za izredne ***kibernetskovarnostne*** razmere bi moral državam članicam zagotoviti podporo z dopolnjevanjem njihovih ukrepov in virov ter druge obstoječe možnosti podpore v primeru odziva na pomembne kibernetskovarnostne incidente in take incidente velikih razsežnosti ter takojšnje obnovitve po njih, kot so storitve, ki jih zagotavlja Agencija Evropske unije za kibernetsko varnost (ENISA) v skladu s svojim mandatom, usklajen odziv in pomoč mreže skupin CSIRT, podpora mreže EU-CyCLONe pri ublažitvi posledic ter medsebojna pomoč med državami članicami, med drugim v okviru člena 42(7) PEU, enot za hitro odzivanje na kibernetske grožnje v okviru stalnega strukturnega sodelovanja (PESCO)[1] in skupin za hitro odzivanje na hibridne grožnje. Obravnavati bi moral potrebo po zagotavljanju razpoložljivosti specializiranih sredstev za podporo pripravljenosti in odzivanju na kibernetskovarnostne incidente po vsej Uniji in v tretjih državah.

(26) Ta instrument ne posega v postopke in okvire za usklajevanje odzivanja na krize na ravni Unije, zlasti mehanizem Unije na področju civilne zaščite[2], enotno ureditev za politično odzivanje na krize[3] in Direktivo (EU) 2022/2555. Prispeva lahko k ukrepom, ki se izvajajo v okviru člena 42(7) PEU ali v primerih, opredeljenih v členu 222 PDEU, ali jih dopolnjuje. Uporabo tega instrumenta bi bilo treba po potrebi uskladiti tudi z izvajanjem ukrepov iz zbirke orodij za kibernetsko diplomacijo.

(27) Pomoč, zagotovljena na podlagi te uredbe, bi morala podpirati in dopolnjevati ukrepe, ki jih države članice sprejmejo na nacionalni ravni. V ta namen bi bilo treba zagotoviti tesno sodelovanje in posvetovanje med Komisijo***, agencijo ENISA*** in prizadeto državo članico. Kadar država članica zaprosi za podporo v okviru mehanizma za izredne ***kibernetskovarnostne*** razmere, bi morala predložiti ustrezne informacije, s katerimi utemelji potrebo po podpori.

(28) V skladu z Direktivo (EU) 2022/2555 morajo države članice imenovati ali ustanoviti enega ali več organov za obvladovanje kibernetskih kriz ter jim zagotoviti ustrezna sredstva za učinkovito in uspešno izvajanje nalog. Države članice morajo tudi določiti zmogljivosti, sredstva in postopke, ki se lahko uporabijo v primeru krize, ter sprejeti nacionalni načrt za odzivanje na kibernetskovarnostne incidente velikih razsežnosti in krize, v katerem so opredeljeni cilji in ureditve obvladovanja kibernetskovarnostnih incidentov velikih razsežnosti in kriz. Prav tako morajo ustanoviti eno ali več skupin CSIRT, ki bodo pristojne za obvladovanje incidentov v skladu z natančno določenim postopkom in bodo zajemale vsaj sektorje, podsektorje in vrste subjektov, ki spadajo na področje uporabe navedene direktive, ter jim zagotoviti ustrezna sredstva za učinkovito izvajanje nalog. Ta uredba ne posega v vlogo Komisije pri zagotavljanju skladnosti držav članic z obveznostmi iz Direktive (EU) 2022/2555. Mehanizem za izredne

---

1 Sklep Sveta (SZVP) 2017/2315 z dne 11. decembra 2017 o vzpostavitvi stalnega strukturnega sodelovanja (PESCO) in določitvi seznama vključenih držav članic.

2 Sklep št. 1313/2013/EU Evropskega parlamenta in Sveta z dne 17. decembra 2013 o mehanizmu Unije na področju civilne zaščite (UL L 347, 20.12.2013, str. 924).

3 Enotna ureditev za politično odzivanje na krize (IPCR) in v skladu s Priporočilom Komisije (EU) 2017/1584 z dne 13. septembra 2017 o usklajenem odzivu na velike kibernetske incidente in krize.

kibernetskovarnostne razmere bi moral zagotavljati pomoč za ukrepe, namenjene krepitvi pripravljenosti, in ukrepe za odzivanje na incidente, da bi ublažili posledice pomembnih kibernetskovarnostnih incidentov in takih incidentov velikih razsežnosti, podprli takojšnjo obnovitev in/ali ponovno vzpostavili delovanje bistvenih storitev.

(29) V okviru ukrepov pripravljenosti bi bilo treba za spodbujanje doslednega pristopa ter krepitev varnosti po vsej Uniji in na njenem notranjem trgu zagotoviti podporo za usklajeno preskušanje in ocenjevanje kibernetske varnosti subjektov, ki delujejo v visoko kritičnih sektorjih, opredeljenih v skladu z Direktivo (EU) 2022/2555. V ta namen bi morala Komisija ob podpori agencije ENISA in v sodelovanju s skupino za sodelovanje na področju varnosti omrežnih in informacijskih sistemov, ustanovljeno z Direktivo (EU) 2022/2555, redno določati ustrezne sektorje ali podsektorje, ki bi morali biti upravičeni do finančne podpore za usklajeno preskušanje na ravni Unije. Sektorje ali podsektorje bi bilo treba izbrati iz Priloge I k Direktivi (EU) 2022/2555 (v nadaljnjem besedilu: visoko kritični sektorji). Usklajeno preskušanje bi moralo temeljiti na skupnih scenarijih tveganja in metodologijah. Pri izbiri sektorjev in razvoju scenarijev tveganja bi bilo treba upoštevati ustrezne ocene tveganja in scenarije tveganja po vsej Uniji, vključno s potrebo po preprečevanju podvajanja, kot so ocena tveganja in scenariji tveganja, h katerim poziva Svet v svojih sklepih o oblikovanju kibernetske drže Evropske unije in ki jih morajo izvesti Komisija, visoki predstavnik in skupina za sodelovanje na področju varnosti omrežnih in informacijskih sistemov v sodelovanju z ustreznimi civilnimi in vojaškimi organi in agencijami ter vzpostavljenimi mrežami, med drugim mrežo EU-CyCLONe, pa tudi ocena tveganja komunikacijskih omrežij in infrastruktur, ki se zahteva na podlagi skupnega ministrskega poziva iz Neversa ter jo izvede skupina za sodelovanje na področju varnosti omrežnih in informacijskih sistemov ob podpori Komisije in agencije ENISA ter v sodelovanju z Organom evropskih regulatorjev za elektronske komunikacije (BEREC), usklajene ocene tveganja, ki se izvedejo v skladu s členom 22 Direktive (EU) 2022/2555, in testiranje digitalne operativne odpornosti, kot je določeno v Uredbi (EU) 2022/2554 Evropskega parlamenta in Sveta[1]. Pri izbiri sektorjev bi bilo treba upoštevati tudi priporočilo Sveta o usklajenem vseevropskem pristopu za krepitev odpornosti kritične infrastrukture.

(30) Poleg tega bi moral mehanizem za izredne ***kibernetskovarnostne*** razmere zagotavljati podporo za druge ukrepe pripravljenosti in podpirati pripravljenost v drugih sektorjih, ki jih usklajeno preskušanje subjektov, ki delujejo v visoko kritičnih sektorjih, ne zajema. Ti ukrepi bi lahko vključevali različne vrste nacionalnih dejavnosti na področju pripravljenosti.

(31) Mehanizem za izredne ***kibernetskovarnostne*** razmere bi moral zagotavljati tudi podporo za ukrepe za odzivanje na incidente za ublažitev posledic pomembnih kibernetskovarnostnih incidentov in takih incidentov velikih razsežnosti, da bi se podprla takojšnja obnovitev ali ponovna vzpostavitev delovanja bistvenih storitev. Kjer je ustrezno, bi moral dopolnjevati mehanizem Unije na področju civilne zaščite, da se zagotovi celovit pristop k odzivanju na posledice kibernetskih incidentov za državljane.

(32) Mehanizem za izredne ***kibernetskovarnostne*** razmere bi moral podpreti pomoč, ki jo države članice zagotovijo državi članici, ki jo je prizadel pomemben

[1] Uredba (EU) 2022/2554 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o digitalni operativni odpornosti za finančni sektor in spremembi uredb (ES) št. 1060/2009, (EU) št. 648/2012, (EU) št. 600/2014, (EU) št. 909/2014 in (EU) 2016/1011.

kibernetskovarnostni incident ali tak incident velikih razsežnosti, med drugim pomoč mreže skupin CSIRT iz člena 15 Direktive (EU) 2022/2555. Državam članicam, ki zagotovijo pomoč, bi bilo treba dovoliti, da vložijo zahtevke za kritje stroškov, povezanih s pošiljanjem strokovnih skupin v okviru medsebojne pomoči. Upravičeni stroški bi lahko vključevali potne stroške, stroške nastanitve in dnevnice strokovnjakov na področju kibernetske varnosti.

(33) Postopno bi bilo treba vzpostaviti kibernetskovarnostno rezervo na ravni Unije, ki bi zajemala storitve zasebnih ponudnikov upravljanih varnostnih storitev za podporo ukrepom odzivanja in takojšnje obnovitve v primeru pomembnih kibernetskovarnostnih incidentov ali takih incidentov velikih razsežnosti. Kibernetskovarnostna rezerva EU bi morala zagotoviti razpoložljivost in pripravljenost storitev***, hkrati pa krepiti odpornost Unije, vključno s sodelovanjem evropskih ponudnikov upravljanih varnostnih storitev, ki so MSP, in zagotavljanjem vzpostavitve ekosistema kibernetske varnosti, zlasti mikropodjetij, MSP, vključno z zagonskimi podjetji, z naložbami v raziskave in inovacije za razvoj najsodobnejših tehnologij, kot so tehnologije, povezane z računalništvom v oblaku in umetno inteligenco***. ***Zaupanja vredni ponudniki, vključno z MSP, bi morali imeti možnost, da za namene izpolnitve zgoraj navedenih meril sodelujejo drug z drugim.*** Storitve iz kibernetskovarnostne rezerve EU bi morale biti kot dopolnitev ukrepov nacionalnih organov na nacionalni ravni namenjene podpori tem organom pri zagotavljanju pomoči prizadetim subjektom, ki delujejo v kritičnih ali visoko kritičnih sektorjih. ***Zato bi bilo treba v sklopu kibernetskovarnostne rezerve spodbujati naložbe v raziskave in inovacije, da bi pospešili razvoj teh tehnologij. Po potrebi bi se lahko izvedle skupne vaje z zaupanja vrednimi ponudniki in potencialnimi uporabniki kibernetskovarnostne rezerve, da bi po potrebi zagotovili njeno učinkovito delovanje.*** Države članice bi morale ob vložitvi zahtevka za podporo iz kibernetskovarnostne rezerve EU opredeliti podporo, zagotovljeno prizadetemu subjektu na nacionalni ravni, ki bi jo bilo treba upoštevati pri oceni zahtevka države članice. Storitve iz kibernetskovarnostne rezerve EU se lahko pod podobnimi pogoji uporabljajo tudi za podporo institucijam, organom, uradom in agencijam Unije. ***Komisija bi morala poskrbeti za vključenost držav članic in obsežne izmenjave z njimi, da ne bi prišlo do podvajanja s podobnimi pobudami, tudi v okviru Organizacije Severnoatlantske pogodbe (NATO).***

(34) Za izbor zasebnih ponudnikov storitev, ki bi storitve zagotavljali v okviru kibernetskovarnostne rezerve EU, je treba določiti sklop minimalnih meril, ki bi jih bilo treba vključiti v razpis za zbiranje ponudb za izbor teh ponudnikov, da se lahko zadosti potrebam organov držav članic in subjektov, ki delujejo v kritičnih ali visoko kritičnih sektorjih. ***Spodbujati je treba sodelovanje manjših ponudnikov, dejavnih na regionalni in lokalni ravni.***

(35) Komisija bi lahko za podporo vzpostavitvi kibernetskovarnostne rezerve EU preučila možnost, da od agencije ENISA zahteva, naj pripravi predlog certifikacijske sheme v skladu z Uredbo (EU) 2019/881 za upravljane varnostne storitve na področjih, ki jih zajema mehanizem za izredne ***kibernetskovarnostne*** razmere. ***Da bi lahko izpolnila dodatne naloge, ki izhajajo iz te določbe, bi morala agencija ENISA prejeti ustrezna dodatna sredstva.***

(36) Za podporo ciljem te uredbe glede spodbujanja skupnega situacijskega zavedanja, krepitve odpornosti Unije ter omogočanja učinkovitega odziva na pomembne kibernetskovarnostne incidente in take incidente velikih razsežnosti bi bilo treba mreži EU-CyCLONe, mreži skupin CSIRT ali Komisiji omogočiti, da agencijo ENISA

zaprosijo, naj pregleda in oceni grožnje, ranljivosti in blažitvene ukrepe v zvezi s posameznim pomembnim kibernetskovarnostnim incidentom ali takim incidentom velikih razsežnosti. Po zaključku pregleda in ocene incidenta bi morala agencija ENISA v sodelovanju z ustreznimi deležniki, vključno s predstavniki iz zasebnega sektorja, držav članic, Komisije in drugih ustreznih institucij, organov, uradov in agencij EU, pripraviti poročilo o pregledu incidenta. Kar zadeva zasebni sektor, agencija ENISA razvija kanale za izmenjavo informacij s specializiranimi ponudniki, vključno s ponudniki upravljanih varnostnih rešitev in prodajalci, da bi prispevala k svojemu poslanstvu doseganja visoke skupne ravni kibernetske varnosti po vsej Uniji. Cilj poročila o pregledu posameznih incidentov, ki temelji na sodelovanju z deležniki, vključno z zasebnim sektorjem, bi moral biti ocena vzrokov, posledic in blažitev incidenta po njegovem nastanku. Posebno pozornost bi bilo treba nameniti prispevku in spoznanjem, ki si jih izmenjujejo ponudniki upravljanih varnostnih storitev, ki izpolnjujejo pogoje največje poklicne integritete, nepristranskosti in potrebnega tehničnega strokovnega znanja, kot se zahtevajo s to uredbo. Poročilo bi bilo treba predložiti mreži EU-CyCLONe, mreži skupin CSIRT in Komisiji, pri čemer bi ga te morale upoštevati pri svojem delu. Če je incident povezan s tretjo državo, bo Komisija poročilo poslala tudi visokemu predstavniku.

(37) Ob upoštevanju nepredvidljive narave kibernetskih napadov in dejstva, da ti pogosto niso omejeni na določeno geografsko območje in da predstavljajo veliko tveganje prelivanja, krepitev odpornosti sosednjih držav in njihove zmogljivosti za učinkovito odzivanje na pomembne kibernetskovarnostne incidente in take incidente velikih razsežnosti prispeva k zaščiti Unije kot celote. Zato lahko podporo iz kibernetskovarnostne rezerve EU prejmejo tretje države, pridružene programu Digitalna Evropa, če je to določeno v ustreznih sporazumih o pridružitvi programu Digitalna Evropa. Unija bi morala financiranje za pridružene tretje države podpreti v okviru ustreznih partnerstev in instrumentov financiranja za te države. Podpora bi morala zajemati storitve na področju odzivanja na pomembne kibernetskovarnostne incidente ali take incidente velikih razsežnosti in takojšnje obnovitve po njih. Pri zagotavljanju podpore tretjim državam, pridruženim programu Digitalna Evropa, bi morali veljati pogoji, določeni za kibernetskovarnostno rezervo EU in zaupanja vredne ponudnike v tej uredbi.

(37a) Tretje države bi lahko prek podpore pri odzivanju na incidente iz kibernetskovarnostne rezerve EU dostopale do virov in podpore v skladu s to uredbo. Poleg tega utegnejo biti za zagotavljanje specifičnih storitev v sklopu kibernetskovarnostne rezerve EU potrebni ponudniki storitev odzivanja na incidente iz tretjih držav, vključno s tretjimi državami, pridruženimi programu Digitalna Evropa, ali drugih mednarodnih partnerskih držav in članic Nata. Z odstopanjem od Uredbe (EU, Euratom) 2018/1046 ter da bi okrepili tehnološko suverenost, odprto strateško avtonomijo, konkurenčnost in odpornost Unije ter zaščitili njena strateška sredstva, interese ali varnost, subjektom s sedežem v tretjih državah, ki niso pogodbenice Sporazuma o javnih naročilih in v zvezi s katerimi ni bil izveden pregled v smislu Uredbe (EU) 2019/452 Evropskega parlamenta in Sveta[1] in po potrebi v zvezi s katerimi niso bili izvedeni ukrepi za zmanjšanje tveganj, ob upoštevanju ciljev iz te uredbe ne bi smelo biti dovoljeno sodelovati. Zunanja razsežnost te uredbe bi morala

[1] ***Uredba (EU) 2019/452 Evropskega parlamenta in Sveta z dne 19. marca 2019 o vzpostavitvi okvira za pregled neposrednih tujih naložb v Uniji (UL L 79 I, 21.3.2019, str. 1, ELI: http://data.europa.eu/eli/reg/2019/452/oj).***

biti skladna z določbami iz pridružitvenega sporazuma v okviru programa Digitalna Evropa. Da se zagotovi, da lahko državljani sodelujejo pri tem procesu, bi morala nadzor nad sodelovanjem tretjih držav izvajati javnost skupaj z akterji z zakonodajnimi pooblastili.

(38) Za zagotovitev enotnih pogojev za izvajanje te uredbe bi bilo treba na Komisijo prenesti izvedbena pooblastila za določitev pogojev za interoperabilnost med čezmejnimi centri za varnostne operacije; določitev postopkovnih ureditev za izmenjavo informacij v zvezi z morebitnim ali tekočim kibernetskovarnostnim incidentom velikih razsežnosti med čezmejnimi centri za varnostne operacije in subjekti Unije; določitev tehničnih zahtev za zagotovitev varnosti evropskega kibernetskega ščita; določi vrste in število storitev za odzivanje, potrebnih za kibernetskovarnostno rezervo EU; in natančneje določi podrobne ureditve za dodeljevanje storitev podpore iz kibernetskovarnostne rezerve EU. Ta pooblastila bi bilo treba izvajati v skladu z Uredbo (EU) 182/2011 Evropskega parlamenta in Sveta*.

---

* ***Uredba (EU) št. 182/2011 Evropskega parlamenta in Sveta z dne 16. februarja 2011 o določitvi splošnih pravil in načel, na podlagi katerih države članice nadzirajo izvajanje izvedbenih pooblastil Komisije (UL L 55, 28.2.2011, str. 13, ELI: https://eur-lex.europa.eu/eli/reg/2011/182/oj?locale=sl).***

(38a) Usposobljeno osebje, ki lahko zanesljivo zagotavlja ustrezne storitve kibernetske varnosti po najvišjih standardih, je nujno za učinkovito izvajanje evropskega kibernetskega ščita in mehanizma za izredne kibernetskovarnostne razmere. Zato je zaskrbljujoče, da se Unija sooča z vrzeljo nadarjenih posameznikov, za katero je značilno pomanjkanje usposobljenih strokovnjakov, hkrati pa se sooča s hitro spreminjajočim se okoljem groženj, kot je navedeno v sporočilu Komisije z dne 18. aprila 2023 o akademiji za kibernetske veščine. Pomembno je premostiti to vrzel na področju talentov s krepitvijo sodelovanja in usklajevanja med različnimi deležniki, vključno z zasebnim sektorjem, akademskim svetom, državami članicami, Komisijo in agencijo ENISA, da bi povečali in ustvarili sinergije na vsem ozemlju za naložbe v izobraževanje in usposabljanje, razvoj javno-zasebnih partnerstev, podporo pobudam na področju raziskav in inovacij, razvoj in vzajemno priznavanje skupnih standardov ter certificiranje znanj in spretnosti na področju kibernetske varnosti, tudi prek evropskega okvira znanj in spretnosti za kibernetsko varnost. To bi moralo olajšati tudi mobilnost strokovnjakov za kibernetsko varnost v Uniji. Cilj te uredbe bi moral biti spodbujanje bolj raznolike delovne sile na področju kibernetske varnosti. Vsi ukrepi za povečanje znanj in spretnosti na področju kibernetske varnosti zahtevajo zaščitne ukrepe, da se prepreči beg možganov in grožnja mobilnosti delovne sile.

(38b) Po vsej Uniji je treba okrepiti specializirane, interdisciplinarne in splošne veščine ter kompetence, s posebnim poudarkom na ženskah, saj še vedno obstajajo razlike med spoloma, ker so ženske na področju kibernetske varnosti na svetovni ravni v povprečju zastopane v deležu 20 %. Ženske morajo biti zastopane ter vključene v oblikovanje digitalne prihodnosti in njeno upravljanje.

(38c) Namen krepitve raziskav in inovacij na področju kibernetske varnosti je povečati odpornost in odprto strateško avtonomijo Unije. Prav tako je pomembno ustvariti sinergije s programi za raziskave in inovacije in obstoječimi instrumenti ter institucijami in povečati sodelovanje ter usklajevanje med različnimi deležniki,

vključno z zasebnim sektorjem, civilno družbo, akademskim svetom, državami članicami, Komisijo in agencijo ENISA;

(38d) Ta uredba bi morala prispevati k zavezi evropske deklaracije o digitalnih pravicah in načelih za digitalno desetletje v zvezi z zaščito interesov naših demokracij, ljudi, podjetij in javnih institucij pred tveganji za kibernetsko varnost in kibernetsko kriminaliteto, vključno s kršitvami varstva podatkov in krajo identitete ali poseganjem vanjo. Uporaba te uredbe bi morala prispevati tudi k boljšemu izvajanju druge zakonodaje, na primer na področju umetne inteligence, zasebnosti podatkov in urejanja podatkov v smislu kibernetske varnosti in kibernetske odpornosti.

(38e) Za uspešno izvajanje te uredbe bo ključnega pomena okrepiti kulturo kibernetske varnosti, ki varnost, med drugim tudi varnost digitalnega okolja, razume kot javno dobro. Zato bi moral biti razvoj ukrepov, s katerimi bo vključena in povečana ozaveščenosti državljanov, še eno sredstvo za zaščito naših demokracij in temeljnih vrednot.

(38f) Za dopolnitev nekaterih nebistvenih elementov te uredbe bi bilo treba na Komisijo prenesti pooblastilo, da v skladu s členom 290 PDEU sprejme akte, s katerimi določi pogoje za interoperabilnost med čezmejnimi centri za varnostne operacije, določi postopkovne ureditve za izmenjavo informacij med čezmejnimi centri za varnostne operacije na eni strani ter mrežo skupin CSIRT in Komisijo na drugi strani, določi vrste in število storitev za odzivanje, potrebnih za kibernetskovarnostno rezervo EU, ter natančneje opredeli podrobne ureditve za dodelitev podpornih storitev iz kibernetskovarnostne rezerve EU. Zlasti je pomembno, da se Komisija pri pripravljalnem delu ustrezno posvetuje, tudi na ravni strokovnjakov, in da se ta posvetovanja izvedejo v skladu z načeli, določenimi v Medinstitucionalnem sporazumu z dne 13. aprila 2016 o boljši pripravi zakonodaje*. Za zagotovitev enakopravnega sodelovanja pri pripravi delegiranih aktov Evropski parlament in Svet zlasti prejmeta vse dokumente sočasno s strokovnjaki iz držav članic, njuni strokovnjaki pa se sistematično lahko udeležujejo sestankov strokovnih skupin Komisije, ki zadevajo pripravo delegiranih aktov.

****UL L 123, 12.5.2016, str. 1, ELI: https://eur-lex.europa.eu/eli/agree_interinstit/2016/512/oj?locale=sl***

(39) ***ker ciljev*** te uredbe***, in sicer okrepiti zmogljivosti Unije za preprečevanje in odkrivanje kibernetskih groženj ter odzivanje nanje in povečati zmogljivosti za obnovitev ter vzpostaviti splošni okvir za odpravo komunikacijskih silosov, ne morejo zadovoljivo doseči države članice,*** ampak jih je lažje doseči na ravni Unije. Zato lahko Unija sprejme ukrepe v skladu z načeloma subsidiarnosti in sorazmernosti iz člena 5 Pogodbe o Evropski uniji. ***V skladu z načelom sorazmernosti, kot je določeno v navedenem členu, ta*** uredba ne presega tistega, kar je potrebno za doseganje navedenega cilja–

SPREJELA NASLEDNJO UREDBO:

Poglavje I

SPLOŠNI CILJI, PREDMET UREJANJA IN OPREDELITVE POJMOV

Člen 1

Predmet urejanja in cilji

1. Ta uredba določa ukrepe za okrepitev zmogljivosti v Uniji za odkrivanje kibernetskovarnostnih groženj in incidentov ter pripravo in odzivanje nanje, ki se uresničujejo zlasti z naslednjimi ukrepi:

(a) vzpostavitvijo vseevropske ***mreže*** centrov za varnostne operacije (v nadaljnjem besedilu: evropski kibernetski ščit) za vzpostavitev in okrepitev skupnih zmogljivosti za odkrivanje in situacijsko zavedanje;

(b) vzpostavitvijo mehanizma za izredne kibernetske razmere za podporo državam članicam pri pripravi na pomembne kibernetskovarnostne incidente in take incidente velikih razsežnosti, odzivanju nanje in takojšnjem okrevanju po njih;

(c) vzpostavitvijo evropskega mehanizma za pregledovanje kibernetskovarnostnih incidentov za pregledovanje in ocenjevanje pomembnih incidentov ali incidentov velikih razsežnosti.

2. Cilj te uredbe je okrepiti solidarnost na ravni Unije z naslednjimi specifičnimi cilji:

(a) okrepiti skupno odkrivanje kibernetskih groženj in incidentov v Uniji ter situacijsko zavedanje o njih, da se tako ***podprejo industrijske zmogljivosti Unije in držav članic v kibernetskem sektorju ter*** okrepi konkurenčni položaj industrijskega ***sektorja***, ***zlasti mikropodjetij, MSP, ki vključujejo zagonska podjetja,*** in storitvenega sektorja v Uniji v celotnem spletnem gospodarstvu ter prispeva k tehnološki suverenosti Unije***, njeni odprti strateški avtonomiji, konkurenčnosti in odpornosti v tem sektorju, kar krepi ekosistem kibernetske varnosti, da bi zagotovili močne zmogljivosti Unije, med drugim sodelovanje z mednarodnimi partnerji***;

(b) okrepiti pripravljenost subjektov, ki delujejo v kritičnih in visoko kritičnih sektorjih po vsej Uniji, ter solidarnost z razvijanjem skupnih zmogljivosti za odzivanje na pomembne kibernetskovarnostne incidente ali take incidente velikih razsežnosti, med drugim z omogočanjem podpore Unije pri odzivanju na kibernetskovarnostne incidente tretjim državam, pridruženim programu Digitalna Evropa;

(c) povečati odpornost Unije in prispevati k učinkovitemu odzivu s pregledovanjem in ocenjevanjem pomembnih incidentov ali incidentov velikih razsežnosti, med drugim na podlagi pridobljenih spoznanj in po potrebi priporočil.

(ca) usklajeno razviti znanja, veščine in kompetence delovne sile, da bi zagotovili kibernetsko varnost in ustvarili sinergije z akademijo za kibernetske veščine.

3. Ta uredba ne posega v primarno odgovornost držav članic za nacionalno varnost, javno varnost ter preprečevanje, preiskovanje, odkrivanje in pregon kaznivih dejanj.

Člen 2

Opredelitev pojmov

V tej uredbi se uporabljajo naslednje opredelitve pojmov:

(-1a) „Nacionalni center za varnostne operacije“ pomeni centralizirano zmogljivost za stalno zbiranje in analiziranje obveščevalnih podatkov o grožnjah ter izboljševanje položaja kibernetske varnosti v skladu s členom 4;

(1) „**čezmejni center za varnostne operacije**“ pomeni večdržavno platformo, ki v usklajeni mrežni strukturi združuje nacionalne centre za varnostne operacije ***v skladu s členom 5***;

(2) **„javni organ“** pomeni ***osebe*** javnega prava, kot so opredeljene v členu 2(1), točka 4, Direktive 2014/24/EU Evropskega parlamenta in Sveta[1];

(3) **„gostiteljski konzorcij“** pomeni konzorcij sodelujočih držav, ki jih zastopajo nacionalni centri za varnostne operacije, ***v skladu s členom 5***;

(4) **„subjekt“** pomeni subjekt, kot je opredeljen v členu 6, točka 38, Direktive (EU) 2022/2555;

(4a) „kritični subjekt“ pomeni kritični subjekt, kot je opredeljen v členu 2(1) Direktive (EU) 2022/2557 Evropskega parlamenta in Sveta[2];

(5) **„subjekti, ki delujejo v kritičnih ali visoko kritičnih sektorjih“**, pomeni subjekte ***v sektorjih*** s seznamov v ***prilogah*** I in II k Direktivi (EU) 2022/2555;

(5a) „obvladovanje incidentov“ pomeni obvladovanje incidentov, kot je opredeljeno v členu 6, točka (8), Direktive (EU) 2022/2555;

(5b) „tveganje“ pomeni tveganje, kot je opredeljeno v členu 6, točka (9), Direktive (EU) 2022/2555;

(6) **„kibernetska grožnja“** pomeni kibernetsko grožnjo, kot je opredeljena v členu 2, točka 8, Uredbe (EU) 2019/881;

(6a) „pomembna kibernetska grožnja“ pomeni pomembno kibernetsko grožnjo, kot je opredeljena v členu 6, točka (11), Uredbe (EU) 2022/2555;

(7) **„pomemben kibernetskovarnostni incident“** pomeni kibernetskovarnostni incident, ki izpolnjuje merila iz člena 23(3) Direktive (EU) 2022/2555;

---

[1] Direktiva 2014/24/EU Evropskega parlamenta in Sveta z dne 26. februarja 2014 o javnem naročanju in razveljavitvi Direktive 2004/18/ES (UL L 94, 28.3.2014, str. 65).

[2] ***Direktiva (EU) 2022/2557 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o odpornosti kritičnih subjektov in razveljavitvi Direktive Sveta 2008/114/ES (UL L 333, 27.12.2022, str. 164, ELI: https://eur-lex.europa.eu/eli/dir/2022/2557/oj).***.

(8) **„kibernetskovarnostni incident velikih razsežnosti“** pomeni incident, kot je opredeljen v členu 6, točka 7, Direktive (EU)2022/2555;

(9) **„pripravljenost“** pomeni stanje pripravljenosti in zmogljivost za zagotovitev učinkovitega hitrega odziva na pomemben kibernetskovarnostni incident ali tak incident velikih razsežnosti, ki se doseže na podlagi vnaprej izvedene ocene tveganja in vnaprej sprejetih ukrepov za spremljanje;

(10) **„odziv“** pomeni ukrepanje v primeru pomembnega kibernetskovarnostnega incidenta ali takega incidenta velikih razsežnosti oziroma med takim incidentom ali po njem za odpravo njegovih takojšnjih in kratkoročnih negativnih posledic;

(10a) „ponudnik upravljanih varnostnih storitev“ pomeni ponudnika plačilnih storitev, kot je opredeljen v členu 6, točka 40, Direktive (EU) 2022/2555;

(11) **„zaupanja vredni ponudniki *upravljanih varnostnih storitev*“** pomeni ponudnike upravljanih varnostnih storitev***, izbrane za vključitev v kibernetskovarnostno rezervo EU*** v skladu s členom 16 te uredbe.

Poglavje II

EVROPSKI KIBERNETSKI ŠČIT

Člen 3

Vzpostavitev evropskega kibernetskega ščita

1. Vzpostavi se ***mreža*** centrov za varnostne operacije (v nadaljnjem besedilu: evropski kibernetski ščit) za razvoj naprednih zmogljivosti Unije za odkrivanje, analiziranje in obdelavo podatkov o kibernetskih grožnjah in ***preprečevanje incidentov*** v Uniji. Ščit sestavljajo vsi nacionalni centri za varnostne operacije in čezmejni centri za varnostne operacije.

Ukrepi za izvajanje evropskega kibernetskega ščita se podprejo s sredstvi iz programa Digitalna Evropa, izvajajo pa se v skladu z Uredbo (EU) 2021/694 in zlasti specifičnim ciljem 3 Uredbe.

2. Evropski kibernetski ščit:

(a) prek čezmejnih centrov za varnostne operacije zbira in izmenjuje podatke o kibernetskih grožnjah in incidentih iz različnih virov ***in, kjer je ustrezno, izmenjuje informacije z mrežo skupin CSIRT***;

(b) z uporabo najsodobnejših orodij, zlasti tehnologij umetne inteligence in podatkovne analitike, zagotavlja visokokakovostne, uporabne informacije in obveščevalne podatke o kibernetskih grožnjah;

(c) prispeva k boljši zaščiti proti kibernetskim grožnjam in k boljšemu odzivanju nanje***, vključno z oblikovanjem konkretnih priporočil subjektom***;

(d) prispeva k hitrejšemu odkrivanju kibernetskih groženj in situacijskemu zavedanju o njih po vsej Uniji;

(e) skupnosti za kibernetsko varnost v Uniji zagotavlja storitve in dejavnosti, med drugim s prispevanjem k razvoju naprednih orodij umetne inteligence in podatkovne analitike.

Razvije se v sodelovanju z infrastrukturo za vseevropsko visokozmogljivostno računalništvo, vzpostavljeno v skladu z Uredbo (EU) 2021/1173.

Člen 4

Nacionalni centri za varnostne operacije

1. ***Da bi lahko sodelovala*** v evropskem kibernetskem ščitu, vsaka država članica imenuje vsaj en nacionalni center za varnostne operacije. Nacionalni center za varnostne operacije je ***centralizirana zmogljivost v javnem organu***. ***Nacionalni centri za varnostne operacije se po možnosti vključijo v skupine CSIRT ali druge obstoječe infrastrukture in upravljanje na področju kibernetske varnosti.***

Lahko deluje kot referenčna točka in točka dostopa do drugih javnih in zasebnih organizacij na nacionalni ravni, ***zlasti njihovih centrov za varnostne operacije***, za zbiranje in analiziranje informacij o kibernetskovarnostnih grožnjah in incidentih ***ter po potrebi izmenjavo teh informacij s člani mreže skupin CSIRT te države članice in*** prispevanje k čezmejnim centrom za varnostne operacije. Opremljen je z najsodobnejšimi tehnologijami, ki so zmožne ***preprečevanja,*** odkrivanja, združevanja in analiziranja podatkov v zvezi s kibernetskovarnostnimi grožnjami in incidenti.

Nacionalni center za varnostne operacije ali skupina CSIRT lahko od ponudnikov upravljanih varnostnih storitev, ki opravljajo storitev za kritični subjekt, zahtevajo telemetrijo, senzorje ali beleženje podatkov o svojih nacionalnih kritičnih subjektih. Ti podatki se izmenjujejo v skladu s pravom Unije o varstvu podatkov in izključno z namenom podpiranja nacionalnega centra za kibernetsko varnost ali skupine CSIRT pri odkrivanju in preprečevanju kibernetskih groženj ter incidentov.

2. Evropski kompetenčni center za kibernetsko varnost (v nadaljnjem besedilu: ECCC) na podlagi razpisa za prijavo interesa ***lahko*** izbere nacionalne centre za varnostne operacije, ki z njim sodelujejo pri skupnem javnem naročanju orodij in infrastruktur. Center ECCC lahko izbranim nacionalnim centrom za varnostne operacije dodeli nepovratna sredstva za financiranje delovanja teh orodij in infrastruktur. Finančni prispevek Unije krije do 50 % stroškov pridobitve orodij in infrastruktur ter do 50 % operativnih stroškov, preostale stroške pa krije država članica. Pred začetkom postopka za pridobitev orodij in infrastruktur center ECCC in nacionalni center za varnostne operacije skleneta sporazum o gostiteljstvu in uporabi, ki ureja uporabo orodij in infrastruktur.

3. Nacionalni center za varnostne operacije, izbran v skladu z odstavkom 2, se zaveže, da bo za sodelovanje v čezmejnem centru za varnostne operacije zaprosil v dveh letih od datuma pridobitve orodij in infrastruktur ali datuma prejema nepovratnih sredstev, kateri koli nastopi

prej. Če nacionalni center za varnostne operacije do takrat ne sodeluje v čezmejnem centru za varnostne operacije, ni upravičen do dodatne podpore Unije v skladu s to uredbo.

Člen 5

Čezmejni centri za varnostne operacije

1. Gostiteljski konzorcij, ki ga sestavljajo vsaj tri države članice, ki jih zastopajo nacionalni centri za varnostne operacije, ki so se zavezali skupnemu usklajevanju dejavnosti odkrivanja in spremljanja kibernetskih groženj, je upravičen do sodelovanja pri ukrepih za ustanovitev čezmejnega centra za varnostne operacije. ***Čezmejni centri za varnostne operacije so zasnovani za odkrivanje in analiziranje kibernetskih groženj, preprečevanje incidentov ter podpiranje priprave visokokakovostnih obveščevalnih podatkov, zlasti z izmenjavo podatkov iz različnih virov, javnih in zasebnih, pa tudi z izmenjavo najsodobnejših orodij in skupnim razvijanjem kibernetskih zmogljivosti za odkrivanje, analizo, preprečevanje in zaščito v zaupanja vrednem in varnem okolju.***

2. Center ECCC na podlagi razpisa za prijavo interesa lahko izbere gostiteljski konzorcij, ki z njim sodeluje pri skupnem javnem naročanju orodij in infrastruktur. Gostiteljskemu konzorciju lahko dodeli nepovratna sredstva za financiranje delovanja orodij in infrastruktur. Finančni prispevek Unije krije do 75 % stroškov pridobitve orodij in infrastruktur ter do 50 % operativnih stroškov, preostale stroške pa krije gostiteljski konzorcij. Pred začetkom postopka za pridobitev orodij in infrastruktur center ECCC in gostiteljski konzorcij skleneta sporazum o gostiteljstvu in uporabi, ki ureja uporabo orodij in infrastruktur.

2a. Z odstopanjem od člena 176 Uredbe (EU, Euratom) 2018/1046 subjekti s sedežem v tretjih državah, ki niso pogodbenice Sporazuma o javnih naročilih, ne sodelujejo pri javnem naročanju orodij in infrastrukture.

3. Članice gostiteljskega konzorcija sklenejo pisno konzorcijsko pogodbo, v kateri so določene njihove notranje ureditve za izvajanje sporazuma o gostiteljstvu in uporabi.

4. Čezmejni center za varnostne operacije za pravne namene zastopa nacionalni center za varnostne operacije, ki deluje kot usklajevalni center za varnostne operacije, ali gostiteljski konzorcij, če je ta pravna oseba. Usklajevalni center za varnostne operacije je odgovoren za zagotavljanje skladnosti z zahtevami iz sporazuma o gostiteljstvu in uporabi ter te uredbe.

Člen 6

Sodelovanje in izmenjava informacij v čezmejnih centrih za varnostne operacije in med njimi

1. Članice gostiteljskega konzorcija si v okviru čezmejnega centra za varnostne operacije izmenjujejo ustrezne informacije, vključno z informacijami, ki se nanašajo na kibernetske grožnje, skorajšnje incidente, ranljivosti, tehnike in postopke, kazalnike ogroženosti, sovražne taktike, specifične informacije o grožnji in akterju, opozorila glede kibernetske varnosti in priporočila glede konfiguracije orodij za kibernetsko varnost za zaznavo kibernetskih napadov, kadar taka izmenjava informacij:

(a) ***izboljša izmenjavo obveščevalnih podatkov o kibernetskih grožnjah med nacionalnimi in čezmejnimi centri za varnostne operacije in industrijskimi centri za izmenjavo in analizo informacij, z namenom preprečevanja, odkrivanja ali blažitev groženj;***

(b) zvišuje raven kibernetske varnosti, zlasti z ozaveščanjem v zvezi s kibernetskimi grožnjami, omejevanjem ali oviranjem zmožnosti širjenja takih groženj, podpiranjem vrste obrambnih zmogljivosti, odpravljanjem in razkrivanjem ranljivosti, tehnikami odkrivanja, omejevanja in preprečevanja groženj, strategijami za zmanjšanje tveganja ali fazami odzivanja in okrevanja ali spodbujanjem sodelovanja med javnimi in zasebnimi subjekti pri raziskovanju kibernetskih groženj.

2. V pisni konzorcijski pogodbi iz člena 5(3) se določijo:

(a) zaveza souporabi ***pomembnih*** ▌ podatkov iz odstavka 1 in pogoji, pod katerimi se te informacije izmenjujejo;

(b) okvir upravljanja, ki spodbuja izmenjavo informacij med vsemi sodelujočimi;

(c) cilji za prispevek k razvoju naprednih orodij umetne inteligence in podatkovne analitike.

3. Da bi spodbudili izmenjavo informacij ***med*** čezmejnimi centri za varnostne operacije ***in industrijskimi centri za izmenjavo in analizo informacij***, čezmejni centri za varnostne operacije zagotavljajo visoko raven medsebojne interoperabilnosti ***in, kjer je to mogoče, z industrijskimi centri za izmenjavo in analizo informacij***. Za spodbujanje interoperabilnosti med čezmejnimi centri za varnostne operacije ***in industrijskimi centri za izmenjavo in analizo informacij bi lahko standarde in protokole za izmenjavo informacij uskladili z mednarodnimi standardi in najboljšimi industrijskimi praksami. Treba bi bilo spodbujati tudi skupno javno naročanje kibernetske infrastrukture, storitev in orodij. Poleg tega se,*** po posvetovanju s centrom ECCC ***in agencijo ENISA na Komisijo prenese pooblastilo, da do ... [šest mesecev od začetka veljavnosti te uredbe] sprejme delegirane akte v skladu s členom 20a in to uredbo dopolni, tako da določi pogoje*** za to interoperabilnost ***v tesnem sodelovanju s čezmejnimi centri za varnostne operacije ter na podlagi mednarodnih standardov in najboljših industrijskih praks***.

4. Čezmejni centri za varnostne operacije med seboj ***in, kjer je ustrezno, z industrijskimi centri za izmenjavo in analizo informacij,*** sklenejo sporazume o sodelovanju, v katerih določijo načela izmenjave informacij ***in interoperabilnosti*** med čezmejnimi platformami, ***pri čemer upoštevajo že obstoječe ustrezne mehanizme za izmenjavo informacij v skladu z Direktivo (EU) 2022/2555***. ***Kjer je ustrezno, čezmejni centri za varnostne operacije sklenejo sporazume o sodelovanju z industrijskimi centri za izmenjavo in analizo informacij. Mehanizmi za izmenjavo informacij pri morebitnem ali tekočem kibernetskovarnostnem incidentu velikih razsežnosti so skladni z ustreznimi določbami iz Direktive (EU) 2022/2555***.

Člen 7

Sodelovanje in izmenjava informacij z mrežo skupin CSIRT

1. Kadar čezmejni centri za varnostne operacije pridobijo informacije v zvezi z morebitnim ali tekočim kibernetskovarnostnim incidentom velikih razsežnosti ***z namenom skupnega zaznavanja razmer, koordinacijski center za kibernetsko varnost*** ustrezne informacije nemudoma ***zagotovi svoji skupini CSIRT ali pristojnemu organu, ki jih bo sporočil*** mreži EU-CyCLON, mreži skupin CSIRT in Komisiji ***ter agenciji ENISA*** glede na njihove vloge ***in postopke*** pri kriznem upravljanju v skladu z Direktivo (EU) 2022/2555. ***Ta odstavek javnim ali zasebnim subjektom ne nalaga nobenih dodatnih obveznosti glede obveščanja o morebitnem ali tekočem kibernetskovarnostnem incidentu velikih razsežnosti zaradi izpolnjevanja obveznosti, določenih v Direktivi (EU) 2022/2555.***

2. Na Komisijo ***se prenese pooblastilo za sprejemanje delegiranih aktov v skladu s členom 20a po posvetovanju z mrežo CSIRT, da to uredbo dopolni, s tem da določi*** postopkovne ureditve za izmenjavo informacij iz odstavka 1 ***tega člena in v skladu z Direktivo (EU) 2022/2555***.

Člen 8

Varnost

1. Države članice, ki sodelujejo v evropskem kibernetskem ščitu, zagotovijo visoko raven ***zaupnosti in*** varnosti podatkov in fizične varnosti infrastrukture evropskega kibernetskega ščita ter ustrezno upravljanje in nadzor infrastrukture, tako da je ta zaščitena pred grožnjami ter da sta zagotovljeni njena varnost in varnost sistemov, med drugim varnost podatkov, ki se izmenjujejo prek infrastrukture.

2. Države članice, ki sodelujejo v evropskem kibernetskem ščitu, zagotovijo, da izmenjava informacij v okviru evropskega kibernetskega ščita s subjekti, ki niso javni organi držav članic, nima negativnih posledic za varnostne interese Unije.

3. Komisija lahko sprejme izvedbene akte, s katerimi določi tehnične zahteve za države članice glede izpolnjevanja njihove obveznosti iz odstavkov 1 in 2. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 21(2) te uredbe. ***Skladni so z direktivama (EU) 2022/2555 in (EU) 2022/2557***. Komisija ***v svojih izvedbenih aktih*** ob podpori visokega predstavnika upošteva ustrezne varnostne standarde na ravni obrambe, da bi se olajšalo sodelovanje z vojaškimi akterji.

Poglavje III

MEHANIZEM ZA IZREDNE KIBERNETSKE VARNOSTNE RAZMERE

Člen 9

Vzpostavitev mehanizma za izredne kibernetske *varnostne* razmere

1. Vzpostavi se mehanizem za izredne kibernetske ***varnostne*** razmere za povečanje odpornosti Unije proti večjim kibernetskovarnostnim grožnjam ter pripravo na kratkoročne posledice pomembnih kibernetskovarnostnih incidentov in takih incidentov velikih razsežnosti in njihovo ublažitev v duhu solidarnosti (v nadaljnjem besedilu: mehanizem).

2. Ukrepi za izvajanje ▌mehanizma se podprejo s sredstvi iz programa Digitalna Evropa, izvajajo pa se v skladu z Uredbo (EU) 2021/694 in zlasti specifičnim ciljem 3 Uredbe.

Člen 10

Vrsta ukrepov

1. Mehanizem podpira naslednje vrste ukrepov:

(a) ukrepe pripravljenosti, vključno z usklajenim preskušanjem pripravljenosti subjektov, ki delujejo v visoko kritičnih sektorjih po vsej Uniji;

(b) ukrepe za odzivanje za podporo odzivu in takojšnjemu okrevanju po pomembnih kibernetskovarnostnih incidentih in takih incidentih velikih razsežnosti, pri čemer ukrepe zagotovijo zaupanja vredni ponudniki ***upravljanih varnostnih storitev***, ki sodelujejo v kibernetskovarnostni rezervi EU, vzpostavljeni v skladu s členom 12;

(c) ukrepe medsebojne pomoči, ki vključujejo pomoč, ki jo nacionalni organi ene države članice zagotovijo drugi državi članici, zlasti kot je določeno v členu 11(3), točka (f), Direktive (EU) 2022/2555.

1a. Po sprožitvi mehanizma Komisija vsako leto oceni in objavi poročilo o pozitivnem in negativnem delovanju tega mehanizma, vključno s tem, ali so potrebne dodatne zahteve glede sodelovanja ali usposabljanja.

Člen 11

Usklajeno preskušanje pripravljenosti subjektov

1. Da bi Komisija podprla usklajeno preskušanje pripravljenosti subjektov iz člena 10(1), točka (a), po vsej Uniji, po posvetovanju s skupino za sodelovanje na področju varnosti omrežnih in informacijskih sistemov in agencijo ENISA med visoko kritičnimi sektorji, navedenimi v Prilogi I k Direktivi (EU) 2022/2555, opredeli zadevne sektorje ali podsektorje, katerih subjekti so lahko predmet usklajenega preskušanja pripravljenosti***, v skladu z ureditvijo, določeno za subjekte v visoko kritičnih sektorjih, navedenih v Prilogi I k Direktivi (EU) 2022/2555***.

2. Skupina za sodelovanje na področju varnosti omrežnih in informacijskih sistemov v sodelovanju s Komisijo, agencijo ENISA, visokim predstavnikom ***in subjekti, katerih pripravljenost se usklajeno preskuša v skladu z odstavkom 1***, razvije skupne scenarije tveganja in metodologije za usklajeno preskušanje ***pripravljenosti, ki se zaključijo z usklajenim delovnim načrtom. Subjekti, za katere se izvaja usklajeno preskušanje pripravljenosti,***

pripravijo in izvajajo sanacijski načrt, v okviru katerega se izvajajo priporočila, oblikovana na podlagi preskusov pripravljenosti.

Skupina za sodelovanje na področju varnosti lahko prispeva k določitvi, kateri sektorji ali podsektorji se prednostno obravnavajo za usklajeno preskušanje pripravljenosti.

Člen 12

Vzpostavitev kibernetskovarnostne rezerve EU

1. Vzpostavi se kibernetskovarnostna rezerva EU za pomoč uporabnikom iz odstavka 3 pri odzivanju ali zagotavljanju podpore pri odzivanju na pomembne kibernetskovarnostne incidente ali take incidente velikih razsežnosti ter pri takojšnjem okrevanju po takih incidentih.

Kadar je očitno, da naročenih storitev ni mogoče v celoti uporabiti za zagotavljanje podpore pri odzivanju na pomembne incidente ali incidente velikega obsega, se lahko te storitve izjemoma pretvorijo v vaje ali usposabljanja za obvladovanje incidentov, ki jih naročnik na zahtevo zagotovi uporabnikom.

2. Kibernetskovarnostno rezervo EU sestavljajo storitve za odzivanje na incidente, ki jih zagotovijo zaupanja vredni ponudniki ***upravljanih varnostnih storitev***, izbrani v skladu z merili iz člena 16. ***Kibernetskovarnostna rezerva EU*** vključuje storitve, k zagotavljanju katerih se ponudniki zavežejo vnaprej. Storitve se lahko uporabljajo v vseh državah članicah, ***krepijo tehnološko suverenost Unije, njeno odprto strateško avtonomijo, konkurenčnost in odpornost na področju kibernetske varnosti, tudi s pospeševanjem inovacij na digitalnem enotnem trgu po vsej Uniji.***

3. Uporabniki storitev iz kibernetskovarnostne rezerve EU so:

(a) organi držav članic za obvladovanje kibernetskih kriz in skupine CSIRT iz člena 9(1) in (2) oziroma člena 10 Direktive (EU) 2022/2555;

(b) Institucije, organi in agencije Unije, ***kot so opredeljeni v členu 3(1) Uredbe (EU) .../2023 Evropskega parlamenta in Sveta[1] ter skupine CERT-EU***.

4. Uporabniki iz odstavka 3, točka (a), storitve iz kibernetskovarnostne rezerve EU uporabljajo za odzivanje na pomembne incidente ali incidente velikih razsežnosti, ki prizadenejo subjekte, ki delujejo v kritičnih ali visoko kritičnih sektorjih, ali za podporo odzivanju nanje in takojšnjemu okrevanju po njih.

5. Za izvajanje kibernetskovarnostne rezerve EU je v celoti odgovorna Komisija. Komisija določi prednostne naloge in razvoj kibernetskovarnostne rezerve EU ***v sodelovanju z usklajevalno skupino NIS2 in*** v skladu z zahtevami uporabnikov iz odstavka 3, nadzoruje njeno izvajanje ter zagotovi dopolnjevanje, doslednost, sinergije in povezave z drugimi podpornimi ukrepi na podlagi te uredbe, pa tudi drugimi ukrepi in programi Unije.

[1] ***Uredba (EU) .../2023 o določitvi ukrepov za visoko skupno raven kibernetske varnosti v institucijah, organih, uradih in agencijah Unije (UL C , , str. , ELI: ...).***

6. Komisija delovanje in upravljanje kibernetskovarnostne rezerve EU s sporazumi o prispevku v celoti ali delno zaupa agenciji ENISA.

7. Da bi agencija ENISA podprla Komisijo pri vzpostavitvi kibernetskovarnostne rezerve EU, ***vključno s potrebnimi spretnostmi ter zmogljivostmi delovne sile na področju kibernetske varnosti,*** po posvetovanju z državami članicami in Komisijo ***ter po potrebi s ponudniki upravljanih varnostnih storitev in drugimi predstavniki industrije kibernetske varnosti***. Po posvetovanju s Komisijo pripravi podoben pregled ***s ponudniki upravljanih varnostnih storitev in po potrebi z drugimi predstavniki industrije kibernetske varnosti*** za opredelitev potreb tretjih držav, upravičenih do podpore iz kibernetskovarnostne rezerve EU v skladu s členom 17. Komisija se po potrebi posvetuje z visokim predstavnikom ***in obvešča Svet o potrebah tretjih držav***.

8. Na Komisijo ***se prenese pooblastilo za sprejemanje delegiranih*** aktov ***v skladu s členom 20a, da to uredbo dopolni, tako da določi*** vrste in število storitev za odzivanje, potrebnih za kibernetskovarnostno rezervo EU. ▌..

Člen 13

Zahtevki za podporo iz kibernetskovarnostne rezerve EU

1. Uporabniki iz člena 12(3) lahko zahtevajo storitve iz kibernetskovarnostne rezerve EU, da bi podprli odzivanje na pomembne kibernetskovarnostne incidente ali take incidente velikih razsežnosti in takojšnjo obnovitev po njih.

2. Da bi uporabniki iz člena 12(3) prejeli podporo iz kibernetskovarnostne rezerve EU, sprejmejo ukrepe za ublažitev učinkov incidenta, v zvezi s katerim zahtevajo podporo, med drugim lahko zagotovijo neposredno tehnično pomoč in druge vire za pomoč pri odzivanju na incident ter si prizadevajo za takojšnjo obnovitev.

3. Zahtevki za podporo uporabnikov iz člena 12(3), točka (a), te uredbe se Komisiji in agenciji ENISA pošljejo prek enotne kontaktne točke, ki jo država članica določi ali vzpostavi v skladu s členom 8(3) Direktive (EU) 2022/2555.

4. Države članice o zahtevkih za podporo pri odzivanju na incidente in takojšnji obnovitvi po njih v skladu s tem členom obvestijo mrežo skupin CSIRT in po potrebi mrežo EU-CyCLONe.

5. Zahtevki za podporo pri odzivanju na incidente in takojšnji obnovitvi po njih vključujejo:

(a) ustrezne informacije o prizadetem subjektu in morebitnih posledicah incidenta ter načrtovani uporabi zahtevane podpore, vključno z navedbo ocenjenih potreb;

(b) informacije o ukrepih, sprejetih za ublažitev incidenta, v zvezi s katerim se zahteva podpora, kot je navedeno v odstavku 2;

(c) informacije o drugih oblikah podpore, ki so na voljo prizadetemu subjektu, vključno s pogodbenimi dogovori, vzpostavljenimi za storitve odzivanja na incidente in takojšnje obnovitve po njih, ter zavarovalnimi pogodbami, ki bi lahko krile tovrstne incidente.

6. Agencija ENISA v sodelovanju s Komisijo in skupino za sodelovanje na področju varnosti omrežnih in informacijskih sistemov pripravi predlogo za lažjo predložitev zahtevkov za podporo iz kibernetskovarnostne rezerve EU.

7. ***Na Komisijo se prenese pooblastilo za sprejemanje delegiranih aktov v skladu s členom 20a, da to uredbo dopolni, tako da*** natančneje določi podrobne ureditve za dodeljevanje storitev podpore iz kibernetskovarnostne rezerve EU. ▌

Člen 14

Izvajanje podpore iz kibernetskovarnostne rezerve EU

1. Zahtevke za podporo iz kibernetskovarnostne rezerve EU oceni Komisija ob podpori agencije ENISA ali kot je opredeljeno v sporazumih o prispevku iz člena 12(6) in uporabnikom iz člena 12(3) se odgovor na zahtevke pošlje ***brez nepotrebnega odlašanja, v vsakem primeru pa v 24 urah*.**

2. V primeru več hkratnih zahtevkov se za njihovo prednostno razvrstitev po potrebi upoštevajo naslednja merila:

(a) resnost kibernetskovarnostnega incidenta;

(b) vrsta prizadetega subjekta, pri čemer imajo prednost incidenti, ki prizadenejo bistvene subjekte, kot so opredeljeni v členu 3(1) Direktive (EU) 2022/2555;

(c) morebitne posledice za prizadete države članice ali uporabnike;

(d) ***obseg in*** morebitna čezmejna narava incidenta in tveganje prelivanja na druge države članice ali uporabnike;

(e) ukrepi, ki jih je uporabnik sprejel za pomoč pri prizadevanjih za odziv in takojšnjo obnovitev, kot je navedeno v členu 13(2) in členu 13(5), točka (b).

3. Storitve kibernetskovarnostne rezerve EU se zagotovijo v skladu s posebnimi sporazumi med ponudnikom storitev in uporabnikom, ki mu je zagotovljena podpora v okviru kibernetskovarnostne rezerve EU. Ti sporazumi vključujejo pogoje glede odgovornosti ***in vse morebitne druge določbe, za katere podpisnice sporazuma menijo, da so potrebne za zagotavljanje zadevne storitve***.

4. Sporazumi iz odstavka 3 ▌ temeljijo na predlogah, ki jih po posvetovanju z državami članicami ***in po potrebi z drugimi uporabniki kibernetskovarnostne rezerve EU*** pripravi agencija ENISA.

5. Komisija in agencija ENISA ne prevzameta pogodbene odgovornosti za škodo, ki jo tretje osebe utrpijo zaradi storitev, zagotovljenih v okviru izvajanja kibernetskovarnostne rezerve EU***, razen, če pri ocenjevanju zahtevka ponudnika storitev pride do hude malomarnosti ali če sta Komisija ali agencija ENISA uporabnici kibernetskovarnostne rezerve EU v skladu s členom 14(3).***

6. Uporabniki v enem mesecu po koncu ukrepa podpore Komisiji, agenciji ENISA***, mreži skupin CSIRT in po potrebi mreži EU-CyCLONe*** predložijo zbirno poročilo o zagotovljeni storitvi, doseženih rezultatih in pridobljenih spoznanjih. Če je uporabnik iz tretje države, kot je določeno v členu 17, se tako poročilo pošlje visokemu predstavniku.
Pri poročilu se spoštuje pravo Unije in nacionalno pravo v zvezi z varstvom občutljivih ali tajnih podatkov.

7. Komisija skupini za sodelovanje na področju varnosti omrežnih in informacijskih sistemov redno ***in vsaj dvakrat letno*** poroča o uporabi podpore in njenih rezultatih. ***V njem se zaupne informacije varujejo v skladu s pravom Unije in nacionalnim pravom v zvezi z varstvom občutljivih ali tajnih podatkov.***

Člen 15

Usklajevanje z mehanizmi kriznega upravljanja

1. Kadar pomembni kibernetskovarnostni incidenti ali taki incidenti velikih razsežnosti izvirajo iz nesreč, kot so opredeljene v Sklepu št. 1313/2013/EU[1], ali povzročijo take nesreče, podpora za odzivanje na take incidente na podlagi te uredbe dopolnjuje ukrepe na podlagi Sklepa št. 1313/2013/EU in brez poseganja vanj.

2. V primeru čezmejnega kibernetskovarnostnega incidenta velikih razsežnosti, pri katerem se uporabi enotna ureditev za politično odzivanje na krize (IPCR), se podpora iz te uredbe za odziv na tak incident obravnava v skladu z ustreznimi protokoli in postopki iz ureditve IPCR.

3. Na podlagi posvetovanja z visokim predstavnikom lahko podpora v okviru mehanizma za izredne ***kibernetskovarnostne*** razmere dopolnjuje pomoč, zagotovljeno v okviru skupne zunanje in varnostne politike ter skupne varnostne in obrambne politike, med drugim prek enot za hitro odzivanje na kibernetske grožnje. Prav tako lahko dopolnjuje pomoč, ki jo ena država članica zagotavlja drugi državi članici, ali k njej prispeva v okviru člena 42(7) Pogodbe o Evropski uniji.

4. Podpora v okviru mehanizma za izredne ***kibernetskovarnostne*** razmere je lahko del skupnega odziva Unije in držav članic v primerih iz člena 222 Pogodbe o delovanju Evropske unije.

Člen 16

Zaupanja vredni ponudniki

1. Javni naročnik v postopkih javnega naročanja za namene vzpostavitve kibernetskovarnostne rezerve EU ravna v skladu z načeli iz Uredbe (EU, Euratom) 2018/1046 in naslednjimi načeli:

(a) zagotovi, da kibernetskovarnostna rezerva EU vključuje storitve, ki se lahko uvedejo v vseh državah članicah, ob upoštevanju zlasti nacionalnih zahtev za zagotavljanje takih storitev, vključno s certificiranjem ali akreditacijo;

(b) zagotovi zaščito bistvenih varnostnih interesov Unije in njenih držav članic;

(c) zagotovi, da kibernetskovarnostna rezerva EU prinaša dodano vrednost EU s prispevanjem k ciljem iz člena 3 Uredbe (EU) 2021/694, med drugim s spodbujanjem razvoja kibernetskovarnostnih veščin v EU ***in doseganjem uravnotežene zastopanosti spolov v sektorju ter krepitvijo tehnološke suverenosti, odprte strateške avtonomije, konkurenčnosti in odpornosti***.

2. Javni naročnik pri javnem naročanju storitev za kibernetskovarnostno rezervo EU v dokumente v zvezi z oddajo javnega naročila vključi naslednja merila za izbiro:

[1] Sklep št. 1313/2013/EU Evropskega parlamenta in Sveta z dne 17. decembra 2013 o mehanizmu Unije na področju civilne zaščite (UL L 347, 20.12.2013, str. 924).

(a) ponudnik dokaže, da ima njegovo osebje najvišjo stopnjo poklicne integritete, neodvisnosti, odgovornosti in potrebne tehnične usposobljenosti za izvajanje dejavnosti na specifičnem področju, ter zagotovi stalnost/kontinuiteto strokovnega znanja in potrebne tehnične vire;

(b) ponudnik, njegova odvisna podjetja in podizvajalci imajo vzpostavljen okvir za varovanje občutljivih informacij v zvezi s storitvijo, zlasti dokazov, ugotovitev in poročil, pri čemer je okvir skladen z varnostnimi pravili Unije o varovanju tajnih podatkov EU;

(c) ponudnik predloži zadostne dokaze, da je njegova struktura upravljanja pregledna ter da ne bo ogrozila njegove nepristranskosti in kakovosti njegovih storitev ali povzročila nasprotja interesov;

(d) ponudnik ima ustrezno varnostno preverjanje, vsaj za osebje, namenjeno uvedbi storitev;

(e) ponudnik zagotavlja ustrezno raven varnosti svojih informacijskih sistemov;

(f) ponudnik je opremljen ***s sodobno*** tehnično strojno in programsko opremo, potrebno za podporo zahtevani storitvi***, in po potrebi izpolnjuje zahteve iz Uredbe (EU) .../... Evropskega parlamenta in Sveta[1] (2022/0272(COD))***;

(g) ponudnik je sposoben dokazati, da ima izkušnje z zagotavljanjem podobnih storitev ustreznim nacionalnim organom ali subjektom, ki delujejo v kritičnih ali visoko kritičnih sektorjih;

(h) ponudnik lahko v državah članicah, v katerih lahko opravi storitev, to zagotovi v kratkem času;

(i) ponudnik lahko storitev zagotovi v lokalnem jeziku države članice, v kateri lahko opravi storitev***, ali v enem od delovnih jezikov Unije***;

(j) ko je vzpostavljena ***evropska*** certifikacijska shema ***za kibernetsko varnost*** za upravljane varnostne storitve (Uredba (EU) 2019/881), se ponudnik certificira v skladu z navedeno shemo ***v roku dveh let po njenem sprejetju;***

(ja) ponudnik lahko storitev zagotovi neodvisno in ne kot del paketa, s čimer se uporabniku omogoči možnost, da zamenja ponudnika storitev;

(jb) za namene člena 12(1) ponudnik v predlog ponudb doda možnost, da se neuporabljene storitve za odzivanje na incidente pretvorijo v vaje ali usposabljanja;

(jc) sedež in strukture izvršne uprave ponudnika so v Uniji, pridruženi državi ali tretji državi, ki je podpisnica Sporazuma o javnih naročilih v okviru Svetovne trgovinske organizacije;

(jd) ponudnik ni pod nadzorom nepridružene tretje države ali subjekta iz nepridružene tretje države, ki ni podpisnica Sporazuma o javnih naročilih, ali pa je moral biti v zvezi s takim subjektom izveden pregled v smislu Uredbe (EU) 2019/452 in je po potrebi sprejel ukrepe za zmanjšanje tveganj ob upoštevanju ciljev iz te uredbe.

[1] Uredba (EU) .../... Evropskega parlamenta in Sveta z dne … o ... (UL L, …, ELI: …).

Člen 17

Podpora tretjim državam

1. Tretje države lahko zaprosijo za podporo iz kibernetskovarnostne rezerve EU, če je to določeno v pridružitvenih sporazumih, sklenjenih v zvezi z njihovim sodelovanjem v programu Digitalna Evropa.

2. Podpora iz kibernetskovarnostne rezerve EU je v skladu s to uredbo in izpolnjuje vse posebne pogoje, določene v pridružitvenih sporazumih iz odstavka 1.

3. Uporabniki iz pridruženih tretjih držav, ki so upravičeni do storitev iz kibernetskovarnostne rezerve EU, vključujejo pristojne organe, kot so skupine CSIRT in organi za obvladovanje kibernetskih kriz.

4. Vsaka tretja država, ki je upravičena do podpore iz kibernetskovarnostne rezerve EU, imenuje organ, ki deluje kot enotna kontaktna točka za namene te uredbe.

5. Preden tretje države prejmejo podporo iz kibernetskovarnostne rezerve EU, Komisiji in visokemu predstavniku predložijo informacije o svoji kibernetski odpornosti in zmogljivostih za obvladovanje tveganj, med drugim vsaj informacije o nacionalnih ukrepih, ki so jih sprejele za pripravo na pomembne kibernetskovarnostne incidente ali take incidente velikih razsežnosti, ter informacije o odgovornih nacionalnih subjektih, vključno s skupinami CSIRT ali enakovrednimi subjekti, njihovih zmogljivostih in virih, ki so jim dodeljeni. Kadar se določbe členov 13 in 14 te uredbe nanašajo na države članice, se uporabljajo tudi za tretje države, kot je določeno v odstavku 1.

6. Komisija ***brez nepotrebnega odlašanja obvesti Svet in*** se z visokim predstavnikom uskladi glede prejetih zahtevkov in izvajanja podpore, dodeljene tretjim državam iz kibernetskovarnostne rezerve EU.

Poglavje IV

MEHANIZEM ZA PREGLEDOVANJE KIBERNETSKOVARNOSTNIH INCIDENTOV

Člen 18

Mehanizem za pregledovanje kibernetskovarnostnih incidentov

1. Agencija ENISA na zahtevo Komisije, mreže EU-CyCLONe ali mreže skupin CSIRT pregleda in oceni grožnje, ranljivosti in blažitvene ukrepe v zvezi s posameznim pomembnim kibernetskovarnostnim incidentom ali takim incidentom velikih razsežnosti. Agencija ENISA po zaključku pregleda in ocene incidenta mreži skupin CSIRT, mreži EU-CyCLONe in Komisiji predloži poročilo o pregledu incidenta, da bi jih podprla pri izvajanju njihovih nalog, zlasti nalog iz členov 15 in 16 Direktive (EU) 2022/2555. Komisija poročilo po potrebi posreduje visokemu predstavniku.

2. Agencija ENISA pri pripravi poročila o pregledu incidenta iz odstavka 1 sodeluje z vsemi ustreznimi deležniki, vključno s predstavniki držav članic, Komisijo, drugimi ustreznimi institucijami, organi, uradi in agencijami EU, ponudniki upravljanih varnostnih storitev ***v nacionalnih in čezmejnih centrih za varnostne operacije*** in uporabniki kibernetskih storitev***, in od teh deležnikov zbere povratne informacije, kar se dopolni z jamstvi in spremljanjem, ki***

zadostujejo za zagotovitev, da bodo akterji s področja kibernetskovarnostnih storitev upoštevali pridobljene izkušnje in prepoznane primere dobre prakse. Po potrebi sodeluje tudi s subjekti, ki so jih prizadeli pomembni kibernetskovarnostni incidenti ali taki incidenti velikih razsežnosti. Za podporo pregledu se lahko posvetuje tudi z drugimi vrstami deležnikov. Predstavniki, s katerimi se opravi posvetovanje, razkrijejo vsako morebitno nasprotje interesov.

3. Poročilo zajema pregled in analizo posameznega pomembnega kibernetskovarnostnega incidenta ali takega incidenta velikih razsežnosti, vključno z glavnimi vzroki, ranljivostmi in pridobljenimi spoznanji. V njem so zaupne informacije zavarovane v skladu s pravom Unije ali nacionalnim pravom v zvezi z varstvom občutljivih ali tajnih podatkov. ***Ne zajema podrobnosti o aktivno izrabljenih ranljivostih, ki so še neodpravljene.***

3a. V poročilu iz odstavka 1 tega člena se navedejo spoznanja, pridobljena pri medsebojnih strokovnih pregledih, izvedenih v skladu s členom 19 Direktive (EU) 2022/2555.

4. Poročilo po potrebi vsebuje priporočila***, tudi za vse ustrezne deležnike,*** za izboljšanje kibernetske drže Unije.

5. Kadar je mogoče, se različica poročila javno objavi. Ta različica vključuje samo informacije javnega značaja.

Poglavje V

KONČNE DOLOČBE

Člen 19

Spremembe Uredbe (EU) 2021/694

Uredba (EU) 2021/694 se spremeni:

(1) člen 6 se spremeni:

(a) odstavek 1 se spremeni:

(***i***) vstavi se naslednja točka (aa):

„(aa) podpora razvoju kibernetskega ščita EU, vključno z razvojem, uvedbo in delovanjem platform nacionalnih in čezmejnih centrov za varnostne operacije, ki prispevajo k situacijskemu zavedanju v Uniji in krepitvi zmogljivosti Unije za pridobivanje obveščevalnih podatkov o kibernetskih grožnjah;“;

(***ii***) doda se naslednja točka (g):

vzpostavitev in upravljanje mehanizma za izredne ***kibernetskovarnostne*** razmere za podporo državam članicam pri pripravi na pomembne kibernetskovarnostne incidente in odzivanju nanje, pri čemer mehanizem dopolnjuje nacionalne vire in zmogljivosti ter druge

oblike podpore, ki so na voljo na ravni Unije, vključno z vzpostavitvijo kibernetskovarnostne rezerve EU.“;

(***b***) odstavek 2 se nadomesti z naslednjim:

„2. Ukrepi v okviru specifičnega cilja 3 se izvajajo predvsem prek Evropskega industrijskega, tehnološkega in raziskovalnega kompetenčnega centra za kibernetsko varnost ter mreže nacionalnih koordinacijskih centrov v skladu z Uredbo (EU) 2021/887 Evropskega parlamenta in Sveta*, razen ukrepov za izvajanje kibernetskovarnostne rezerve EU, ki jih izvajata Komisija in agencija ENISA.“;

_____

* Uredba (EU) 2021/887 Evropskega parlamenta in Sveta z dne 20. maja 2021 o vzpostavitvi Evropskega industrijskega, tehnološkega in raziskovalnega kompetenčnega centra za kibernetsko varnost ter Mreže nacionalnih koordinacijskih centrov (UL L 202, 8.6.2021, str. 1, ***ELI: http://data.europa.eu/eli/reg/2021/887/oj).“;***

(2) člen 9 se spremeni:

(a) v odstavku 2 se točke (b), (c) in (d) nadomestijo z naslednjim:

„(b) 1 776 956 000 EUR za specifični cilj 2 – umetna inteligenca;

(c) ***1 620 566 000*** EUR za specifični cilj 3 – kibernetska varnost in zaupanje;

(d) ***500 347 000*** EUR za specifični cilj 4 – napredne digitalne veščine;“;

(aa) vstavi se naslednji nov odstavek 2a:

„ 2a. Znesek iz odstavka 2, točka (c), se uporabi predvsem za doseganje operativnih ciljev iz člena 6, odstavek 1, točke a-f, Programa.“;

(ab) vstavi se naslednji nov odstavek 2b:

„ 2b. Znesek za vzpostavitev in izvedbo kibernetskovarnostne rezerve EU ne sme presegati 27 milijonov EUR za predvideno trajanje uredbe o določitvi ukrepov za okrepitev solidarnosti in zmogljivosti v Uniji za odkrivanje kibernetskovarnostnih groženj in incidentov ter pripravo in odzivanje nanje.“;

(b) doda se naslednji odstavek 8:

„8. Z odstopanjem od člena 12(4) Uredbe (EU, Euratom) 2018/1046 se neporabljene odobritve za prevzem obveznosti in odobritve plačil za ukrepe ***v okviru izvajanja kibernetskovarnostne rezerve EU***, s katerimi se uresničujejo cilji iz člena 6(1), točka (g), te uredbe, samodejno prenesejo ter se lahko prevzamejo in izplačajo do 31. decembra naslednjega proračunskega leta.

Komisija obvesti Parlament in Svet o odobritvah, prenesenih v skladu s členom 12(6) Uredbe (EU, Euratom) 2018/1046.“;

(3) v členu 14 se odstavek 2 nadomesti z naslednjim:

„2. Program lahko zagotovi financiranje v kateri koli obliki, določeni v ***Uredbi (EU, Euratom) 2018/1046***, v osnovni obliki zlasti kot javna naročila, ali v obliki nepovratnih sredstev in nagrad.

Kadar je za doseganje cilja ukrepa potrebno javno naročanje inovativnega blaga in storitev, se lahko nepovratna sredstva dodelijo le upravičencem, ki so javni naročniki ali naročniki, kot so opredeljeni v direktivah 2014/24/EU [27] in 2014/25/EU [28] Evropskega parlamenta in Sveta.

Kadar je treba za doseganje ciljev ukrepa dobaviti inovativno blago ali opraviti digitalne storitve, ki še niso na voljo v večjem komercialnem obsegu, lahko javni naročnik ali naročnik odobri oddajo več naročil v okviru istega postopka javnega naročanja.

Javni naročnik ali naročnik lahko iz ustrezno utemeljenih razlogov javne varnosti zahteva, da mora biti kraj izvajanja pogodbe znotraj ozemlja Unije.

Komisija in agencija ENISA lahko pri izvajanju postopkov javnega naročanja za kibernetskovarnostno rezervo EU, vzpostavljeno s členom 12 Uredbe (EU) 2023/**...**, delujeta kot osrednji nabavni organ za javno naročanje v imenu tretjih držav, pridruženih Programu v skladu s členom 10. Delujeta lahko tudi kot trgovec na debelo, tako da za navedene tretje države kupujeta, skladiščita in nadalje prodajata ali darujeta blago in storitve, vključno z najemi. Z odstopanjem od člena 169(3) Uredbe (EU) **…/…** za pooblastilo Komisije ali agencije ENISA za ukrepanje zadostuje zahtevek ene same tretje države.

Komisija in agencija ENISA lahko pri izvajanju postopkov javnega naročanja za kibernetskovarnostno rezervo EU, vzpostavljeno s členom 12 Uredbe (EU) 2023/**…**XX, delujeta kot osrednji nabavni organ za javno naročanje v imenu institucij, organov in agencij Unije. Delujeta lahko tudi kot trgovec na debelo, tako da za institucije, organe in agencije Unije kupujeta, skladiščita in nadalje prodajata ali darujeta blago in storitve, vključno z najemi. Z odstopanjem od člena 169(3) Uredbe (EU) **…/…** za pooblastilo Komisije ali agencije ENISA za ukrepanje zadostuje zahtevek ene same institucije, organa ali agencije Unije.

Programom lahko zagotovi tudi financiranje v obliki finančnih instrumentov v okviru operacij mešanega financiranja. “;

(4) doda se naslednji člen 16a:

„***Člen 16a***

V primeru ukrepov za izvajanje evropskega kibernetskega ščita, vzpostavljenega s členom 3 Uredbe (EU) 2023/XX, se uporabljajo pravila iz členov 4 in 5 Uredbe (EU) 2023/**….** V primeru neskladja med določbami te uredbe ter členoma 4 in 5 Uredbe (EU) 2023/**…** imata prednost navedena člena, ki se uporabljata za te specifične ukrepe.“;

(5) člen 19 se nadomesti z naslednjim:

„Nepovratna sredstva v okviru Programa se dodeljujejo in upravljajo v skladu z naslovom VIII ***Uredbe (EU, Euratom) 2018/1046*** ter lahko krijejo do 100 % upravičenih stroškov brez poseganja v načelo sofinanciranja, kot je določeno v členu 190 ***Uredbe (EU, Euratom) 2018/1046***. Taka nepovratna sredstva se dodeljujejo in upravljajo, kot je določeno za vsak specifični cilj.

Podporo v obliki nepovratnih sredstev lahko center ECCC dodeli neposredno, brez razpisa za zbiranje predlogov, nacionalnim centrom za varnostne operacije iz člena 4 Uredbe ***(EU) .../...*** in gostiteljskemu konzorciju iz člena 5 Uredbe ***(EU) .../...*** v skladu s členom 195(1), točka (d), ***Uredbe (EU, Euratom) 2018/1046***.

Podporo v obliki nepovratnih sredstev za mehanizem za izredne ***kibernetskovarnostne*** razmere iz člena 10 Uredbe ***(EU) .../...*** lahko center ECCC dodeli neposredno, brez razpisa za zbiranje predlogov, državam članicam v skladu s členom 195(1), točka (d), ***Uredbe (EU, Euratom) 2018/1046***.

Kar zadeva ukrepe iz člena 10(1), točka (c), Uredbe ***(EU) .../...***, center ECCC Komisijo in agencijo ENISA obvesti o zahtevkih držav članic za neposredna nepovratna sredstva, ki se dodelijo brez razpisa za zbiranje predlogov.

Za podporo v obliki medsebojne pomoči pri odzivanju na pomemben kibernetskovarnostni incident ali tak incident velikih razsežnosti, kot je opredeljen v členu 10, točka (c), Uredbe ***(EU) .../...***, in v skladu s členom 193(2), drugi pododstavek, točka (a), ***Uredbe (EU, Euratom) 2018/1046*** se lahko v ustrezno utemeljenih primerih stroški štejejo za upravičene, tudi če so nastali pred vložitvijo zahtevka za nepovratna sredstva.“;

(6) prilogi I in II k Uredbi (EU) 2021/694 se spremenita v skladu s Prilogo k tej uredbi.

Člen 19a
Dodatna sredstva za agencijo ENISA

Agencija ENISA prejme dodatna sredstva za izvajanje dodatnih nalog, ki so ji podeljene s to uredbo. Ta dodatna podpora, tudi v obliki finančnih sredstev, ne sme ogroziti uresničitve ciljev drugih programov Unije, zlasti programa Digitalna Evropa.

Člen 20

Ocena *in pregled*

1. Komisija do … [***dve leti od datuma*** začetka uporabe te uredbe], ***nato pa vsaki dve leti oceni delovanje ukrepov iz te uredbe ter*** Evropskemu parlamentu in Svetu predloži poročilo ▌.

2. Pri tem se zlasti ocenijo:

(a) uporaba in dodana vrednost čezmejnih centrov za varnostne operacije ter v kolikšni meri prispevajo k hitrejšemu odkrivanju kibernetskih groženj in odzivanju nanje ter k situacijskemu zavedanju; dejavno sodelovanje nacionalnih centrov za varnostne operacije v evropskem kibernetskem ščitu, tudi število vzpostavljenih nacionalnih in čezmejnih centrov za varnostne operacije, pa tudi, v kolikšni meri, je prispevalo k pripravi in izmenjavi visokokakovostnih uporabnih informacij in obveščevalnih podatkov o kibernetskih grožnjah; število in stroški skupno naročenih infrastruktur in/ali orodij za kibernetsko varnost; število sporazumov o sodelovanju, sklenjenih med čezmejnimi centri za varnostne operacije in sektorskimi centri za izmenjavo in analizo informacij; število incidentov, sporočenih mreži skupin CSIRT, in njihov vpliv na delo mreže skupin CSIRT;

(b) pozitivni in negativni vidik delovanja mehanizma za izredne kibernetskovarnostne razmere, med drugim, ali so potrebne nadaljnje zahteve glede sodelovanja ali usposabljanja;

(c) prispevek te uredbe h krepitvi odpornosti in odprte strateške avtonomije Unije, izboljšanju konkurenčnosti zadevnih industrijskih sektorjev, mikropodjetij, MSP, tudi zagonskih podjetij, ter razvoju kibernetskovarnostnih veščin v EU;

(d) uporaba in dodana vrednost kibernetskovarnostne rezerve EU, tudi število zaupanja vrednih ponudnikov varnostnih storitev, ki so del kibernetskovarnostne rezerve EU; število, vrsta, stroški in učinek izvedenih ukrepov v podporo odzivanju na kibernetskovarnostne incidente ter njihovih uporabnikov in ponudnikov; povprečni čas, potreben, da Komisija prepozna incident, se mobilizira kibernetskovarnostna rezerva EU in se poda odziv nanj ter uporabnik po njem obnovi delovanje sistemov; ali bi bilo treba področje uporabe kibernetskovarnostne rezerve EU razširiti na storitve za pripravljenost na incidente ali skupne vaje z zaupanja vrednimi ponudniki upravljanih varnostnih storitev in potencialnimi uporabniki kibernetskovarnostne rezerve, da se po potrebi zagotovi njeno učinkovito delovanje;

(e) prispevek te uredbe k razvoju in izboljšanju veščin in kompetenc delovne sile v sektorju kibernetske varnosti, ki so potrebne za krepitev zmogljivosti Unije za odkrivanje in preprečevanje kibernetskih groženj in incidentov ter odzivanje nanje in obnovitev po njih;

(f) prispevek te uredbe k uvajanju in razvoju najsodobnejših tehnologij v Uniji.

3. Komisija Evropskemu parlamentu in Svetu na podlagi poročil iz odstavka 1 po potrebi predloži zakonodajni predlog za spremembo te uredbe.

Člen 20a

Izvajanje prenosa pooblastila

1. Pooblastilo za sprejemanje delegiranih aktov je preneseno na Komisijo pod pogoji, določenimi v tem členu.

2. Pooblastilo za sprejemanje delegiranih aktov iz členov 6(3), 7(2), 12(8) in 13(7) se prenese na Komisijo za obdobje ... let od … [datum začetka veljavnosti temeljnega zakonodajnega akta ali kateri koli drug datum, ki ga določita sozakonodajalca]. Komisija pripravi poročilo o prenosu pooblastila najpozneje devet mesecev pred koncem ...-letnega obdobja. Prenos pooblastila se samodejno podaljšuje za enako dolga obdobja, razen če Evropski parlament ali Svet nasprotuje temu podaljšanju najpozneje tri mesece pred koncem vsakega obdobja.

3. Prenos pooblastila iz členov 6(3), 7(2), 12(8) in 13(7) lahko kadar koli prekliče Evropski parlament ali Svet. S sklepom o preklicu preneha veljati prenos pooblastila iz navedenega sklepa. Sklep začne učinkovati dan po njegovi objavi v Uradnem listu Evropske unije ali na poznejši dan, ki je določen v navedenem sklepu. Sklep ne vpliva na veljavnost že veljavnih delegiranih aktov.

4. Komisija se pred sprejetjem delegiranega akta posvetuje s strokovnjaki, ki jih imenujejo države članice, v skladu z načeli, določenimi v Medinstitucionalnem sporazumu z dne 13. aprila 2016 o boljši pripravi zakonodaje.

5. Komisija takoj po sprejetju delegiranega akta o njem sočasno uradno obvesti Evropski parlament in Svet.

6. Delegirani akt, sprejet na podlagi člena 6(3), 7(2), 12(8) ali 13(7), začne veljati le, če mu niti Evropski parlament niti Svet ne nasprotuje v roku dveh mesecev od uradnega obvestila Evropskemu parlamentu in Svetu o tem aktu ali če pred iztekom tega roka tako Evropski parlament kot Svet obvestita Komisijo, da mu ne bosta nasprotovala. Ta rok se na pobudo Evropskega parlamenta ali Sveta podaljša za [dva meseca].

Člen 21

Postopek v odboru

1. Komisiji pomaga odbor za usklajevanje programa Digitalna Evropa, ustanovljen z Uredbo (EU) 2021/694. Ta odbor je odbor v smislu Uredbe (EU) št. 182/2011.
2. Pri sklicevanju na ta odstavek se uporablja člen 5 Uredbe (EU) št. 182/2011.

Člen 22

Začetek veljavnosti

Ta uredba začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

Ta uredba je v celoti zavezujoča in se neposredno uporablja v vseh državah članicah.

V Strasbourgu,

Za Evropski parlament	*Za Svet*
predsednica	*predsednik*

PRILOGA

Uredba (EU) 2021/694 se spremeni:

(1) v Prilogi I se oddelek/poglavje „Specifični cilj 3 – kibernetska varnost in zaupanje“ nadomesti z naslednjim:

„Specifični cilj 3 – kibernetska varnost in zaupanje

Program spodbuja krepitev, razvoj in pridobivanje osnovnih zmogljivosti za zaščito digitalnega gospodarstva, družbe in demokracije v Uniji s krepitvijo industrijskega potenciala in konkurenčnosti Unije na področju kibernetske varnosti ter z izboljšanjem zmogljivosti zasebnega in javnega sektorja za zaščito državljanov in podjetij pred kibernetskimi grožnjami, vključno s podporo pri izvajanju Direktive (EU) 2016/1148.

Začetni in po potrebi poznejši ukrepi v okviru tega cilja vključujejo:

1. Sovlaganje držav članic v kibernetskovarnostno napredno opremo, infrastrukture ter tehnično znanje in izkušnje, ki so ključnega pomena za zaščito kritičnih infrastruktur in digitalnega enotnega trga na splošno. Tako sovlaganje lahko vključuje naložbe v zmogljivosti za razvoj kvantnih tehnologij in podatkovne vire za kibernetsko varnost, situacijsko zavedanje v kibernetskem prostoru***, vključno z nacionalnimi centri za varnostne operacije in čezmejnimi centri za varnostne operacije, ki sestavljajo evropski kibernetski ščit,*** ter druga orodja, ki se dajo na voljo javnemu in zasebnemu sektorju po vsej Evropi.

2. Obsežnejši razvoj obstoječih tehnoloških zmogljivosti in mreženje strokovnih centrov držav članic ter zagotavljanje, da se te zmogljivosti odzivajo na potrebe javnega sektorja in industrije, vključno z izdelki in storitvami, ki krepijo kibernetsko varnost znotraj digitalnega enotnega trga.

3. Zagotavljanje široke uvedbe učinkovitih najsodobnejših rešitev za kibernetsko varnost in zaupanje v vseh državah članicah. Taka uvedba vključuje krepitev zanesljivosti in varnosti izdelkov, od njihovega oblikovanja do trženja.

4. Podpora zapolnjevanju vrzeli v veščinah glede kibernetske varnosti***, pri čemer se posebna pozornost nameni doseganju uravnotežene zastopanosti spolov v sektorju,*** na primer z usklajevanjem programov za razvoj takih veščin, ***njihovim prilagajanjem*** specifičnim sektorskim potrebam, ***vključno z interdisciplinarnim in splošnim poudarkom***, ***ter olajšanjem*** dostopa do specializiranih, ciljno usmerjenih usposabljanj***, da bi lahko vsakdo in vsa ozemlja izkoristili priložnosti, ki jih ponuja ta uredba***.

5. Spodbujanje solidarnosti med državami članicami pri pripravi na pomembne kibernetskovarnostne incidente in odzivanju nanje z uvedbo čezmejnih storitev kibernetske

varnosti, med drugim s podporo za medsebojno pomoč med javnimi organi in vzpostavitvijo rezerve zaupanja vrednih ponudnikov ***upravljanih varnostnih*** storitev na ravni Unije.“;

(2) v Prilogi II se oddelek/poglavje „Specifični cilj 3 – kibernetska varnost in zaupanje“ nadomesti z naslednjim:

„Specifični cilj 3 – kibernetska varnost in zaupanje

3.1. Število infrastruktur ali orodij za kibernetsko varnost ali obojega, ki so bili ***kot del ščita kibernetske varnosti skupno naročeni.***

3.2. Število uporabnikov in uporabniških skupnosti, ki imajo dostop do evropskih zmogljivosti za kibernetsko varnost.

3.3. Število, ***vrsta, stroški in učinek*** ukrepov, ***izvedenih*** za podporo pripravljenosti in odzivanju na kibernetskovarnostne incidente v okviru mehanizma za izredne ***kibernetskovarnostne*** razmere. ***Obseg, v katerem je uporabnik uvedel in izvedel priporočila glede testov pripravljenosti, ter povprečni čas, potreben, da Komisija incident prepozna, se kibernetskovarnostna rezerva EU nanj odzove in uporabnik po njem obnovi delovanje sistemov.“***