Uradni list
Evropske unije

SL
Serija L

2025/38

15.1.2025

UREDBA (EU) 2025/38 EVROPSKEGA PARLAMENTA IN SVETA

z dne 19. decembra 2024

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

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,

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 ([4]),

ob upoštevanju naslednjega:

(1) Uporaba informacijskih in komunikacijskih tehnologij ter odvisnost od njih sta postali ključna vidika v vseh sektorjih gospodarske dejavnosti in družbe zaradi vse večje medsebojne povezanosti in medsebojne odvisnosti javnih uprav, podjetij in državljanov držav članic v različnih sektorjih in prek meja, hkrati pa sta tudi vir morebitnih ranljivosti.

(2) Obseg, pogostost in posledice kibernetskih incidentov se, vključno z napadi na oskrbovalno verigo za namene kibernetskega vohunjenja, izsiljevalskega programja ali povzročanja motenj, po vsej Uniji in tudi na svetovni ravni povečujejo. Ti predstavljajo veliko grožnjo za delovanje omrežja in informacijskih sistemov. Glede na hitro razvijajočo se krajino groženj je treba zaradi nevarnosti morebitnih kibernetskih incidentov velikih razsežnosti, ki povzročajo velike motnje ali škodo na kritični infrastrukturi, povečati pripravljenost okvira Unije za kibernetsko varnost. Ta nevarnost presega vojno agresijo Rusije proti Ukrajini in se bo verjetno nadaljevala, glede na številne akterje, vpletene v trenutne geopolitične napetosti. Taki incidenti lahko ovirajo zagotavljanje javnih storitev, saj so kibernetski napadi pogosto usmerjeni v lokalne, regionalne ali nacionalne javne storitve in infrastrukturo, pri čemer so lokalni organi še posebej ranljivi, tudi zaradi svojih omejenih virov. Ovirajo lahko tudi opravljanje gospodarskih dejavnosti, tudi v visoko kritičnih sektorjih ali drugih kritičnih sektorjih, povzročijo znatne finančne izgube, spodkopljejo zaupanje uporabnikov, povzročijo veliko škodo gospodarstvu in demokratičnim sistemom Unije in imajo lahko celo zdravstvene ali življenjsko nevarne posledice. Poleg tega so kibernetski incidenti nepredvidljivi, saj pogosto nastanejo in se razvijejo hitro, niso omejeni na določeno geografsko območje in se zgodijo hkrati ali se takoj razširijo po številnih državah. Pomembno je, da javni in zasebni sektor, akademski svet, civilna družba in mediji tesno sodelujejo.

(3) Okrepiti je treba konkurenčni položaj industrije in storitev v Uniji v celotnem digitalnem gospodarstvu ter podpreti njuno digitalno preobrazbo, in sicer z okrepitvijo ravni kibernetske varnosti na enotnem digitalnem trgu, kot je priporočeno v treh različnih predlogih Konference o prihodnosti Evrope. Treba je povečati odpornost državljanov, podjetij, vključno z mikropodjetji, malimi in srednjimi podjetji ter zagonskimi podjetji, in subjektov, ki upravljajo kritično infrastrukturo, proti vse večjim kibernetskim grožnjam, ki imajo lahko uničujoče družbene in gospodarske posledice. Zato so potrebne naložbe v infrastrukturo in storitve ter krepitev zmogljivosti za razvoj kibernetskih

([1]) Mnenje z dne 18. aprila 2023 (še ni objavljeno v Uradnem listu).
([2]) UL C 349, 29.9.2023, str. 167.
([3]) UL C, C/2024/1049, 9.2.2024, ELI: http://data.europa.eu/eli/C/2024/1049/oj.
([4]) Stališče Evropskega parlamenta z dne 24. aprila 2024 (še ni objavljeno v Uradnem listu) in odločitev Sveta z dne 2. decembra 2024.

veščin, ki bodo podpirale hitrejše odkrivanje kibernetskih groženj in incidentov ter hitrejše odzivanje nanje. Poleg tega države članice potrebujejo pomoč pri boljši pripravi na pomembne kibernetske incidente in kibernetske incidente velikih razsežnosti ter odzivanju nanje in pomoči pri začetni obnovitvi po njih. Unija bi morala na podlagi obstoječih struktur in v tesnem sodelovanju z njimi tudi povečati svoje zmogljivosti na teh področjih, zlasti kar zadeva zbiranje in analizo podatkov o kibernetskih grožnjah in incidentih.

(4) Unija je že sprejela več ukrepov za zmanjšanje ranljivosti in povečanje odpornosti kritične infrastrukture in subjektov proti tveganjem, zlasti Uredbo (EU) 2019/881 Evropskega parlamenta in Sveta ([5]), direktivi 2013/40/EU ([6]) in (EU) 2022/2555 ([7]) Evropskega parlamenta in Sveta ter Priporočilo Komisije (EU) 2017/1584 ([8]). Poleg tega so države članice v Priporočilu Sveta z dne 8. decembra 2022 o usklajenem vseevropskem pristopu za krepitev odpornosti kritične infrastrukture pozvane, naj sprejmejo ukrepe ter 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 jasnega tveganja hitrega prelivanja incidentov iz ene države članice v druge in iz tretje države v Unijo, je treba okrepiti solidarnost na ravni Unije za boljše odkrivanje kibernetskih groženj in incidentov, pripravo in odzivanje nanje ter obnovitev po njih, zlasti s krepitvijo zmogljivosti obstoječih struktur. Poleg tega je Svet v sklepih z dne 23. maja 2022 o oblikovanju kibernetske drže Evropske unije pozval Komisijo, naj predstavi predlog o novem skladu za odzivanje na izredne razmere na področju kibernetske varnosti.

(6) V skupnem sporočilu Komisije in visokega predstavnika Unije za zunanje zadeve in varnostno politiko z dne 10. novembra 2022 Evropskemu parlamentu in Svetu o politiki EU za kibernetsko obrambo je bila napovedana pobuda EU za kibernetsko solidarnost s cilji okrepitve skupnih zmogljivosti EU za odkrivanje, situacijskega zavedanja in odzivanja s spodbujanjem uvedbe infrastrukture centrov za varnostne operacije v EU, podpiranjem postopne vzpostavitve rezerve za kibernetsko varnost na ravni EU s storitvami zaupanja vrednih zasebnih ponudnikov in preskušanjem kritičnih subjektov glede morebitnih ranljivosti na podlagi ocen tveganja EU.

(7) Izboljšati je treba odkrivanje kibernetskih groženj in incidentov ter situacijsko zavedanje o njih po vsej Uniji ter okrepiti solidarnost s povečanjem pripravljenosti in zmogljivosti držav članic in Unije za preprečevanje in odzivanje na pomembne kibernetske incidente in kibernetske incidente velikih razsežnosti. Zato bi bilo treba vzpostaviti vseevropsko mrežo kibernetskih vozlišč (v nadaljnjem besedilu: evropski sistem za opozarjanje na področju kibernetske varnosti), da bi se oblikovale usklajene zmogljivosti za odkrivanje in situacijsko zavedanje ter tako okrepile zmogljivosti Unije za odkrivanje groženj in deljenje informacij o njih; vzpostaviti bi bilo treba mehanizem za izredne razmere na področju kibernetske varnosti, da bi države članice na njihovo zahtevo podprli pri pripravi na pomembne kibernetske incidente in kibernetske incidente velikih razsežnosti, odzivanju nanje, blaženju njihovih posledic in začetku obnovitve po njih ter druge uporabnike podprli pri odzivanju na pomembne kibernetske incidente in kibernetske incidente, enakovredne incidentom velikih razsežnosti; vzpostaviti bi bilo treba evropski mehanizem za pregledovanje kibernetskih incidentov za pregledovanje in ocenjevanje posameznih pomembnih kibernetskih incidentov ali kibernetskih incidentov velikih razsežnosti. Ukrepi, sprejeti na podlagi te uredbe, bi se morali izvajati ob ustreznem upoštevanju pristojnosti držav članic ter bi morali dopolnjevati in ne podvajati dejavnosti, ki jih izvajajo mreža skupin CSIRT, Evropska organizacijska mreža za povezovanje v kibernetski krizi (v nadaljnjem besedilu: mreža EU-CyCLONe) ali skupina za sodelovanje na področju varnosti omrežnih in informacijskih sistemov (v nadaljnjem besedilu: skupina za sodelovanje), vse ustanovljene na podlagi Direktive (EU) 2022/2555. Ti ukrepi ne posegajo v člena 107 in 108 Pogodbe o delovanju Evropske unije (PDEU).

([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).

([6]) 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).

([7]) 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 VOIS 2) (UL L 333, 27.12.2022, str. 80).

([8]) 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).

(8) Za dosego teh ciljev je treba na nekaterih področjih spremeniti Uredbo (EU) 2021/694 Evropskega parlamenta in Sveta ([9]). Zlasti bi bilo treba s to uredbo spremeniti Uredbo (EU) 2021/694, kar zadeva dodajanje novih operativnih ciljev v zvezi z evropskim sistemom za opozarjanje na področju kibernetske varnosti in mehanizmom za izredne razmere na področju kibernetske varnosti 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 kibernetskih groženj in odzivanje nanje ter izboljšati čezmejno sodelovanje in usklajevanje na področju kibernetske varnosti. Evropski sistem za opozarjanje na področju kibernetske varnosti bi lahko imel pomembno vlogo pri podpiranju držav članic pri predvidevanju kibernetskih groženj in zaščiti pred njimi, EU rezerva za kibernetsko varnost pa pri podpiranju držav članic, institucij, organov, uradov in agencij Unije ter tretjih držav, pridruženih programu Digitalna Evropa, pri odzivanju na pomembne kibernetske incidente, kibernetske incidente velikih razsežnosti in kibernetske incidente, enakovredne incidentom velikih razsežnosti, ter pri blaženju njihovih posledic. Te posledice bi lahko bili znatna materialna ali nematerialna škoda ter resna tveganja za javno varnost in zaščito in podobno. Glede na posebni vlogi, ki bi ju lahko imela evropski sistem za opozarjanje na področju kibernetske varnosti in EU rezerva za kibernetsko varnost, bi bilo treba s to uredbo spremeniti Uredbo (EU) 2021/694, kar zadeva sodelovanje pravnih subjektov, ki so bili ustanovljeni v Uniji, nadzirani pa so iz tretjih držav, kadar obstaja resnično tveganje, da v Uniji ni na voljo potrebnih in zadostnih orodij, infrastrukture in storitev ali tehnologije, strokovnega znanja in zmogljivosti, koristi vključitve teh subjektov pa so večje od varnostnega tveganja. Določiti bi bilo treba posebne pogoje, pod katerimi se lahko dodeli finančna podpora za ukrepe, s katerimi se izvajata evropski sistem za opozarjanje na področju kibernetske varnosti in EU rezerva za kibernetsko varnost, 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.

(9) Za okrepitev odziva Unije na kibernetske grožnje in incidente je ključno sodelovanje z mednarodnimi organizacijami ter z zaupanja vrednimi, podobno mislečimi mednarodnimi partnerji. V tem okviru bi bilo treba zaupanja vredne, podobno misleče mednarodne partnerje razumeti kot države, ki delijo načela, ki so bila podlaga nastanka Unije, in sicer demokracija, pravna država, univerzalnost in nedeljivost človekovih pravic in temeljnih svoboščin, spoštovanje človekovega dostojanstva, enakost in solidarnost ter spoštovanje načel Ustanovne listine Združenih narodov in mednarodnega prava, ter ki ne ogrožajo bistvenih varnostnih interesov Unije ali njenih držav članic. To sodelovanje bi lahko bilo koristno tudi pri ukrepih, sprejetih na podlagi te uredbe, zlasti pri evropskem sistemu za opozarjanje na področju kibernetske varnosti in EU rezervi za kibernetsko varnost. Uredba (EU) 2021/694 bi morala, pod nekaterimi pogoji glede razpoložljivosti in varnosti, določati, da so razpisi za evropski sistem za opozarjanje na področju kibernetske varnosti in EU rezervo za kibernetsko varnost odprti tudi za pravne subjekte, ki so nadzorovani iz tretjih držav, in sicer ob izpolnjevanju varnostnih zahtev. Pomembno je, da se pri ocenjevanju varnostnega tveganja, povezanega s takim odpiranjem javnega naročanja, upoštevajo načela in vrednote, ki jih Unija deli s podobno mislečimi mednarodnimi partnerji, kadar so ta načela in vrednote povezana z njenimi bistvenimi varnostnimi interesi. Poleg tega bi se lahko pri obravnavi teh varnostnih zahtev na podlagi Uredbe (EU) 2021/694 upoštevalo več elementov, kot so korporativna struktura in postopek odločanja subjekta, varnost podatkov in tajnih ali občutljivih informacij ter zagotavljanje, da rezultati ukrepa ne bodo predmet nadzora ali omejitev neupravičenih tretjih držav.

(10) 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 ukrepe, določene v okviru specifičnega cilja 3 programa Digitalna Evropa. Posebni pogoji za sodelovanje v zvezi z vsakim ukrepom morajo biti določeni v ustreznih delovnih programih v skladu z Uredbo (EU) 2021/694.

(11) 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) 2024/2509 Evropskega parlamenta in Sveta ([10]) in določajo zlasti postopek za določitev in izvrševanje proračuna Unije ter urejajo nadzor nad odgovornostmi

([9]) 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).

([10]) Uredba (EU, Euratom) 2024/2509 Evropskega parlamenta in Sveta z dne 23. septembra 2024 o finančnih pravilih, ki se uporabljajo za splošni proračun Unije (UL L, 2024/2509, 26.9.2024, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).

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 ([11]).

(12) Čeprav so ukrepi za preprečevanje in pripravljenost bistveni za krepitev odpornosti Unije pri obravnavanju pomembnih kibernetskih incidentov, kibernetskih incidentov velikih razsežnosti in kibernetskih incidentov, enakovrednih incidentom velikih razsežnosti, pa se pojav, čas in obseg teh incidentov ne dajo predvideti. Finančna sredstva, ki so potrebna za zagotovitev ustreznega odziva, se iz leta v leto precej spreminjajo in bi morala biti na voljo takoj. Za združevanje proračunskega načela predvidljivosti s potrebo po hitrem odzivanju na nove potrebe bi bilo treba torej prilagoditi finančno izvajanje delovnih programov. Zato je primerno, da se poleg prenosa odobritev, odobrenega na podlagi člena 12(4) Uredbe (EU, Euratom) 2024/2509, odobri tudi prenos neporabljenih odobritev, vendar samo za naslednje leto ter samo za EU rezervo za kibernetsko varnost in ukrepe, ki podpirajo medsebojno pomoč.

(13) 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 infrastrukturo na ozemlju Unije, vključno z njihovo geografsko porazdelitvijo, medsebojno povezanostjo in morebitnimi učinki v primeru kibernetskih napadov na to infrastrukturo. Proaktiven pristop k prepoznavanju, blaženju in preprečevanju kibernetskih groženj vključuje povečano zmogljivost boljšega odkrivanja teh groženj. Evropski sistem za opozarjanje na področju kibernetske varnosti bi moral biti sestavljen iz več interoperabilnih čezmejnih kibernetskih vozlišč, od katerih vsako združuje tri ali več nacionalnih kibernetskih vozlišč. Ta infrastruktura bi morala služiti interesom in potrebam držav in Unije na področju kibernetske varnosti, spodbujati najsodobnejšo tehnologijo za napredno zbiranje ustreznih, po potrebi anonimiziranih, podatkov in informacij, in analitična orodja, okrepiti usklajene zmogljivosti kibernetskega odkrivanja in upravljanja ter zagotavljati situacijsko zavedanje v realnem času. Ta infrastruktura bi morala biti namenjena izboljšanju kibernetske drže, in sicer s povečanjem odkrivanja, združevanja in analize podatkov in informacij, da bi se preprečile kibernetske grožnje in incidenti ter tako dopolnjevali in podpirali subjekti in omrežja Unije, odgovorni za obvladovanje kibernetskih kriz v Uniji, zlasti mreža EU-CyCLONe.

(14) Države članice v evropskem sistemu za opozarjanje na področju kibernetske varnosti sodelujejo prostovoljno. Vsaka država članica bi morala imenovati en sam subjekt na nacionalni ravni, ki bi bil zadolžen za usklajevanje dejavnosti odkrivanja kibernetskih groženj v tej državi članici. Ta nacionalna kibernetska vozlišča bi morala delovati kot referenčna točka in točka dostopa na nacionalni ravni za sodelovanje v evropskem sistemu za opozarjanje na področju kibernetske varnosti ter zagotoviti, da se informacije o kibernetskih grožnjah, ki jih predložijo javni in zasebni subjekti, na nacionalni ravni delijo in zbirajo na učinkovit in poenostavljen način. Nacionalna kibernetska vozlišča bi lahko okrepila sodelovanje in deljenje informacij med javnimi in zasebnimi subjekti, podpirala pa bi lahko tudi izmenjavo relevantnih podatkov in informacij z ustreznimi sektorskimi in medsektorskimi skupnostmi, vključno z ustreznimi panožnimi centri za izmenjavo in analizo informacij. Za krepitev kibernetske odpornosti Unije je osrednjega pomena, da javni in zasebni subjekti tesno in usklajeno sodelujejo med seboj. Tako sodelovanje je še posebej dragoceno v okviru deljenja analitike kibernetskih groženj, da bi se izboljšala aktivna kibernetska zaščita. Nacionalna kibernetska vozlišča bi lahko v okviru takega sodelovanja in deljenja informacij zahtevala specifične informacije in jih tudi prejela. Ta uredba nacionalnih kibernetskih vozlišč ne obvezuje niti jih ne pooblašča za izvrševanje takih zahtev. Kadar je ustrezno ter v skladu s pravom Unije in nacionalnim pravom, bi lahko zahtevane ali prejete informacije vključevale telemetrične in senzorske podatke ter podatke o beleženju od subjektov, kot so ponudniki upravljanih varnostnih storitev, ki delujejo v visoko kritičnih sektorjih ali drugih kritičnih sektorjih v tej državi članici, da bi že v zgodnji fazi hitreje odkrivali morebitne kibernetske grožnje in incidente, s tem pa izboljšali situacijsko zavedanje. Če nacionalno kibernetsko vozlišče ni pristojni organ, ki ga je imenovala ali ustanovila ustrezna država članica na podlagi člena 8(1) Direktive (EU) 2022/2555, je osrednjega pomena, da se o zahtevah za take podatke in njihovem prejemu usklajuje s tem pristojnim organom.

(15) V okviru evropskega sistema za opozarjanje na področju kibernetske varnosti bi bilo treba ustanoviti več čezmejnih kibernetskih vozlišč. Ta čezmejna kibernetska vozlišča bi morala združevati nacionalna kibernetska vozlišča iz vsaj treh držav članic, da bi lahko v celoti izkoristili prednosti čezmejnega odkrivanja groženj ter deljenja in upravljanja informacij. Splošna cilja čezmejnih kibernetskih vozlišč bi morala biti okrepitev zmogljivosti za analizo,

([11]) 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).

preprečevanje in odkrivanje kibernetskih groženj ter podpora pripravi visokokakovostne analitike kibernetskih groženj, zlasti z deljenjem ustreznih, po potrebi anonimiziranih, informacij v zaupanja vrednem in varnem okolju 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. Čezmejna kibernetska vozlišča bi morala zagotoviti nove dodatne zmogljivosti, ki bi temeljile na obstoječih centrih za varnostne operacije, skupinah CSIRT ter drugih ustreznih akterjih, vključno z mrežo skupin CSIRT, in jih dopolnjevale.

(16) Država članica, ki jo Evropski industrijski, tehnološki in raziskovalni kompetenčni center za kibernetsko varnost (ECCC), vzpostavljen z Uredbo (EU) 2021/887 Evropskega parlamenta in Sveta ([12]), na podlagi razpisa za prijavo interesa izbere za vzpostavitev ali okrepitev zmogljivosti nacionalnega kibernetskega vozlišča, bi morala skupaj z ECCC kupiti ustrezna orodja, infrastrukturo ali storitve. Taka država članica bi morala biti upravičena do nepovratnih sredstev za upravljanje orodij, infrastrukture ali storitev. Gostiteljski konzorcij, ki ga sestavljajo vsaj tri države članice in ki ga izbere ECCC na podlagi razpisov za prijavo interesa za vzpostavitev ali okrepitev zmogljivosti čezmejnega kibernetskega vozlišča, bi moral kupiti ustrezna orodja, infrastrukturo ali storitve skupaj z ECCC. Gostiteljski konzorcij bi moral biti upravičen do nepovratnih sredstev za upravljanje orodij, infrastrukture ali storitev. Postopek javnega naročanja za nakup ustreznih orodij, infrastrukture ali storitev bi morali skupaj izvesti ECCC in ustrezni javni naročniki držav članic, izbranih na podlagi takih razpisov za prijavo interesa. Tako javno naročanje bi moralo biti skladno s členom 168(2) Uredbe (EU, Euratom) 2024/2509 in finančnimi pravili ECCC. Zasebni subjekti zato ne bi smeli biti upravičeni do sodelovanja v razpisih za prijavo interesa za nakup orodij, infrastrukture ali storitev skupaj z ECCC, niti do prejemanja nepovratnih sredstev za upravljanje teh orodij, infrastrukture ali storitev. Vendar bi morale imeti države članice možnost, da zasebne subjekte v vzpostavitev, izboljšanje in delovanje njihovih nacionalnih kibernetskih vozlišč in čezmejnih nacionalnih vozlišč vključijo na druge načine, ki se jim zdijo primerni, v skladu s pravom Unije in nacionalnim pravom. Zasebni subjekti bi prav tako lahko bili upravičeni do prejemanja financiranja Unije na podlagi Uredbe (EU) 2021/887 za namene podpore nacionalnih kibernetskih vozlišč.

(17) Za izboljšanje odkrivanja kibernetskih groženj in situacijskega zavedanja v Uniji bi se morala država članica, ki je na podlagi razpisov za prijavo interesa izbrana za vzpostavitev ali okrepitev zmogljivosti nacionalnega kibernetskega vozlišča, zavezati, da se bo prijavila za sodelovanje v čezmejnem kibernetskem vozlišču. Če država članica ne sodeluje v čezmejnem kibernetskem vozlišču v dveh letih od datuma pridobitve orodij, infrastrukture ali storitev ali datuma prejema nepovratnih sredstev, kateri koli nastopi prej, ne bi smela biti upravičena do sodelovanja pri nadaljnjih podpornih ukrepih Unije v okviru evropskega sistema za opozarjanje na področju kibernetske varnosti za krepitev zmogljivosti svojega nacionalnega kibernetskega vozlišča. V takih primerih bi lahko subjekti iz držav članic še vedno sodelovali v razpisih za zbiranje predlogov o drugih temah v okviru programa Digitalna Evropa ali drugih programov financiranja Unije, vključno z razpisi za zmogljivosti za kibernetsko odkrivanje in izmenjavo informacij, če ti subjekti izpolnjujejo merila upravičenosti, določena v teh programih.

(18) Skupine CSIRT si informacije izmenjujejo v okviru mreže skupin CSIRT v skladu z Direktivo (EU) 2022/2555. Evropski sistem za opozarjanje na področju kibernetske varnosti bi moral predstavljati novo zmogljivost, ki dopolnjuje mrežo skupin CSIRT, saj bi prispeval k boljšemu situacijskemu zavedanju Unije, kar bi omogočilo okrepitev zmogljivosti mreže skupin CSIRT. Čezmejna kibernetska vozlišča bi se morala usklajevati in tesno sodelovati z mrežo skupin CSIRT. Delovati bi morala z združevanjem podatkov in deljenjem ustreznih, po potrebi anonimiziranih, informacij javnih in zasebnih subjektov o kibernetskih grožnjah, povečevanjem vrednosti takih podatkov in informacij s strokovno analizo ter skupno pridobljeno infrastrukturo in najsodobnejšimi orodji ter s prispevanjem k tehnološki suverenosti Unije, njeni odprti strateški avtonomiji, konkurenčnosti in odpornosti ter razvoju zmogljivosti Unije.

(19) Čezmejna kibernetska vozlišča bi morala delovati kot osrednje točke, ki bi omogočale obsežno združevanje ustreznih podatkov in analitike kibernetskih groženj, ter omogočati širjenje informacij o grožnjah med velikim in raznolikim naborom deležnikov, na primer skupinami za odzivanje na računalniške grožnje (v nadaljnjem besedilu: skupine CERT), skupinami CSIRT, centri za izmenjavo in analizo informacij ter upravljavci kritičnih infrastruktur. Članice gostiteljskega konzorcija bi morale v konzorcijski pogodbi navesti ustrezne informacije, ki jih je treba deliti med sodelujočimi v zadevnem čezmejnem kibernetskem vozlišču. Informacije, ki si jih izmenjujejo sodelujoči v čezmejnem kibernetskem vozlišču, bi lahko vključevale na primer podatke iz omrežij in senzorjev, obveščevalne podatke o grožnjah, kazalnike ogroženosti in kontekstualizirane informacije o incidentih, kibernetskih grožnjah,

([12]) 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).

skorajšnjih incidentih, ranljivostih, tehnikah in postopkih, sovražnih taktikah, specifičnih informacijah o grožnji in akterju, opozorilih glede kibernetske varnosti in priporočilih glede konfiguracije orodij za kibernetsko varnost za zaznavo kibernetskih napadov. Poleg tega bi morala čezmejna kibernetska vozlišča skleniti tudi sporazume o medsebojnem sodelovanju. Taki sporazumi o sodelovanju bi morali zlasti določati načela deljenja informacij in interoperabilnosti. Njihove klavzule v zvezi z interoperabilnostjo, zlasti oblike in protokoli za deljenje informacij, bi morale upoštevati smernice za interoperabilnost, ki jih je izdala Agencija Evropske unije za kibernetsko varnost, vzpostavljena z Uredbo (EU) 2019/881 (ENISA), in zato tudi temeljiti na teh smernicah. Te smernice bi bilo treba izdati hitro, da se zagotovi, da jih čezmejna kibernetska vozlišča lahko upoštevajo že v zgodnji fazi. V smernicah bi se morali upoštevati mednarodni standardi in najboljše prakse ter delovanje vseh vzpostavljenih čezmejnih kibernetskih vozlišč.

(20) Čezmejna kibernetska vozlišča in mreža skupin CSIRT bi morali tesno sodelovati, da bi zagotovili sinergije in dopolnjevanje dejavnosti. V ta namen bi se morali dogovoriti o postopkovnih ureditvah o sodelovanju in deljenju ustreznih informacij. To bi lahko vključevalo deljenje ustreznih informacij o kibernetskih grožnjah in pomembnih kibernetskih incidentih ter zagotavljanje deljenja izkušenj z najsodobnejšimi orodji, zlasti tehnologijo umetne inteligence in podatkovne analitike, ki se uporabljajo v čezmejnih kibernetskih vozliščih, z mrežo skupin CSIRT.

(21) Skupno situacijsko zavedanje med ustreznimi organi je nujen osnovni pogoj za pripravljenost in usklajevanje na ravni Unije v zvezi s pomembnimi kibernetskimi incidenti in kibernetskimi incidenti velikih razsežnosti. Z Direktivo (EU) 2022/2555 je bila ustanovljena mreža EU-CyCLONe za podporo usklajenemu obvladovanju kibernetskih incidentov velikih razsežnosti in kriz na operativni ravni ter zagotovitev redne izmenjave ustreznih informacij med državami članicami ter institucijami, organi, uradi in agencijami Unije. Z Direktivo (EU) 2022/2555 je bila vzpostavljena tudi mreža skupin CSIRT za spodbujanje hitrega in učinkovitega operativnega sodelovanja med vsemi državami članicami. Za zagotovitev situacijskega zavedanja in krepitev solidarnosti bi morala čezmejna kibernetska vozlišča v primerih, kadar pridobijo informacije v zvezi z morebitnim ali tekočim kibernetskim incidentom velikih razsežnosti, mreži skupin CSIRT zagotoviti ustrezne informacije in kot zgodnje opozarjanje obveščati mrežo EU-CyCLONe. Glede na okoliščine bi lahko informacije, ki jih je treba deliti, vključevale zlasti tehnične informacije, informacije o naravi in motivih napadalca ali morebitnega napadalca ter netehnične informacije na višji ravni o morebitnem ali tekočem kibernetskem incidentu velikih razsežnosti. V zvezi s tem bi bilo treba ustrezno upoštevati načelo potrebe po seznanitvi in morda občutljivo naravo deljenih informacij. 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 ([13]), ter njeno odgovornost za zagotavljanje analitičnih poročil za enotno ureditev EU za politično odzivanje na krize (v nadaljnjem besedilu: ureditev IPCR) na podlagi Izvedbenega sklepa Sveta (EU) 2018/1993 ([14]). Kadar čezmejna kibernetska vozlišča delijo ustrezne informacije in zgodnja opozorila v zvezi z morebitnim ali tekočim kibernetskim incidentom velikih razsežnosti z mrežo EU-CyCLONe in mrežo skupin CSIRT, je nujno, da se te informacije prek teh mrež delijo z organi držav članic in Komisijo. V zvezi s tem Direktiva (EU) 2022/2555 določa, da je mreža EU-CyCLONe namenjena podpiranju usklajenega obvladovanja kibernetskih incidentov velikih razsežnosti in kriz na operativni ravni ter zagotavljanju redne izmenjave ustreznih informacij med državami članicami ter institucijami, organi, uradi in agencijami Unije. Naloge mreže EU-CyCLONe vključujejo razvoj skupnega situacijskega zavedanja o takih incidentih in krizah. Izjemno pomembno je, da mreža EU-CyCLONe v skladu s svojim namenom in nalogami zagotovi, da se take informacije nemudoma zagotovijo ustreznim predstavnikom držav članic in Komisiji. V ta namen je bistveno, da poslovnik mreže EU-CyCLONe vključuje ustrezne določbe.

(22) Subjekti, ki sodelujejo v evropskem sistemu za opozarjanje na področju kibernetske varnosti, bi morali zagotoviti visoko raven medsebojne interoperabilnosti, po potrebi tudi kar zadeva formate podatkov, taksonomijo ter orodja za obravnavanje in analizo podatkov. Zagotoviti bi morali 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 vzrokov odkritih kibernetskih groženj in tveganj bi bilo treba upoštevati obstoječe delo, opravljeno v okviru izvajanja Direktive (EU) 2022/2555.

([13]) 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, ELI: http://data.europa.eu/eli/dec/2013/1313/oj).

([14]) 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).

(23) Da bi omogočili obsežno izmenjavo ustreznih podatkov in informacij o kibernetskih grožnjah iz različnih virov v zaupanja vrednem in varnem okolju, bi morali biti subjekti, ki sodelujejo v evropskem sistemu za opozarjanje na področju kibernetske varnosti, opremljeni z najsodobnejšimi, izjemno varnimi orodji, opremo in infrastrukturo 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.

(24) Evropski sistem za opozarjanje na področju kibernetske varnosti bi moral z zbiranjem, analiziranjem, deljenjem in izmenjavanjem ustreznih podatkov in informacij okrepiti tehnološko suverenost in odprto strateško avtonomijo Unije na področju kibernetske varnosti, konkurenčnosti in odpornosti. Združevanje visokokakovostnih pripravljenih podatkov bi lahko prispevalo tudi k razvoju naprednih tehnologij umetne inteligence in podatkovne analitike. Človeški nadzor in s tem tudi usposobljena delovna sila imata še vedno ključno vlogo pri učinkovitem združevanju visokokakovostnih podatkov.

(25) Čeprav je evropski sistem za opozarjanje na področju kibernetske varnosti civilni projekt, bi lahko imela kibernetsko obrambna skupnost koristi od okrepljenih zmogljivosti civilnega odkrivanja in situacijskega zavedanja, ki so bile razvite za zaščito kritične infrastrukture.

(26) Deljenje informacij med sodelujočimi v evropskem sistemu za opozarjanje na področju kibernetske varnosti 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. Prejemnik informacij bi moral, če je potrebna obdelava osebnih podatkov, izvajati tehnične in organizacijske ukrepe, ki varujejo pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, in podatke uničiti takoj, ko niso več potrebni za navedeni namen, ter subjekt, ki daje podatke na voljo, obvestiti, da so bili podatki uničeni.

(27) Ohranjanje zaupnosti in informacijske varnosti je bistvenega pomena za vse tri stebre te uredbe, bodisi za spodbujanje deljenja ali izmenjave informacij v okviru evropskega sistema za opozarjanje na področju kibernetske varnosti, ohranjanje interesov subjektov, ki zaprosijo za podporo v okviru mehanizma za izredne razmere na področju kibernetske varnosti, bodisi za zagotavljanje, da lahko poročila v okviru evropskega mehanizma za pregledovanje kibernetskih incidentov prinesejo koristna spoznanja, ne da bi negativno vplivala na subjekte, ki so jih incidenti prizadeli. Sodelovanje držav članic in subjektov v teh mehanizmih je odvisno od razmerij zaupanja med njihovimi sestavnimi deli. Kadar so informacije zaupne na podlagi pravil Unije ali nacionalnih pravil, bi moralo biti njihovo deljenje ali izmenjava na podlagi te uredbe omejeno na to, kar je ustrezno za namen deljenja ali izmenjave in sorazmerno z njim. Pri tem deljenju ali izmenjavi bi se morala ohraniti zaupnost zadevnih informacij, vključno z zaščito varnosti in poslovnih interesov zadevnih subjektov. Deljenje ali izmenjava informacij na podlagi te uredbe bi lahko potekala na podlagi sporazumov o nerazkrivanju podatkov ali smernic za razširjanje informacij, kot je semaforski protokol. Semaforski protokol je treba razumeti kot sredstvo za zagotavljanje informacij o kakršnih koli omejitvah v zvezi z nadaljnjim širjenjem informacij. Uporablja se v skoraj vseh skupinah CSIRT in nekaterih panožnih centrih za izmenjavo in analizo informacij. Poleg teh splošnih zahtev bi bilo treba v zvezi z evropskim sistemom za opozarjanje na področju kibernetske varnosti v pogodbah o gostiteljskih konzorcijih določiti posebna pravila v zvezi s pogoji za deljenje informacij v zadevnem čezmejnem kibernetskem vozlišču. Te pogodbe bi lahko zlasti zahtevale, da se informacije delijo samo v skladu s pravom Unije in nacionalnim pravom.

(28) V zvezi z uvedbo EU rezerve za kibernetsko varnost so potrebna posebna pravila o zaupnosti. Podpora se bo zahtevala, ocenila in nudila v kriznih razmerah in v zvezi s subjekti, ki delujejo v občutljivih sektorjih. Za učinkovito delovanje EU rezerve za kibernetsko varnost je bistveno, da lahko uporabniki in subjekti brez odlašanja delijo vse informacije, ki jih vsak subjekt potrebuje za sodelovanje pri ocenjevanju zahtevkov in uporabi podpore, ter omogočijo dostop do njih. V skladu s tem bi morala ta uredba določati, da se vse take informacije uporabijo ali delijo le, kadar je to potrebno za delovanje EU rezerve za kibernetsko varnost, ter da bi se morale informacije, ki so zaupne ali tajne na podlagi prava Unije in nacionalnega prava, uporabljati in deliti le v skladu s tem pravom. Poleg tega bi morali imeti uporabniki možnost, da za podrobnejšo opredelitev omejitev po potrebi uporabijo protokole za deljenje informacij, kot je semaforski protokol. Čeprav imajo uporabniki v zvezi s tem diskrecijsko pravico, je pomembno, da pri uporabi takih omejitev upoštevajo možne posledice, zlasti v zvezi z zamudo pri ocenjevanju ali zagotavljanju zahtevanih storitev. Za učinkovito EU rezervo za kibernetsko varnost je pomembno, da javni naročnik

pred vložitvijo zahtevka uporabniku pojasni te posledice. Ti zaščitni ukrepi so omejeni na zahtevek za storitve EU rezerve za kibernetsko varnost in njihovo zagotavljanje ter ne vplivajo na izmenjavo informacij v drugih okvirih, na primer pri javnem naročanju EU rezerve za kibernetsko varnost.

(29) Glede na vse večja tveganja in število incidentov, ki prizadenejo države članice, je treba vzpostaviti instrument podpore ob krizi, in sicer mehanizem za izredne razmere na področju kibernetske varnosti, da se izboljša odpornost Unije proti pomembnim kibernetskim incidentom, kibernetskim incidentom velikih razsežnosti in kibernetskim incidentom, enakovrednim incidentom velikih razsežnosti, ter da se ukrepi držav članic dopolnijo z nujno finančno podporo za pripravljenost, odzivanje na incidente in začetno obnovitev bistvenih storitev. Ker je popolna obnovitev po incidentu celovit proces ponovne vzpostavitve delovanja subjekta, ki ga je incident prizadel, v stanje pred incidentom in bi lahko bil dolgotrajen proces z znatnimi stroški, bi morala biti podpora iz EU rezerve za kibernetsko varnost omejena na začetno fazo procesa obnovitve, ki bi privedla do ponovne vzpostavitve osnovnih funkcij sistemov. Mehanizem za izredne razmere na področju kibernetske varnosti 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 preprečevanje incidentov in kriz ter pripravo in odzivanje nanje v prvi vrsti odgovorne države članice, mehanizem za izredne razmere na področju kibernetske varnosti spodbuja solidarnost med državami članicami v skladu s členom 3(3) Pogodbe o Evropski uniji (PEU).

(30) Mehanizem za izredne razmere na področju kibernetske varnosti bi moral državam članicam zagotoviti podporo z dopolnjevanjem njihovih ukrepov in virov ter druge obstoječe možnosti podpore v primeru odziva na pomembne kibernetske incidente in kibernetske incidente velikih razsežnosti ter začetne obnovitve po njih, kot so storitve, ki jih zagotavlja 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), vzpostavljenih na podlagi Sklepa Sveta (SZVP) 2017/2315 ([15]). Obravnavati bi moral potrebo po zagotavljanju razpoložljivosti specializiranih sredstev za podporo pripravljenosti in odzivanju na take incidente ter obnovitvi po njih po vsej Uniji in v tretjih državah, pridruženih programu Digitalna Evropa.

(31) Ta uredba ne posega v postopke in okvire za usklajevanje odzivanja na krize na ravni Unije, zlasti Direktivo (EU) 2022/2555, mehanizem Unije na področju civilne zaščite, vzpostavljen s Sklepom št. 1313/2013/EU Evropskega parlamenta in Sveta ([16]), ureditev IPCR ter Priporočilo Komisije (EU) 2017/1584 ([17]). Podpora, zagotovljena v okviru mehanizma za izredne razmere na področju kibernetske varnosti, lahko 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, ob upoštevanju civilne narave mehanizma za izredne razmere na področju kibernetske varnosti. Podpora, zagotovljena v okviru mehanizma za izredne razmere na področju kibernetske varnosti, lahko dopolnjuje ukrepe, ki se izvajajo v okviru člena 42(7) PEU, vključno s pomočjo, ki jo ena država članica zagotovi drugi državi članici, ali je del skupnega odziva Unije in držav članic ali v primerih iz člena 222 PDEU. Izvajanje te uredbe bi bilo treba po potrebi uskladiti tudi z izvajanjem ukrepov iz zbirke orodij za kibernetsko diplomacijo.

(32) 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, ENISA, državami članicami in po potrebi ECCC. Kadar države članice zaprosijo za podporo v okviru mehanizma za izredne razmere na področju kibernetske varnosti, bi morale predložiti ustrezne informacije, s katerimi utemeljijo potrebo po podpori.

(33) 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 kibernetske incidente velikih razsežnosti in krize, v katerem so opredeljeni cilji in ureditve obvladovanja kibernetskih 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

([15]) Sklep Sveta (SZVP) 2017/2315 z dne 11. decembra 2017 o vzpostavitvi stalnega strukturnega sodelovanja (PESCO) in določitvi seznama sodelujočih držav članic (UL L 331, 14.12.2017, str. 57, ELI: http://data.europa.eu/eli/dec/2017/2315/oj).

([16]) 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).

([17]) 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).

zajemale vsaj sektorje, podsektorje in vrste subjekta, ki spadajo na področje uporabe navedene direktive, ter jim zagotoviti zadostna 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 razmere na področju kibernetske varnosti bi moral zagotavljati pomoč za ukrepe, namenjene krepitvi pripravljenosti, in ukrepe za odzivanje na incidente, da bi ublažili posledice pomembnih kibernetskih incidentov in kibernetskih incidentov velikih razsežnosti, podprli začetno obnovitev ali ponovno vzpostavili osnovne funkcionalnosti storitev, ki jih zagotavljajo subjekti, ki delujejo v visoko kritičnih sektorjih, ali subjekti, ki delujejo v drugih kritičnih sektorjih.

(34) 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 na podlagi Direktive (EU) 2022/2555, tudi z vajami in usposabljanjem. V ta namen bi morala Komisija po posvetovanju z ENISA, skupino za sodelovanje in mrežo EU-CyCLONe redno določati ustrezne sektorje ali podsektorje, ki bi morali biti upravičeni do prejemanja finančne podpore za usklajeno preskušanje pripravljenosti na ravni Unije. Sektorje ali podsektorje bi bilo treba izbrati izmed visoko kritičnih sektorjev, navedenih v Prilogi I k Direktivi (EU) 2022/2555. Usklajeno preskušanje pripravljenosti 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 Unije za zunanje zadeve in varnostno politiko (v nadaljnjem besedilu: visoki predstavnik) in skupina za sodelovanje 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 infrastrukture, ki se zahteva na podlagi skupnega ministrskega poziva iz Neversa ter jo izvede skupina za sodelovanje ob podpori Komisije in ENISA ter v sodelovanju z Organom evropskih regulatorjev za elektronske komunikacije, ustanovljenim z Uredbo (EU) 2018/1971 Evropskega parlamenta in Sveta ([18]), usklajene ocene tveganja za varnost na ravni Unije za kritične dobavne verige, ki se izvedejo na podlagi člena 22 Direktive (EU) 2022/2555, in testiranje digitalne operativne odpornosti, kot je določeno v Uredbi (EU) 2022/2554 Evropskega parlamenta in Sveta ([19]). Pri izbiri sektorjev bi bilo treba upoštevati tudi priporočilo Sveta o usklajenem vseevropskem pristopu za krepitev odpornosti kritične infrastrukture.

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

(36) Kadar države članice prejmejo nepovratna sredstva za podporo ukrepom za pripravljenost, lahko subjekti v visoko kritičnih sektorjih prostovoljno sodelujejo pri teh ukrepih. Dobra praksa je, da na podlagi takih ukrepov sodelujoči subjekti pripravijo načrt popravnih ukrepov za izvedbo vseh priporočil glede posameznih ukrepov, ki izhajajo iz tega, da bi kar najbolje izkoristili koristi ukrepa za pripravljenost. Čeprav je pomembno, da države članice v okviru ukrepov zahtevajo, da sodelujoči subjekti pripravijo in izvajajo take načrte popravnih ukrepov, ta uredba države članice ne obvezuje niti jih ne pooblašča za izvrševanje takih zahtev. Take zahteve ne posegajo v zahteve za subjekte in nadzorna pooblastila za pristojne organe v skladu z Direktivo (EU) 2022/2555.

(37) Mehanizem za izredne razmere na področju kibernetske varnosti bi moral zagotavljati tudi podporo za ukrepe za odzivanje na incidente za ublažitev posledic pomembnih kibernetskih incidentov, kibernetskih incidentov velikih razsežnosti in kibernetskih incidentov, enakovrednim incidentom velikih razsežnosti, da bi se podprla začetna obnovitev ali ponovna vzpostavitev delovanja bistvenih storitev. Kadar je ustrezno, bi moral dopolnjevati mehanizem Unije na področju civilne zaščite, da se zagotovi celovit pristop k odzivanju na posledice incidentov za državljane.

([18]) Uredba (EU) 2018/1971 Evropskega parlamenta in Sveta z dne 11. decembra 2018 o ustanovitvi Organa evropskih regulatorjev za elektronske komunikacije (BEREC) in Agencije za podporo BEREC-u (Urad BEREC), spremembi Uredbe (EU) 2015/2120 ter razveljavitvi Uredbe (ES) št. 1211/2009 (UL L 321, 17.12.2018, str. 1).

([19]) 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 (UL L 333, 27.12.2022, str. 1).

(38) Mehanizem za izredne razmere na področju kibernetske varnosti bi moral podpirati tehnično pomoč, ki jo ena država članica zagotavlja drugi državi članici, ki jo je prizadel pomemben kibernetski incident ali kibernetski incident velikih razsežnosti, med drugim s skupinami CSIRT iz člena 11(3), točka (f), Direktive (EU) 2022/2555. Državam članicam, ki zagotovijo tako 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.

(39) Glede na bistveno vlogo, ki jo imajo zasebna podjetja pri odkrivanju kibernetskih incidentov velikih razsežnosti in kibernetskih incidentov, enakovrednih incidentom velikih razsežnosti, pripravljenosti in odzivanju nanje, je pomembno priznati vrednost prostovoljnega sodelovanja s takimi podjetji, ki bi ponujala storitve brez plačila v primeru kibernetskih incidentov velikih razsežnosti in kriz ter kibernetskih incidentov, enakovrednim incidentom velikih razsežnosti, in kriz. ENISA bi lahko v sodelovanju z mrežo EU-CyCLONe spremljala razvoj takih brezplačnih pobud in spodbujala njihovo skladnost z merili, ki se na podlagi te uredbe uporabljajo za zaupanja vredne ponudnike upravljanih varnostnih storitev, tudi v zvezi z zanesljivostjo zasebnih podjetij, njihovimi izkušnjami in zmožnostjo varnega ravnanja z občutljivimi informacijami.

(40) Kot del mehanizma za izredne razmere na področju kibernetske varnosti bi bilo treba postopno vzpostaviti EU rezervo za kibernetsko varnost, ki bi zajemala storitve zaupanja vrednih ponudnikov upravljanih varnostnih storitev za podporo ukrepom odzivanja in uvedbo ukrepov okrevanja v primeru pomembnih kibernetskih incidentov, kibernetskih incidentov velikih razsežnosti ali kibernetskih incidentov, enakovrednih incidentom velikih razsežnosti, ki prizadenejo države članice, institucije, organe, urade ali agencije Unije ali tretje države, pridružene programu Digitalna Evropa. EU rezerva za kibernetsko varnost bi morala zagotoviti razpoložljivost in pripravljenost storitev. Zato bi morala vključevati storitve, za katere so vnaprej prevzete obveznosti, vključno na primer z zmogljivostmi, ki so v pripravljenosti in jih je mogoče hitro uporabiti. Storitve iz EU rezerve za kibernetsko varnost bi morale biti namenjene podpori nacionalnim organom pri zagotavljanju pomoči prizadetim subjektom, ki delujejo v visoko kritičnih sektorjih, ali prizadetim subjektom, ki delujejo v drugih kritičnih sektorjih, kot dopolnitev njihovih ukrepov na nacionalni ravni. Moralo bi biti mogoče, da se storitve iz EU rezerve za kibernetsko varnost pod podobnimi pogoji uporabljajo tudi za podporo institucijam, organom, uradom in agencijam Unije. EU rezerva za kibernetsko varnost bi lahko prispevala tudi h krepitvi konkurenčnega položaja industrije in storitev v Uniji v celotnem digitalnem gospodarstvu, vključno z mikropodjetji, malimi in srednjimi podjetji ter zagonskimi podjetji, tudi z zagotavljanjem spodbud za naložbe v raziskave in inovacije. Pri zagotavljanju storitev za EU rezervo za kibernetsko varnost je pomembno upoštevati okvir znanj in spretnosti za kibernetsko varnost ENISA. Uporabniki bi morali ob vložitvi zahtevka za podporo iz EU rezerve za kibernetsko varnost v svojo vlogo vključiti ustrezne informacije o prizadetem subjektu in morebitnih posledicah, informacije o zahtevani storitvi iz EU rezerve za kibernetsko varnost ter podporo, zagotovljeno prizadetemu subjektu na nacionalni ravni, ki bi jo bilo treba upoštevati pri oceni zahtevka vlagatelja. Da bi dopolnili druge oblike podpore, ki so na voljo prizadetemu subjektu, bi zahtevek med drugim moral vključevati informacije, kadar so na voljo, o pogodbenih ureditvah za storitve odziva na incidente in storitve začetne obnovitve, ter zavarovalnih pogodbah, ki bi lahko krile tovrstne incidente.

(41) Za učinkovito uporabo sredstev Unije bi moralo biti možno storitve, k zagotavljanju katerih se ponudniki v okviru EU rezerve za kibernetsko varnost zavežejo vnaprej, v skladu z ustrezno pogodbo pretvoriti v storitve za pripravljenost, povezane s preprečevanjem incidentov in odzivanjem nanje, v primeru, da se te storitve, k zagotavljanju katerih se ponudniki zavežejo vnaprej, ne uporabijo za odziv na incidente v času, za katerega so se ponudniki zavezali vnaprej. Te storitve bi morale biti dopolnilne in ne bi smele podvajati ukrepov za pripravljenost, ki jih bo upravljal ECCC.

(42) Zahtevke za podporo iz EU rezerve za kibernetsko varnost, ki jih vložijo organi držav članic za obvladovanje kibernetskih kriz in skupine CSIRT ali CERT-EU v imenu institucij, organov, uradov in agencij Unije, bi moral oceniti javni naročnik. Kadar je bilo upravljanje in delovanje EU rezerve za kibernetsko varnost zaupano ENISA, je ta javni naročnik ENISA. Zahtevke za podporo iz tretjih držav, pridruženih programu Digitalna Evropa, bi morala oceniti Komisija. Za lažjo predložitev in oceno zahtevkov za podporo bi ENISA lahko vzpostavila varno platformo.

(43) Kadar je prejetih več sočasnih zahtevkov, bi bilo treba te zahtevke prednostno razvrstiti v skladu z merili iz te uredbe. Glede na splošne cilje te uredbe bi morala ta merila vključevati obseg in resnost incidenta, vrsto prizadetega subjekta, morebitni vpliv incidenta na prizadete države članice in uporabnike, morebitno čezmejno naravo incidenta in tveganje prelivanja ter ukrepe, ki jih je uporabnik že sprejel za pomoč pri odzivu in začetni obnovitvi. Ob upoštevanju teh ciljev in glede na to, da so zahteve uporabnikov iz držav članic namenjene izključno podpori

subjektom, ki delujejo v visoko kritičnih sektorjih, ali subjektom, ki delujejo v drugih kritičnih sektorjih, v Uniji, je primerno dati večjo prednost zahtevam uporabnikov iz držav članic, kadar sta dve zahtevi ali več na podlagi teh meril ocenjeni kot enakovredni. To ne posega v obveznosti, ki bi jih države članice lahko imele na podlagi ustreznih sporazumov o gostovanju, da sprejmejo ukrepe za zaščito institucij, organov, uradov in agencij Unije.

(44) Za izvajanje EU rezerve za kibernetsko varnost bi morala biti v celoti odgovorna Komisija. Glede na obsežne izkušnje, ki jih je ENISA pridobila s podpornim delovanjem za kibernetsko varnost, je ENISA najprimernejša agencija za izvajanje EU rezerve za kibernetsko varnost. Zato bi morala Komisija ENISA delno ali, kadar meni, da je to primerno, v celoti, zaupati delovanje in upravljanje EU rezerve za kibernetsko varnost. Ta prenos odgovornosti bi bilo treba izvesti v skladu z veljavnimi pravili iz Uredbe (EU, Euratom) 2024/2509 in zlasti bi zanj morali veljati ustrezni pogoji za podpis sporazuma o prispevku. Vse vidike delovanja in upravljanja EU rezerve za kibernetsko varnost, ki niso zaupani ENISA, bi morala Komisija neposredno upravljati, tudi pred podpisom sporazuma o prispevku.

(45) Države članice bi morale imeti ključno vlogo pri vzpostavljanju, uporabi in nadaljnjih ukrepih po uporabi EU rezerve za kibernetsko varnost. Ker je Uredba (EU) 2021/694 ustrezni temeljni akt za ukrepe, s katerimi se izvaja EU rezerva za kibernetsko varnost, bi bilo treba ukrepe iz te rezerve določiti v delovnih programih iz člena 24 Uredbe (EU) 2021/694. Na podlagi odstavka 6 navedenega člena bi morala Komisija te delovne programe sprejeti z izvedbenimi akti v skladu s postopkom pregleda. Komisija bi poleg tega morala določiti prednostne naloge in razvoj EU rezerve za kibernetsko varnost v sodelovanju s skupino za sodelovanje.

(46) Pogodbe, sklenjene v okviru EU rezerve za kibernetsko varnost, ne bi smele vplivati na odnose med podjetji in obstoječe obveznosti med prizadetim subjektom ali uporabniki in ponudnikom storitve.

(47) Za izbor zasebnih ponudnikov storitev, ki bi storitve zagotavljali v okviru EU rezerve za kibernetsko varnost, je treba določiti sklop minimalnih meril in zahtev, ki bi jih bilo treba vključiti v razpis za zbiranje ponudb za izbor teh ponudnikov, da se lahko zadosti potrebam organov držav članic, subjektov, ki delujejo v visoko kritičnih sektorjih, in subjektov, ki delujejo v drugih kritičnih sektorjih. Da bi obravnavali posebne potrebe držav članic pri javnem naročanju storitev za EU rezervo za kibernetsko varnost, bi moral javni naročnik po potrebi oblikovati merila in zahteve za izbor, poleg tistih iz te uredbe. Spodbujati je treba sodelovanje manjših ponudnikov, dejavnih na regionalni in lokalni ravni.

(48) Pri izbiri ponudnikov za vključitev v EU rezervo za kibernetsko varnost bi si moral javni naročnik prizadevati zagotoviti, da EU rezerva za kibernetsko varnost kot celota vsebuje ponudnike, ki se lahko prilagodijo jezikovnim zahtevam uporabnikov. V ta namen bi moral javni naročnik, preden pripravi razpisne zahteve, preveriti, ali imajo potencialni uporabniki EU rezerve za kibernetsko varnost posebne jezikovne zahteve, tako da se lahko podporne storitve EU rezerve za kibernetsko varnost zagotavljajo v enem od uradnih jezikov institucij Unije ali držav članic, ki ga uporabnik ali prizadeti subjekt verjetno razume. V primeru, da uporabnik zahteva več kot en jezik za zagotavljanje podpornih storitev EU rezerve za kibernetsko varnost in so bile te storitve zagotovljene v teh jezikih za tega uporabnika, bi moral ta uporabnik biti sposoben navesti, v zahtevi za podporo EU rezerve za kibernetsko varnost, v katerem od teh jezikov bi bilo treba zagotavljati storitve v zvezi s posebnim incidentom, na podlagi katerega je bila vložena zahteva.

(49) Pomembno je, da Komisija za podporo vzpostavitvi EU rezerve za kibernetsko varnost od ENISA zahteva, naj pripravi predlog certifikacijske sheme za kibernetsko varnost za upravljane varnostne storitve na podlagi Uredbe (EU) 2019/881 na področjih, ki jih zajema mehanizem za izredne razmere na področju kibernetske varnosti.

(50) Za podporo ciljem te uredbe glede spodbujanja skupnega situacijskega zavedanja, krepitve odpornosti Unije ter omogočanja učinkovitega odziva na pomembne kibernetske incidente in kibernetske incidente velikih razsežnosti bi morala imeti Komisija ali mreža EU-CyCLONe, s podporo mreže skupin CSIRT in z odobritvijo zadevnih držav članic, možnost, da ENISA zaprosita, naj pregleda in oceni kibernetske grožnje, znane ranljivosti, ki jih mogoče izrabiti, in blažitvene ukrepe v zvezi s posameznim pomembnim kibernetskim incidentom ali kibernetskim incidentom velikih razsežnosti. Po zaključku pregleda in ocene incidenta bi morala ENISA v sodelovanju z zadevno državo članico, ustreznimi deležniki, vključno s predstavniki iz zasebnega sektorja, Komisije in drugih ustreznih

institucij, organov, uradov in agencij Unije, pripraviti poročilo o pregledu incidenta. 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, ki bi ga morale upoštevati pri svojem delu, kakor tudi delu ENISA. Kadar je incident povezan s tretjo državo, pridruženo programu Evropa, bi morala Komisija poročilo zagotoviti tudi visokemu predstavniku.

(51) 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 kibernetske incidente in kibernetske incidente, enakovredne incidentom velikih razsežnosti, prispeva k zaščiti Unije in zlasti njenega notranjega trga in industrije kot celote. Takšne dejavnosti bi lahko dodatno prispevale h kibernetski diplomaciji Unije. Zato bi morale imeti tretje države, pridružene programu Digitalna Evropa, možnost, da zaprosijo za podporo iz EU rezerve za kibernetsko varnost na celotnem ali delu svojega ozemlja, kadar je to določeno v sporazumu, preko katerega je tretja država pridružena programu Digitalna Evropa. Unija bi morala financiranje za tretje države, pridružene programu Digitalna Evropa, podpreti v okviru ustreznih partnerstev in instrumentov financiranja za te države. Podpora bi morala zajemati storitve na področju odzivanja na pomembne kibernetske incidente ali kibernetske incidente, enakovredne incidentom velikih razsežnosti in začetno obnovitev po njih.

(52) Pri zagotavljanju podpore tretjim državam, pridruženim programu Digitalna Evropa, bi se morali uporabljati pogoji, določeni za EU rezervo za kibernetsko varnost in zaupanja vredne ponudnike upravljanih varnostnih storitev v tej uredbi. Tretje države, pridružene programu Digitalna Evropa, bi morale imeti možnost, da za podporo zaprosijo EU rezervo za kibernetsko varnost, kadar so ciljni subjekti, za katere zaprosijo za podporo iz EU rezerve za kibernetsko varnost, subjekti, ki delujejo v visoko kritičnih sektorjih, ali subjekti, ki delujejo v drugih kritičnih sektorjih, in kadar odkriti incidenti povzročijo znatne operativne motnje oziroma bi lahko imeli učinke prelivanja v Uniji. Tretje države, pridružene programu Digitalna Evropa, lahko prejmejo podporo le, kadar je to določeno v sporazumu, preko katerega je tretja država pridružena programu Digitalna Evropa. Poleg tega bi morale take tretje države ostati upravičene le, če so izpolnjena tri merila. Prvič, tretja država bi morala v celoti spoštovati ustrezne pogoje tega sporazuma. Drugič, glede na dopolnilno naravo EU rezerve za kibernetsko varnost bi morala tretja država sprejeti ustrezne ukrepe za pripravo na pomembne kibernetske incidente ali kibernetske incidente, enakovredne incidentom velikih razsežnosti. Tretjič, zagotavljanje podpore iz EU rezerve za kibernetsko varnost bi moralo biti skladno s politiko Unije do te države in njenimi splošnimi odnosi z njo ter z drugimi politikami Unije na področju varnosti. V okviru svoje ocene glede skladnosti s tem tretjim merilom bi se morala Komisija posvetovati z visokim predstavnikom glede uskladitve dodeljevanja te podpore s skupno zunanjo in varnostno politiko.

(53) Zagotavljanje podpore tretjim državam, pridruženim programu Digitalna Evropa, lahko vpliva na odnose s tretjimi državami in varnostno politiko Unije, tudi v okviru skupne zunanje in varnostne politike ter skupne varnostne in obrambne politike. Zato je primerno, da se Svetu podelijo izvedbena pooblastila za odobritev in določitev obdobja, v katerem se taka podpora lahko zagotavlja. Svet bi moral ukrepati na podlagi predloga Komisije, ob upoštevanju ocene treh meril, ki jo je opravila Komisija. Enako bi moralo veljati za podaljšanja in predloge za spremembo ali razveljavitev takih aktov. Kadar Svet v izjemnih okoliščinah meni, da je pri tretjem merilu prišlo do občutne spremembe okoliščin, bi moral imeti možnost, da ukrepa na lastno pobudo s spremembo ali razveljavitvijo izvedbenega akta, ne da bi čakal na predlog Komisije. Take pomembne spremembe bodo verjetno zahtevale nujno ukrepanje, s še posebej pomembnimi posledicami za odnose s tretjimi državami, in predhodne natančne ocene Komisije ne bodo potrebne. Poleg tega bi Komisija morala sodelovati z visokim predstavnikom glede zahtev za podporo od tretjih držav, pridruženih programu Digitalna Evropa, in izvajanju podpore, odobrene takim tretjim državam. Komisija bi morala upoštevati tudi vsa stališča ENISA v zvezi s takimi zahtevami in podporo. Komisija bi morala Svetu sporočiti izid ocene zahtev, vključno z ustreznimi premisleki v zvezi s tem, in o storitvah, ki se uporabljajo.

(54) V sporočilu Komisije z dne 18. aprila 2023 o akademiji za kibernetske veščine je priznano pomanjkanje usposobljenih strokovnjakov. Take veščine so potrebne za uresničevanje ciljev te uredbe. Unija nujno potrebuje strokovnjake z veščinami in kompetencami za preprečevanje in odkrivanje kibernetskih napadov in odvračanje od njih ter obrambo Unije pred takimi napadi, tudi njene najbolj kritične infrastrukture, in za zagotavljanje njene odpornosti. V ta namen je pomembno okrepiti sodelovanje med deležniki, vključno z zasebnim sektorjem, akademskimi krogi in javnim sektorjem. Prav tako je pomembno, da se na vseh ozemljih Unije ustvarijo sinergije za naložbe v izobraževanje in usposabljanje, da se spodbudi oblikovanje zaščitnih ukrepov za preprečevanje bega možganov ali večanja vrzeli v veščinah v nekaterih regijah bolj kot v drugih. Nujno je zapolniti vrzeli v veščinah, povezanih s kibernetsko varnostjo, s posebnim poudarkom na zmanjšanju vrzeli pri delovni sili na področju kibernetske varnosti, da bi spodbujali prisotnost in udeležbo žensk pri zasnovi digitalnega upravljanja.

(55) Povečanje raziskav in inovacij na področju kibernetske varnosti je pomembno za spodbujanje enotnega digitalnega trga, saj prispeva k povečanju odpornosti držav članic in odprte strateške avtonomije Unije, ki sta cilja te uredbe. Sinergije so bistvene za povečanje sodelovanja in usklajevanja med različnimi deležniki, vključno z zasebnim sektorjem, civilno družbo in akademskim svetom.

(56) Ta uredba bi morala upoštevati zavezo, določeno v Skupni deklaraciji z dne 26. januarja 2022 Evropskega parlamenta, Sveta in Komisije z naslovom „Evropska deklaracija o digitalnih pravicah in načelih za digitalno desetletje“, da bi zaščitili interese demokracij, ljudi, podjetij in javnih institucij Unije pred tveganji za kibernetsko varnost in kibernetsko kriminaliteto, vključno s kršitvami varstva podatkov in krajo identitete ali poseganjem vanjo.

(57) Da bi lahko dopolnili nekatere nebistvene elemente te uredbe, bi bilo treba na Komisijo prenesti pooblastilo, da v skladu s členom 290 PDEU sprejme akte v zvezi z določitvijo vrste in števila storitev za odzivanje, potrebnih za EU rezervo za kibernetsko varnost. Zlasti je pomembno, da se Komisija pri svojem pripravljalnem delu ustrezno posvetuje, vključno 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 ([20]). 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.

(58) Za zagotovitev enotnih pogojev za izvajanje te uredbe bi bilo treba na Komisijo prenesti izvedbena pooblastila za natančnejšo določitev podrobnih postopkovnih ureditev za dodeljevanje podpornih storitev iz EU rezerve za kibernetsko varnost. Ta pooblastila bi bilo treba izvajati v skladu z Uredbo (EU) št. 182/2011 Evropskega parlamenta in Sveta ([21]).

(59) Brez poseganja v pravila v zvezi z letnim proračunom Unije na podlagi Pogodb bi morala Komisija pri ocenjevanju proračunskih in kadrovskih potreb ENISA upoštevati obveznosti, ki izhajajo iz te uredbe.

(60) Komisija bi morala redno izvajati ocenjevanje ukrepov, določenih v tej uredbi. Prva taka ocena bi morala biti opravljena v prvih dveh letih po datumu začetka veljavnosti te uredbe in nato vsaj vsaka štiri leta, ob upoštevanju časovnega poteka revizije večletnega finančnega okvira, sprejetega na podlagi člena 312 PDEU. Komisija bi morala predložiti poročilo o doseženem napredku Evropskemu parlamentu in Svetu. Da bi Komisija ocenila različne potrebne elemente, vključno z obsegom informacij, ki se izmenjujejo v okviru evropskega sistema za opozarjanje na področju kibernetske varnosti, bi se morala opreti izključno na informacije, ki so takoj na voljo ali se zagotavljajo prostovoljno. Ob upoštevanju geopolitičnega razvoja dogodkov, pa tudi za zagotovitev, da se bodo ukrepi iz te uredbe izvajali in nadalje razvijali tudi po letu 2027, je pomembno, da Komisija oceni potrebo po dodelitvi ustreznih proračunskih sredstev v večletnem finančnem okviru od leta 2028 do leta 2034.

([20]) UL L 123, 12.5.2016, str. 1, ELI: http://data.europa.eu/eli/agree_interinstit/2016/512/oj.

([21]) 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: http://data.europa.eu/eli/reg/2011/182/oj).

(61) Ker ciljev te uredbe, in sicer krepiti konkurenčni položaj industrije in storitev v Uniji v celotnem digitalnem gospodarstvu ter prispevati k tehnološki suverenosti in odprti strateški avtonomiji Unije na področju kibernetske varnosti, države članice ne morejo zadovoljivo doseči, temveč se lažje dosežeta na ravni Unije, lahko Unija sprejme ukrepe v skladu z načeloma subsidiarnosti iz člena 5 PEU. V skladu z načelom sorazmernosti iz navedenega člena ta uredba ne presega tistega, kar je potrebno za doseganje navedenih ciljev –

SPREJELA NASLEDNJO UREDBO:

POGLAVJE I

SPLOŠNE DOLOČBE

Člen 1

Predmet urejanja in cilji

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

(a) vseevropske mreže kibernetskih vozlišč (evropski sistem za opozarjanje na področju kibernetske varnosti) za vzpostavitev in okrepitev usklajenih zmogljivosti za odkrivanje in skupnih zmogljivosti za situacijsko zavedanje;

(b) mehanizma za izredne razmere na področju kibernetske varnosti za podporo državam članicam pri pripravi na pomembne kibernetske incidente in kibernetske incidente velikih razsežnosti, odzivanju nanje, blaženju njihovega učinka in začetku obnovitve po njih ter za podporo drugim uporabnikom pri odzivanju na pomembne kibernetske incidente in kibernetske incidente, enakovredne incidentom velikih razsežnosti;

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

2. Splošni cilji te uredbe so okrepitev konkurenčnega položaja industrije in storitev v Uniji v celotnem digitalnem gospodarstvu, vključno z mikropodjetji ter malimi in srednjimi ter zagonskimi podjetji, ter prispevanje k tehnološki suverenosti in odprti strateški avtonomiji Unije na področju kibernetske varnosti, vključno s spodbujanjem inovacij na enotnem digitalnem trgu. Te cilje uresničuje s krepitvijo solidarnosti na ravni Unije, krepitvijo ekosistema kibernetske varnosti, krepitvijo kibernetske odpornosti držav članic ter razvojem veščin, strokovnega znanja, sposobnosti in kompetenc delovne sile v zvezi s kibernetsko varnostjo.

3. Splošni cilji iz odstavka 2 se dosegajo z uresničevanjem naslednjih specifičnih ciljev:

(a) okrepiti skupne usklajene zmogljivosti Unije za odkrivanje kibernetskih groženj in incidentov ter skupno situacijsko zavedanje o njih;

(b) okrepiti pripravljenost subjektov, ki delujejo v visoko kritičnih sektorjih ali subjektov, ki delujejo v drugih kritičnih sektorjih po vsej Uniji, ter solidarnost z razvijanjem usklajenega preskušanja pripravljenosti in okrepljenih zmogljivosti za odzivanje in obnovitev za obvladovanje pomembnih kibernetskih incidentov, kibernetskih incidentov velikih razsežnosti ali kibernetskih incidentov, enakovrednih incidentom velikih razsežnosti, med drugim z možnostjo omogočanja podpore Unije pri odzivanju na kibernetske incidente tretjim državam, pridruženim programu Digitalna Evropa;

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

4. Ukrepi na podlagi te uredbe se izvajajo ob ustreznem upoštevanju pristojnosti držav članic in dopolnjujejo dejavnosti, ki jih izvajajo mreža skupin CSIRT, mreža EU-CyCLONe in skupina za sodelovanje na področju varnosti omrežnih in informacijskih sistemov (v nadaljnjem besedilu: skupina za sodelovanje).

5. Ta uredba ne posega v temeljne državne funkcije držav članic, vključno z zagotavljanjem ozemeljske celovitosti države, vzdrževanjem javnega reda in miru ter varovanjem nacionalne varnosti. Zlasti nacionalna varnost ostaja v izključni pristojnosti vsake države članice.

6. Deljenje ali izmenjava informacij na podlagi te uredbe, ki so zaupne na podlagi pravil Unije ali nacionalnih pravil, je omejena na to, kar je relevantno za namen tega deljenja ali izmenjave in sorazmerno z njim. Pri takem deljenju ali izmenjavi informacij se ohrani zaupnost informacij ter zaščitijo varnost in poslovni interesi zadevnih subjektov. To ne vključuje zagotavljanja informacij, katerih razkritje bi bilo v nasprotju z bistvenimi interesi držav članic na področjih nacionalne varnosti, javne varnosti ali obrambe.

Člen 2

Opredelitev pojmov

V tej uredbi se uporabljajo naslednje opredelitve pojmov:

(1) „čezmejno kibernetsko vozlišče“ pomeni večdržavno platformo, vzpostavljeno s pisno konzorcijsko pogodbo, ki v usklajeni mrežni strukturi združuje nacionalna kibernetska vozlišča iz vsaj treh držav članic in je namenjena izboljšanju spremljanja, odkrivanja in analiziranja kibernetskih groženj za preprečevanje incidentov ter podpiranju priprave analitike kibernetskih groženj, zlasti z izmenjavanjem ustreznih, po potrebi anonimiziranih, podatkov in informacij, pa tudi z izmenjavanjem najsodobnejših orodij in skupnim razvijanjem zmogljivosti za kibernetsko odkrivanje, analizo ter preprečevanje in zaščito v zaupanja vrednem okolju;

(2) „gostiteljski konzorcij“ pomeni konzorcij sodelujočih držav članic, ki so se dogovorile, da bodo vzpostavile orodja, infrastrukturo ali storitve ter prispevale k njihovem pridobivanju za čezmejno kibernetsko vozlišče in njegovo delovanje;

(3) „skupina CSIRT“ pomeni skupino CSIRT, določeno ali vzpostavljeno na podlagi člena 10 Direktive (EU) 2022/2555;

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

(5) „subjekti, ki delujejo v visoko kritičnih sektorjih“ pomeni vrste subjekta, navedene v Prilogi I k Direktivi (EU) 2022/2555;

(6) „subjekti, ki delujejo v drugih kritičnih sektorjih“ pomeni vrste subjekta, navedene v Prilogi II k Direktivi (EU) 2022/2555;

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

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

(9) „incident“ pomeni incident, kakor je opredeljen v členu 6, točka 6, Direktive (EU) 2022/2555;

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

(11) „večji incident“ pomeni večji incident, kakor je opredeljen v členu 3, točka 8, Uredbe (EU, Euratom) 2023/2841 Evropskega parlamenta in Sveta ([22]);

(12) „kibernetski incident velikih razsežnosti“ pomeni kibernetski incident velikih razsežnosti, kakor je opredeljen v členu 6, točka 7, Direktive (EU) 2022/2555;

([22]) Uredba (EU, Euratom) 2023/2841 Evropskega parlamenta in Sveta z dne 13. decembra 2023 o določitvi ukrepov za visoko skupno raven kibernetske varnosti v institucijah, organih, uradih in agencijah Unije (UL L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj).

(13) „kibernetski incident, enakovreden incidentom velikih razsežnosti“ v primeru institucij, organov, uradov in agencij Unije pomeni večji incident, v primeru tretjih držav, ki so pridružene programu Digitalna Evropa, pa incident, ki povzroči motnje, ki presegajo zmogljivost zadevne tretje države, ki je pridružena programu Digitalna Evropa, da se nanj odzove;

(14) „tretja država, pridružena programu Digitalna Evropa“ pomeni tretjo državo, ki je pogodbenica sporazuma z Unijo, ki omogoča njeno sodelovanje v programu Digitalna Evropa na podlagi člena 10 Uredbe (EU) 2021/694;

(15) „javni naročnik“ pomeni Komisijo ali, kolikor je bilo delovanje in upravljanje EU rezerve za kibernetsko varnost zaupano ENISA na podlagi člena 14(5), ENISA;

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

(17) „zaupanja vredni ponudniki upravljanih varnostnih storitev“ pomeni ponudnike upravljanih varnostnih storitev, izbrane za vključitev v EU rezervo za kibernetsko varnost v skladu s členom 17.

POGLAVJE II

EVROPSKI SISTEM ZA OPOZARJANJE NA PODROČJU KIBERNETSKE VARNOSTI

Člen 3

Vzpostavitev evropskega sistema za opozarjanje na področju kibernetske varnosti

1. Vzpostavi se vseevropska mreža infrastrukture, ki jo sestavljajo nacionalna kibernetska vozlišča in čezmejna kibernetska vozlišča, ki se prostovoljno pridružijo, imenovana evropski sistem za opozarjanje na področju kibernetske varnosti, da se podpre razvoj naprednih zmogljivosti Unije za okrepitev zmogljivosti odkrivanja, analiziranja in obdelave podatkov v zvezi s kibernetskimi grožnjami in preprečevanjem incidentov v Uniji.

2. Evropski sistem za opozarjanje na področju kibernetske varnosti:

(a) prispeva k boljši zaščiti in odzivanju na kibernetske grožnje s podpiranjem in krepitvijo zmogljivosti ustreznih subjektov, zlasti skupin CSIRT, mreže skupin CSIRT, mreže EU-CyCLONe in pristojnih organov, imenovanih ali ustanovljenih na podlagi člena 8(1) Direktive (EU) 2022/2555, ter sodelovanjem s temi subjekti;

(b) združuje ustrezne podatke in informacije o kibernetskih grožnjah in incidentih iz različnih virov v čezmejnih kibernetskih vozliščih ter prek teh vozlišč deli analizirane ali zbirne informacije, kadar je to ustrezno, z mrežo skupin CSIRT;

(c) z uporabo najsodobnejših orodij in naprednih tehnologij zbira in podpira pripravo visokokakovostnih, uporabnih informacij in analitike kibernetskih groženj ter izmenjuje te informacije in analitiko kibernetskih groženj;

(d) prispeva k boljšemu usklajenemu odkrivanju kibernetskih groženj in skupnemu situacijskemu zavedanju o njih po vsej Uniji ter izdajanju opozoril, po potrebi tudi z zagotavljanjem konkretnih priporočil subjektom;

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

3. Ukrepi za izvajanje evropskega sistema za opozarjanje na področju kibernetske varnosti se podprejo s sredstvi iz programa Digitalna Evropa, izvajajo pa se v skladu z Uredbo (EU) 2021/694, zlasti specifičnim ciljem 3 navedene uredbe.

Člen 4

Nacionalna kibernetska vozlišča

1. Kadar se država članica odloči za sodelovanje v evropskem sistemu za opozarjanje na področju kibernetske varnosti, za namene te uredbe imenuje ali po potrebi vzpostavi nacionalno kibernetsko vozlišče.

2. Nacionalno kibernetsko vozlišče je en sam subjekt, ki deluje pod vodstvom države članice. To je lahko skupina CSIRT ali, kadar je ustrezno, nacionalni organ za obvladovanje kibernetskih kriz ali drug pristojni organ, imenovan ali ustanovljen na podlagi člena 8(1) Direktive (EU) 2022/2555, ali drug subjekt. Nacionalno kibernetsko vozlišče:

(a) mora biti sposobno delovati kot referenčna točka in točka dostopa do drugih javnih in zasebnih organizacij na nacionalni ravni za zbiranje in analiziranje informacij o kibernetskih grožnjah in incidentih ter prispevanje k čezmejnemu kibernetskemu vozlišču iz člena 5 ter

(b) mora biti sposobno odkrivati, združevati in analizirati podatke in informacije, pomembne za kibernetske grožnje in incidente, kot je analitika kibernetskih groženj, zlasti z uporabo najsodobnejših tehnologij, z namenom preprečevanja incidentov.

3. V okviru funkcij iz odstavka 2 tega člena lahko nacionalna kibernetska vozlišča sodelujejo s subjekti zasebnega sektorja pri izmenjavi ustreznih podatkov in informacij za namene odkrivanja in preprečevanja kibernetskih groženj in incidentov, tudi s sektorskimi in medsektorskimi skupnostmi bistvenih in pomembnih subjektov iz člena 3 Direktive (EU) 2022/2555. Kadar je ustrezno in v skladu s pravom Unije in nacionalnim pravom, lahko informacije, ki jih zahtevajo ali prejmejo nacionalna kibernetska vozlišča, vključujejo telemetrične in senzorske podatke ter podatke o beleženju.

4. Država članica, izbrana na podlagi člena 9(1), se zaveže, da bo zaprosila za sodelovanje svojega nacionalnega kibernetskega vozlišča v čezmejnem kibernetskem vozlišču.

Člen 5

Čezmejna kibernetska vozlišča

1. Kadar so vsaj tri države članice zavezane zagotavljanju, da njihova nacionalna kibernetska vozlišča sodelujejo pri usklajevanju dejavnosti odkrivanja in spremljanja kibernetskih groženj, lahko te države članice za namene te uredbe ustanovijo gostiteljski konzorcij.

2. Gostiteljski konzorcij je sestavljen iz vsaj treh sodelujočih držav članic, ki so se dogovorile, da bodo vzpostavile orodja, infrastrukturo ali storitve ter prispevale k njihovem pridobivanju za čezmejno kibernetsko vozlišče in njegovo delovanje v skladu z odstavkom 4.

3. Kadar je gostiteljski konzorcij izbran v skladu s členom 9(3), njegovi člani sklenejo pisno konzorcijsko pogodbo, v kateri:

(a) so določene notranje ureditve za izvajanje sporazuma o gostiteljstvu in uporabi iz člena 9(3);

(b) se vzpostavi čezmejno kibernetsko vozlišče gostiteljskega konzorcija ter

(c) so vključene posebne klavzule, zahtevane na podlagi člena 6(1) in (2).

4. Čezmejno kibernetsko vozlišče je večdržavna platforma, vzpostavljena s pisno konzorcijsko pogodbo iz odstavka 3. V usklajeni mrežni strukturi združuje nacionalna kibernetska vozlišča držav članic gostiteljskega konzorcija. Zasnovano je za izboljšanje spremljanja, odkrivanja in analiziranja kibernetskih groženj, preprečevanje incidentov ter podpiranje priprave analitike kibernetskih groženj, zlasti z izmenjavo ustreznih, po potrebi anonimiziranih, podatkov in informacij, pa tudi z izmenjavo najsodobnejših orodij in skupnim razvijanjem zmogljivosti za kibernetsko odkrivanje, analizo, preprečevanje in zaščito v zaupanja vrednem okolju.

5. Čezmejno kibernetsko vozlišče za pravne namene zastopa član zadevnega gostiteljskega konzorcija, ki deluje kot koordinator, ali gostiteljski konzorcij, če ima ta pravno osebnost. Odgovornost za skladnost čezmejnega kibernetskega vozlišča s to uredbo ter sporazumom o gostiteljstvu in uporabi se dodeli v pisni konzorcijski pogodbi iz odstavka 3.

6. Država članica se lahko pridruži obstoječemu gostiteljskemu konzorciju s soglasjem članov gostiteljskega konzorcija. Pisna konzorcijska pogodba iz odstavka 3 ter sporazum o gostiteljstvu in uporabi se ustrezno spremenita. To ne vpliva na lastninske pravice Evropskega industrijskega, tehnološkega in raziskovalnega kompetenčnega centra za kibernetsko varnost (ECCC) na orodjih, infrastrukturi ali storitvah, ki so že bili naročeni skupaj z navedenim gostiteljskim konzorcijem.

Člen 6

Sodelovanje in deljenje informacij v čezmejnih kibernetskih vozliščih in med njimi

1. Članice gostiteljskega konzorcija zagotovijo, da njihova nacionalna kibernetska vozlišča v skladu s pisno konzorcijsko pogodbo iz člena 5(3) medsebojno v okviru čezmejnega kibernetskega vozlišča delijo ustrezne, po potrebi anonimizirane, informacije, kot so informacije, 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 tako deljenje informacij:

(a) spodbuja in krepi odkrivanje kibernetskih groženj ter krepi zmogljivosti mreže skupin CSIRT za preprečevanje incidentov in odzivanje nanje ali ublažitev njihovih posledic;

(b) zvišuje raven kibernetske varnosti, na primer 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, fazami odzivanja in obnovitve 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 deljenju informacij iz odstavka 1 med članicami gostiteljskega konzorcija in pogoji, pod katerimi se te informacije delijo;

(b) okvir upravljanja, ki pojasnjuje in spodbuja deljenje ustreznih, po potrebi anonimiziranih, informacij iz odstavka 1 s strani vseh sodelujočih;

(c) cilji za prispevek k razvoju naprednih orodij in tehnologij, kot so orodja umetne inteligence in podatkovne analitike.

V pisni konzorcijski pogodbi se lahko določi, da se informacije iz odstavka 1 delijo v skladu s pravom Unije in nacionalnim pravom.

3. Čezmejna kibernetska vozlišča med seboj sklenejo sporazume o sodelovanju, v katerih določijo načela interoperabilnosti in deljenja informacij med čezmejnimi kibernetskimi vozlišči. Čezmejna kibernetska vozlišča Komisijo obvestijo o sklenjenih sporazumih o sodelovanju.

4. Deljenje informacij iz odstavka 1 med čezmejnimi kibernetskimi vozlišči se zagotovi z visoko ravnjo interoperabilnosti. V podporo tej interoperabilnosti ENISA v tesnem posvetovanju s Komisijo brez nepotrebnega odlašanja in v vsakem primeru do 5. februarja 2026 izda smernice za interoperabilnost, v katerih določi zlasti oblike in protokole za deljenje informacij, pri čemer upošteva mednarodne standarde in najboljše prakse ter delovanje vseh vzpostavljenih čezmejnih kibernetskih vozlišč. Zahteve glede interoperabilnosti iz sporazumov o sodelovanju čezmejnih kibernetskih vozlišč temeljijo na smernicah, ki jih izda ENISA.

Člen 7

Sodelovanje in deljenje informacij z mrežami na ravni Unije

1. Čezmejna kibernetska vozlišča in mreža skupin CSIRT tesno sodelujejo, zlasti z namenom deljenja informacij. V ta namen se dogovorijo o postopkovnih ureditvah o sodelovanju in deljenju ustreznih informacij ter, brez poseganja v odstavek 2, o vrstah informacij, ki se delijo.

2. Kadar čezmejna kibernetska vozlišča pridobijo informacije v zvezi z morebitnim ali tekočim kibernetskim incidentom velikih razsežnosti, za namene skupnega situacijskega zavedanja zagotovijo, da se organom držav članic in Komisiji prek mreže EU-CyCLONe in mreže skupin CSIRT brez nepotrebnega odlašanja zagotovijo ustrezne informacije in zgodnja opozorila.

Člen 8

Varnost

1. Države članice, ki sodelujejo v evropskem sistemu za opozarjanje na področju kibernetske varnosti, zagotovijo visoko raven kibernetske varnosti, vključno z zaupnostjo in varnostjo podatkov, pa tudi fizične varnosti evropskega sistema za opozarjanje na področju kibernetske varnosti ter ustrezno upravljanje in nadzor mreže, tako da je ta zaščitena pred grožnjami ter da sta zagotovljeni njena varnost in varnost sistemov, med drugim varnost podatkov in informacij, ki se delijo prek mreže.

2. Države članice, ki sodelujejo v evropskem sistemu za opozarjanje na področju kibernetske varnosti, zagotovijo, da deljenje informacij iz člena 6(1) v okviru evropskega sistema za opozarjanje na področju kibernetske varnosti s katerim koli subjektom, ki ni javni organ ali telo države članice, nima negativnih posledic za varnostne interese Unije ali držav članic.

Člen 9

Financiranje evropskega sistema za opozarjanje na področju kibernetske varnosti

1. ECCC na podlagi razpisov za prijavo interesa držav članic, ki nameravajo sodelovati v evropskem sistemu za opozarjanje na področju kibernetske varnosti, izbere države članice za sodelovanje z ECCC pri skupnem javnem naročanju orodij, infrastrukture ali storitev, da se vzpostavijo nacionalna kibernetska vozlišča, imenovana ali vzpostavljena na podlagi iz člena 4(1), ali okrepijo njihove zmogljivosti. ECCC lahko izbranim državam članicam dodeli nepovratna sredstva za financiranje delovanja takih orodij, infrastrukture ali storitev. Finančni prispevek Unije krije do 50 % stroškov pridobitve orodij, infrastrukture ali storitev ter do 50 % operativnih stroškov. Preostale stroške krijejo izbrane države članice. Pred začetkom postopka za pridobitev orodij, infrastrukture ali storitev ECCC in izbrane države članice sklenejo sporazum o gostiteljstvu in uporabi, ki ureja uporabo orodij, infrastrukture ali storitev.

2. Kadar nacionalno kibernetsko vozlišče države članice ne sodeluje v čezmejnem kibernetskem vozlišču v dveh letih od datuma pridobitve orodij, infrastrukture ali storitev ali datuma prejema nepovratnih sredstev, kateri koli nastopi prej, država članica ni upravičena do dodatne podpore Unije na podlagi tega poglavja, dokler se ne pridruži čezmejnemu kibernetskemu vozlišču.

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

4. ECCC vsaj vsaki dve leti pripravi pregled orodij, infrastrukture ali storitev, ki so potrebni in dovolj kakovostni za vzpostavitev ali krepitev zmogljivosti nacionalnih kibernetskih vozlišč in čezmejnih kibernetskih vozlišč, ter njihovo razpoložljivost, vključno s pravnimi subjekti, ki imajo sedež v državi članici ali se to zanje šteje, ter jih nadzirajo države članice ali državljani držav članic. ECCC se pri pripravi pregleda posvetuje z mrežo skupin CSIRT, vsemi obstoječimi čezmejnimi kibernetskimi vozlišči, ENISA in Komisijo.

POGLAVJE III

MEHANIZEM ZA IZREDNE RAZMERE NA PODROČJU KIBERNETSKE VARNOSTI

Člen 10

Vzpostavitev mehanizma za izredne razmere na področju kibernetske varnosti

1. Vzpostavi se mehanizem za izredne razmere na področju kibernetske varnosti za podporo povečanju odpornosti Unije proti kibernetskim grožnjam ter pripravo na kratkoročne posledice pomembnih kibernetskih incidentov, kibernetskih incidentov velikih razsežnosti ter kibernetskih incidentov, enakovrednih incidentom velikih razsežnosti, in njihovo ublažitev v duhu solidarnosti.

2. V primeru držav članic se ukrepi v okviru mehanizma za izredne razmere na področju kibernetske varnosti zagotovijo na zahtevo ter dopolnjujejo prizadevanja in ukrepe držav članic za pripravo na incidente, odzivanje nanje in obnovitev po njih.

3. Ukrepi za izvajanje mehanizma za izredne razmere na področju kibernetske varnosti se podprejo s financiranjem iz programa Digitalna Evropa, izvajajo pa se v skladu z Uredbo (EU) 2021/694, zlasti s specifičnim ciljem 3 navedene uredbe.

4. Ukrepi v okviru mehanizma za izredne razmere na področju kibernetske varnosti se izvajajo predvsem prek ECCC v skladu z Uredbo (EU) 2021/887. Ukrepe za izvajanje EU rezerve za kibernetsko varnost iz člena 11, točka (b), te uredbe pa bi morali izvajati Komisija in ENISA.

Člen 11

Vrste ukrepov

Mehanizem za izredne razmere na področju kibernetske varnosti podpira naslednje vrste ukrepov:

(a) ukrepe pripravljenosti, in sicer:

   (i) usklajeno preskušanje pripravljenosti subjektov, ki delujejo v visoko kritičnih sektorjih po vsej Uniji, kot je določeno v členu 12;

   (ii) druge ukrepe pripravljenosti za subjekte, ki delujejo v visoko kritičnih sektorjih ali subjekte, ki delujejo v drugih kritičnih sektorjih, kot je določeno v členu 13;

(b) ukrepe za podporo odzivu in začetek obnovitve po pomembnih kibernetskih incidentih, kibernetskih incidentih velikih razsežnosti in kibernetskih incidentih, enakovrednih incidentom velikih razsežnosti, pri čemer ukrepe zagotovijo zaupanja vredni ponudniki upravljanih varnostnih storitev, ki sodelujejo v EU rezervi za kibernetsko varnost, vzpostavljeni na podlagi člena 14;

(c) ukrepe, ki podpirajo medsebojno pomoč iz člena 18.

Člen 12

Usklajeno preskušanje pripravljenosti subjektov

1. Mehanizem za izredne razmere na področju kibernetske varnosti podpira prostovoljno usklajeno preskušanje pripravljenosti subjektov, ki delujejo v visoko kritičnih sektorjih.

2. Usklajeno preskušanje pripravljenosti lahko vključuje dejavnosti na področju pripravljenosti, kot je penetracijsko testiranje, in oceno groženj.

3. Podpora za ukrepe pripravljenosti iz tega člena se državam članicam zagotovi predvsem v obliki nepovratnih sredstev in pod pogoji iz ustreznih delovnih programov iz člena 24 Uredbe (EU) 2021/694.

4. Da bi Komisija podprla usklajeno preskušanje pripravljenosti subjektov iz člena 11, točka (a)(i), te uredbe po vsej Uniji, po posvetovanju s skupino za sodelovanje, mrežo EU-CyCLONe in ENISA med visoko kritičnimi sektorji, navedenimi

v Prilogi I k Direktivi (EU) 2022/2555, opredeli zadevne sektorje ali podsektorje, za katere se lahko objavi razpis za zbiranje predlogov za dodelitev nepovratnih sredstev. Države članice pri teh razpisih za zbiranje predlogov sodelujejo prostovoljno.

5. Komisija pri opredelitvi sektorjev ali podsektorjev iz odstavka 4 upošteva usklajene ocene tveganja in testiranje odpornosti na ravni Unije ter njihove rezultate.

6. Skupina za sodelovanje v sodelovanju s Komisijo, visokim predstavnikom Unije za zunanje zadeve in varnostno politiko (v nadaljnjem besedilu: visoki predstavnik) in ENISA ter v okviru svojega mandata z mrežo EU-CyCLONe razvije skupne scenarije tveganja in metodologije za usklajeno preskušanje pripravljenosti iz člena 11(1), točka (a)(i), in po potrebi za druge ukrepe pripravljenosti iz točke (a)(ii) navedenega člena.

7. Kadar subjekt, ki deluje v visoko kritičnem sektorju, prostovoljno sodeluje pri usklajenem preskušanju pripravljenosti in se na podlagi tega preskušanja priporočijo posebni ukrepi, ki bi jih sodelujoči subjekt lahko vključil v načrt popravnih ukrepov, organ države članice, pristojen za usklajeno preskušanje pripravljenosti, po potrebi pregleda nadaljnje ukrepanje sodelujočih subjektov v zvezi s temi ukrepi z namenom krepitve pripravljenosti.

Člen 13

Drugi ukrepi pripravljenosti

1. Mehanizem za izredne razmere na področju kibernetske varnosti podpira ukrepe pripravljenosti, ki niso zajeti v členu 12. Ti ukrepi vključujejo ukrepe pripravljenosti za subjekte v sektorjih, ki niso opredeljeni za usklajeno preskušanje pripravljenosti na podlagi člena 12. Ti ukrepi lahko podpirajo spremljanje ranljivosti, spremljanje tveganja, vaje in usposabljanje.

2. Podpora za ukrepe pripravljenosti iz tega člena se državam članicam zagotovi na zahtevo in predvsem v obliki nepovratnih sredstev ter pod pogoji, določenimi v ustreznih delovnih programih iz člena 24 Uredbe (EU) 2021/694.

Člen 14

Vzpostavitev EU rezerve za kibernetsko varnost

1. Vzpostavi se EU rezerva za kibernetsko varnost, da se uporabnikom iz odstavka 3 na zahtevo pomaga pri odzivanju ali zagotavljanju podpore pri odzivanju na pomembne kibernetske incidente, kibernetske incidente velikih razsežnosti ali kibernetske incidente, enakovredne incidentom velikih razsežnosti, ter pri začetku obnovitve po takih incidentih.

2. EU rezervo za kibernetsko varnost sestavljajo storitve za odzivanje, ki jih zagotovijo zaupanja vredni ponudniki upravljanih varnostnih storitev, izbrani v skladu z merili iz člena 17(2). EU rezerva za kibernetsko varnost lahko vključuje storitve, k zagotavljanju katerih se ponudniki zavežejo vnaprej. Storitve zaupanja vrednega ponudnika upravljanih varnostnih storitev, k zagotavljanju katerih se ponudniki zavežejo vnaprej, se lahko pretvorijo v storitve za pripravljenost, povezane s preprečevanjem incidentov in odzivanjem nanje, kadar se te storitve, h katerim se ponudniki zavežejo vnaprej, ne uporabljajo za odzivanje na incidente v času, h kateremu se ponudniki zavežejo vnaprej. EU rezerva za kibernetsko varnost se lahko na zahtevo uporablja v vseh državah članicah, v institucijah, organih, uradih in agencijah Unije ter v tretjih državah, pridruženih programu Digitalna Evropa, iz člena 19(1).

3. Uporabniki storitev iz EU rezerve za kibernetsko varnost vključujejo:

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

(b) CERT-EU v skladu s členom 13 Uredbe (EU, Euratom) 2023/2841;

(c) pristojne organe, kot so skupine za odzivanje na incidente na področju računalniške varnosti in organi za obvladovanje kibernetskih kriz v tretjih državah, pridruženih programu Digitalna Evropa, v skladu s členom 19(8).

4. Za izvajanje EU rezerve za kibernetsko varnost je v celoti odgovorna Komisija. Komisija določi prednostne naloge in razvoj EU rezerve za kibernetsko varnost v sodelovanju s skupino za sodelovanje 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. Te prednostne naloge se pregledajo in po potrebi revidirajo vsaki dve leti. Komisija Evropski parlament in Svet obvesti o teh prednostnih nalogah in vseh njihovih spremembah.

5. Brez poseganja v celotno odgovornost Komisije za izvajanje EU rezerve za kibernetsko varnost iz odstavka 4 tega člena in na podlagi sporazuma o prispevku, kakor je opredeljen v členu 2, točka 19, Uredbe (EU, Euratom) 2024/2509, Komisija delovanje in upravljanje EU rezerve za kibernetsko varnost v celoti ali delno zaupa ENISA. Vidiki, ki niso zaupani ENISA, ostanejo pod neposrednim upravljanjem Komisije.

6. ENISA vsaj vsaki dve leti pripravi pregled storitev, ki jih potrebujejo uporabniki iz odstavka 3, točki (a) in (b), tega člena. Pregled zajema tudi razpoložljivost takih storitev, tudi s strani pravnih subjektov, ki imajo sedež v državi članici ali se to zanje šteje, ter jih nadzirajo države članice ali državljani držav članic. ENISA pri pripravi pregleda te razpoložljivosti oceni veščine in zmogljivosti delovne sile Unije na področju kibernetske varnosti, ki so pomembne za cilje EU rezerve za kibernetsko varnost. ENISA se pri pripravi pregleda posvetuje s skupino za sodelovanje, mrežo EU-CyCLONe, Komisijo in po potrebi z Medinstitucionalnim odborom za kibernetsko varnost, ustanovljenim na podlagi člena 10 Uredbe (EU, Euratom) 2023/2841 (IICB). ENISA se pri pripravi pregleda razpoložljivosti storitev posvetuje tudi z ustreznimi deležniki iz industrije kibernetske varnosti, vključno s ponudniki upravljanih varnostnih storitev. ENISA pripravi podoben pregled, potem ko obvesti Svet ter potem ko se posvetuje z mrežo EU-CyCLONe, Komisijo in po potrebi z visokim predstavnikom, da se opredelijo potrebe uporabnikov iz odstavka 3, točka (c), tega člena.

7. Na Komisijo se prenese pooblastilo za sprejemanje delegiranih aktov v skladu s členom 23 za dopolnitev te uredbe z določitvijo vrst in števila storitev za odzivanje, potrebnih za EU rezervo za kibernetsko varnost. Komisija pri pripravi teh delegiranih aktov upošteva pripravo pregleda iz odstavka 6 tega člena ter si lahko izmenjuje nasvete in sodeluje s skupino za sodelovanje ter ENISA.

Člen 15

Zahtevki za podporo iz EU rezerve za kibernetsko varnost

1. Uporabniki iz člena 14(3) lahko zahtevajo storitve iz EU rezerve za kibernetsko varnost, da bi podprli odzivanje na pomembne kibernetske incidente, kibernetske incidente velikih razsežnosti ali kibernetske incidente, enakovredne incidentom velikih razsežnosti, in začeli obnovitev po njih.

2. Da bi uporabniki iz člena 14(3) prejeli podporo iz EU rezerve za kibernetsko varnost, sprejmejo vse ustrezne ukrepe za ublažitev učinkov incidenta, v zvezi s katerim zahtevajo podporo, med drugim po potrebi zagotovijo neposredno tehnično pomoč in druge vire za pomoč pri odzivanju na incident ter si prizadevajo za obnovitev.

3. Zahtevki za podporo se javnemu naročniku pošljejo:

(a) v primeru uporabnikov iz člena 14(3), točka (a), te uredbe prek enotne kontaktne točke, imenovane ali vzpostavljene na podlagi člena 8(3) Direktive (EU) 2022/2555;

(b) v primeru uporabnika iz člena 14(3), točka (b), s strani tega uporabnika;

(c) v primeru uporabnikov iz člena 14(3), točka (c), prek enotne kontaktne točke iz člena 19(9).

4. V primeru zahtevkov uporabnikov iz člena 14(3), točka (a), države članice o zahtevkih za podporo pri odzivanju na incidente in začetni obnovitvi na podlagi tega člena obvestijo mrežo skupin CSIRT in po potrebi mrežo EU-CyCLONe.

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

(a) ustrezne informacije o prizadetem subjektu in morebitnih posledicah incidenta za:

(i) v primeru uporabnikov iz člena 14(3), točka (a), prizadete države članice in uporabnike, vključno s tveganjem prelivanja na drugo državo članico;

(ii) v primeru uporabnika iz člena 14(3), točka (b), prizadete institucije, organe, urade ali agencije Unije;

(iii) v primeru uporabnikov iz člena 14(3), točka (c), prizadete države, pridružene programu Digitalna Evropa;

(b) informacije o zahtevani storitvi, skupaj z načrtovano uporabo zahtevane podpore in vključno z navedbo ocenjenih potreb;

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

(d) kadar je ustrezno, razpoložljive informacije o drugih oblikah podpore, ki so na voljo prizadetemu subjektu.

6. ENISA v sodelovanju s Komisijo in mrežo EU-CyCLONe pripravi predlogo za lažjo predložitev zahtevkov za podporo iz EU rezerve za kibernetsko varnost.

7. Komisija lahko z izvedbenimi akti natančneje določi podrobne postopkovne ureditve glede načina, kako se na podlagi tega člena, člena 16(1) in člena 19(10) zahtevajo podporne storitve iz EU rezerve za kibernetsko varnost in način, na katerega se odgovarja na te zahtevke, vključno z ureditvami za predložitev takih zahtevkov in predložitev odgovorov ter predloge za poročila iz člena 16(9). Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 24(2).

Člen 16

Izvajanje podpore iz EU rezerve za kibernetsko varnost

1. V primeru zahtevkov uporabnikov iz člena 14(3), točki (a) in (b), zahtevke za podporo iz EU rezerve za kibernetsko varnost oceni javni naročnik. Odgovor se pošlje uporabnikom iz člena 14(3), točki (a) in (b), brez odlašanja, v vsakem primeru pa najpozneje v 48 urah po vložitvi zahtevka, da se zagotovi učinkovitost podpore. Javni naročnik obvesti Svet in Komisijo o rezultatih postopka.

2. Kar zadeva informacije, ki se delijo med zahtevanjem storitev EU rezerve za kibernetsko varnost in njihovim zagotavljanjem, vse strani, ki sodelujejo pri uporabi te uredbe:

(a) omejijo uporabo in deljenje teh informacij na tisto, kar je potrebno, da se izpolnijo njihove obveznosti ali funkcije na podlagi te uredbe;

(b) vse informacije, ki so zaupne ali tajne na podlagi prava Unije in nacionalnega prava, uporabljajo in delijo samo v skladu z navedenim pravom ter

(c) zagotovijo uspešno, učinkovito in varno izmenjavo informacij, po potrebi z uporabo in upoštevanjem ustreznih protokolov za deljenje informacij, vključno s semaforskim protokolom.

3. Pri ocenjevanju posameznih zahtevkov na podlagi člena 16(1) in člena 19(10) javni naročnik ali Komisija, kot je ustrezno, najprej oceni, ali so izpolnjena merila iz člena 15(1) in (2). V tem primeru se oceni trajanje in naravo podpore, ki je primerna, ob upoštevanju cilja iz člena 1(3), točka (b), in po potrebi naslednjih meril:

(a) obseg in resnost incidenta;

(b) vrsta prizadetega subjekta, pri čemer imajo prednost incidenti, ki prizadenejo bistvene subjekte iz člena 3(1) Direktive (EU) 2022/2555;

(c) morebitne posledice incidenta za prizadete države članice, institucije, organe, urade ali agencije Unije ali tretje države, pridružene programu Digitalna Evropa;

(d) morebitna čezmejna narava incidenta in tveganje prelivanja na druge države članice, institucije, organe, urade ali agencije Unije ali tretje države, pridružene programu Digitalna Evropa;

(e) ukrepi, ki jih je uporabnik sprejel za pomoč pri prizadevanjih za odziv in začetno obnovitev, iz člena 15(2).

4. V primeru več hkratnih zahtevkov uporabnikov iz člena 14(3) se za njihovo prednostno razvrstitev po potrebi upoštevajo merila iz odstavka 3 tega člena, brez poseganja v načelo lojalnega sodelovanja med državami članicami ter institucijami, organi, uradi in agencijami Unije. Kadar sta dva ali je več zahtevkov ocenjenih kot enakih na podlagi teh meril, imajo prednost zahtevki uporabnikov iz držav članic. Kadar je bilo delovanje in upravljanje EU rezerve za kibernetsko varnost v celoti ali delno zaupano ENISA na podlagi člena 14(5), ENISA in Komisija tesno sodelujeta pri prednostni razvrstitvi zahtevkov v skladu s tem odstavkom.

5. Storitve EU rezerve za kibernetsko varnost se zagotovijo v skladu s posebnimi sporazumi med zaupanja vrednim ponudnikom upravljanih varnostnih storitev in uporabnikom, ki mu je zagotovljena podpora v okviru EU rezerve za kibernetsko varnost. Te storitve se lahko zagotovijo v skladu s posebnimi sporazumi med zaupanja vrednim ponudnikom upravljanih varnostnih storitev, uporabnikom in prizadetim subjektom. Vsi sporazumi iz tega odstavka med drugim vključujejo pogoje glede odgovornosti.

6. Sporazumi iz odstavka 5 temeljijo na predlogah, ki jih po posvetovanju z državami članicami in po potrebi z drugimi uporabniki EU rezerve za kibernetsko varnost pripravi ENISA.

7. Komisija, ENISA in uporabniki EU rezerve za kibernetsko varnost ne prevzamejo pogodbene odgovornosti za škodo, ki jo tretjim osebam povzročijo storitve, zagotovljene v okviru izvajanja EU rezerve za kibernetsko varnost.

8. Uporabniki lahko storitve EU rezerve za kibernetsko varnost, ki se zagotavljajo kot odgovor na zahtevek na podlagi člena 15(1), uporabljajo le za podporo odzivanju na pomembne kibernetske incidente, kibernetske incidente velikih razsežnosti ali kibernetske incidente, enakovredne incidentom velikih razsežnosti, ter začetek obnovitve po njih. Te storitve lahko uporabljajo v zvezi s:

(a) subjekti, ki delujejo v visoko kritičnih sektorjih, ali subjekti, ki delujejo v drugih kritičnih sektorjih, v primeru uporabnikov iz člena 14(3), točka (a), in enakovrednimi subjekti v primeru uporabnikov iz člena 14(3), točka (c), ter

(b) institucijami, organi, uradi in agencijami Unije v primeru uporabnikov iz člena 14(3), točka (b).

9. Uporabniki, ki so prejeli podporo, v dveh mesecih od konca podpore predložijo zbirno poročilo o zagotovljeni storitvi, doseženih rezultatih in pridobljenih spoznanjih:

(a) Komisiji, ENISA, mreži skupin CSIRT in mreži EU-CyCLONe v primeru uporabnikov iz člena 14(3), točka (a);

(b) Komisiji, ENISA in IICB predložijo zbirno poročilo v primeru uporabnika iz člena 14(3), točka (b);

(c) Komisiji v primeru uporabnikov iz člena 14(3), točka (c).

Komisija posreduje vsa zbirna poročila, ki jih prejme od uporabnikov iz člena 14(3) na podlagi prvega pododstavka, točka (c), tega odstavka, Svetu in visokemu predstavniku.

10. Kadar je bilo delovanje in upravljanje EU rezerve za kibernetsko varnost v celoti ali delno zaupano ENISA na podlagi člena 14(5) te uredbe, ENISA o tem redno poroča Komisiji in se z njo posvetuje. V zvezi s tem ENISA Komisiji nemudoma pošlje vse zahteve, ki jih prejme od uporabnikov iz člena 14(3), točka (c), te uredbe, in, kadar je to potrebno za namene prednostnega razvrščanja na podlagi tega člena, vse zahteve, ki jih je prejela od uporabnikov iz člena 14(3), točka (a) ali (b), te uredbe. Obveznosti iz tega odstavka ne posegajo v člen 14 Uredbe (EU) 2019/881.

11. V primeru uporabnikov iz člena 14(3), točki (a) in (b), javni naročnik skupini za sodelovanje redno in vsaj dvakrat letno poroča o uporabi podpore in njenih rezultatih.

12. V primeru uporabnikov iz člena 14(3), točka (c), Komisija poroča Svetu in obvešča visokega predstavnika redno in vsaj dvakrat letno o uporabi in rezultatih podpore.

Člen 17

Zaupanja vredni ponudniki upravljanih varnostnih storitev

1. Javni naročnik v postopkih javnega naročanja za namene vzpostavitve EU rezerve za kibernetsko varnost ravna v skladu z načeli iz Uredbe (EU, Euratom) 2024/2509 in naslednjimi načeli:

(a) zagotovi, da so, gledano v celoti, storitve, vključene v EU rezervo za kibernetsko varnost, takšne, da EU rezerva za kibernetsko varnost vključuje storitve, ki se lahko uvedejo v vseh državah članicah, ob upoštevanju zlasti nacionalnih zahtev za zagotavljanje takih storitev, vključno z jeziki, certificiranjem ali akreditacijo;

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

(c) zagotovi, da EU rezerva za kibernetsko varnost prinaša dodano vrednost Uniji s prispevanjem k ciljem iz člena 3 Uredbe (EU) 2021/694, med drugim s spodbujanjem razvoja kibernetskih veščin v Uniji.

2. Javni naročnik pri javnem naročanju storitev za EU rezervo za kibernetsko varnost v dokumente v zvezi z oddajo javnega naročila vključi naslednja merila in zahteve:

(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 in kontinuiteto strokovnega znanja in potrebne tehnične vire;

(b) ponudnik ter vsa zadevna odvisna podjetja in podizvajalci ravnajo v skladu z veljavnimi pravili o varovanju tajnih podatkov in imajo vzpostavljene ustrezne ukrepe, po potrebi vključno z medsebojnimi sporazumi, za varovanje zaupnih informacij v zvezi s storitvijo, zlasti dokazov, ugotovitev in poročil;

(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 dovoljenje, vsaj za osebje, namenjeno uvedbi storitev, kadar to zahteva država članica;

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

(f) ponudnik je opremljen s strojno in programsko opremo, potrebno za podporo zahtevani storitvi, ki ne vsebuje znanih ranljivosti, ki jih je mogoče izrabiti, vključuje najnovejše varnostne posodobitve in v vsakem primeru izpolnjuje vse veljavne določbe Uredbe (EU) 2024/2847 Evropskega parlamenta in Sveta ([23]);

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

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

(i) ponudnik lahko storitev zagotovi v enem ali več uradnih jezikih institucij Unije ali države članice, če tako zahtevajo države članice ali uporabniki iz člena 14(3), točki (b) in (c), v kateri ponudnik lahko opravi storitev;

(j) ko je vzpostavljena evropska certifikacijska shema za kibernetsko varnost za upravljane varnostne storitve na podlagi Uredbe (EU) 2019/881, se ponudnik certificira v skladu z navedeno shemo v dveh letih od datuma začetka uporabe sheme;

([23]) Uredba (EU) 2024/2847 Evropskega parlamenta in Sveta z dne 23. oktobra 2024 o horizontalnih zahtevah glede kibernetske varnosti za izdelke z digitalnimi elementi in spremembi uredb (EU) št. 168/2013 in (EU) 2019/1020 ter Direktive (EU) 2020/1828 (Akt o kibernetski odpornosti) (UL L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

(k) ponudnik v ponudbo vključi pogoje pretvorbe za vse neuporabljene storitve odzivanja na incidente, ki bi se lahko pretvorile v storitve za pripravljenost, tesno povezane z odzivanjem na incidente, kot so vaje ali usposabljanje.

3. Javni naročnik lahko za namene javnega naročanja storitev za EU rezervo za kibernetsko varnost v tesnem sodelovanju z državami članicami po potrebi pripravi merila in zahteve poleg tistih iz odstavka 2.

Člen 18

Ukrepi, ki podpirajo medsebojno pomoč

1. Mehanizem za izredne razmere na področju kibernetske varnosti zagotavlja podporo za tehnično pomoč ene države članice drugi državi članici, ki jo je prizadel pomemben kibernetski incident ali kibernetski incident velikih razsežnosti, med drugim v primerih iz člena 11(3), točka (f), Direktive (EU) 2022/2555.

2. Podpora za tehnično medsebojno pomoč iz odstavka 1 tega člena se zagotovi v obliki nepovratnih sredstev in pod pogoji, določenimi v ustreznih delovnih programih iz člena 24 Uredbe (EU) 2021/694.

Člen 19

Podpora tretjim državam, pridruženim programu Digitalna Evropa

1. Tretja država, pridružena programu Digitalna Evropa, lahko zaprosi za podporo iz EU rezerve za kibernetsko varnost, kadar je sodelovanje v EU rezervi za kibernetsko varnost določeno v sporazumu, na podlagi katerega se je pridružila programu Digitalna Evropa. Ta sporazum mora vključevati določbe, ki od zadevne tretje države, pridružene programu Digitalna Evropa, zahtevajo, da izpolnjuje obveznosti iz odstavkov 2 in 9 tega člena. Za namene sodelovanja tretje države v EU rezervi za kibernetsko varnost lahko delna pridružitev tretje države programu Digitalna Evropa vključuje pridružitev, omejeno na operativni cilj iz člena 6(1), točka (g), Uredbe (EU) 2021/694.

2. V treh mesecih od sklenitve sporazuma iz odstavka 1 in v vsakem primeru preden tretje države, pridružene programu Digitalna Evropa, prejmejo podporo iz EU rezerve za kibernetsko varnost, Komisiji 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 kibernetske incidente, kibernetske incidente velikih razsežnosti ali kibernetske incidente, enakovredne incidentom velikih razsežnosti, ter informacije o odgovornih nacionalnih subjektih, vključno s skupinami za odzivanje na incidente na področju računalniške varnosti ali enakovrednimi subjekti, njihovih zmogljivostih in virih, ki so jim dodeljeni. Tretja država, pridružena programu Digitalna Evropa, redno in vsaj enkrat letno posodablja te informacije. Komisija te informacije zagotovi visokemu predstavniku in ENISA, da bi olajšala uporabo odstavka 11.

3. Komisija redno in vsaj enkrat letno ocenjuje naslednja merila za vsako tretjo državo, pridruženo programu Digitalna Evropa, iz odstavka 1:

(a) ali ta država izpolnjuje pogoje sporazuma iz odstavka 1, kolikor se ti pogoji nanašajo na sodelovanje v EU rezervi za kibernetsko varnost;

(b) ali je ta država na podlagi informacij iz odstavka 2 sprejela ustrezne ukrepe za pripravo na pomembne kibernetske incidente ali kibernetske incidente, enakovredne incidentom velikih razsežnosti, ter

(c) ali je zagotavljanje podpore skladno s politiko Unije do te države in njenimi odnosi z njo na splošno ter z drugimi politikami Unije na področju varnosti.

Komisija se pri izvajanju ocene iz prvega pododstavka posvetuje z visokim predstavnikom v zvezi z merilom iz točke (c) navedenega pododstavka.

Kadar Komisija ugotovi, da tretja država, pridružena programu Digitalna Evropa, izpolnjuje vse pogoje iz prvega pododstavka, Svetu predloži predlog za sprejetje izvedbenega akta v skladu z odstavkom 4, s katerim se odobri zagotavljanje podpore iz EU rezerve za kibernetsko varnost tej državi.

4. Svet lahko sprejme izvedbene akte iz odstavka 3. Ti izvedbeni akti veljajo največ eno leto. Njihova veljavnost se lahko podaljša. Vključujejo lahko omejitev števila dni na najmanj 75 dni, za katere se lahko zagotovi podpora na podlagi enega samega zahtevka.

Za namene tega člena Svet ukrepa hitro in izvedbene akte iz tega odstavka praviloma sprejme v osmih tednih po sprejetju zadevnega predloga Komisije na podlagi odstavka 3, tretji pododstavek.

5. Svet lahko na predlog Komisije kadar koli spremeni ali razveljavi izvedbeni akt, sprejet na podlagi odstavka 4.

Kadar Svet meni, da je prišlo do bistvene spremembe merila iz odstavka 3, prvi pododstavek, točka (c), lahko na ustrezno utemeljeno pobudo ene ali več držav članic spremeni ali razveljavi izvedbeni akt, sprejet na podlagi odstavka 4.

6. Svet pri izvajanju svojih izvedbenih pooblastil na podlagi tega člena uporablja merila iz odstavka 3, prvi pododstavek, in pojasni svojo oceno teh meril. Zlasti kadar ukrepa na lastno pobudo na podlagi odstavka 5, drugi pododstavek, Svet pojasni pomembne spremembe iz navedenega pododstavka.

7. Podpora iz EU rezerve za kibernetsko varnost tretji državi, pridruženi programu Digitalna Evropa, izpolnjuje vse posebne pogoje, določene v sporazumu iz odstavka 1.

8. Uporabniki iz tretjih držav, pridruženih programu Digitalna Evropa, ki so upravičeni do storitev iz EU rezerve za kibernetsko varnost, vključujejo pristojne organe, kot so skupine za odzivanje na incidente na področju računalniške varnosti ali enakovredni subjekti in organi za obvladovanje kibernetskih kriz.

9. Vsaka tretja država, pridružena programu Digitalna Evropa, ki je upravičena do podpore iz EU rezerve za kibernetsko varnost, imenuje organ, ki deluje kot enotna kontaktna točka za namene te uredbe.

10. Zahtevke za podporo iz EU rezerve za kibernetsko varnost na podlagi tega člena oceni Komisija. Javni naročnik lahko zagotovi podporo tretji državi le, kadar in dokler velja izvedbeni akt Sveta, ki dovoljuje tako podporo v zvezi s to državo, sprejet na podlagi odstavka 4 tega člena. Odgovor se brez nepotrebnega odlašanja pošlje uporabnikom iz člena 14(3), točka (c).

11. Po prejemu zahtevka za podporo na podlagi tega člena Komisija o tem nemudoma obvesti Svet. Komisija Svet obvešča o oceni zahtevka. Komisija sodeluje tudi z visokim predstavnikom glede prejetih zahtevkov in izvajanja podpore, dodeljene tretjim državam, pridruženim programu Digitalna Evropa, iz EU rezerve za kibernetsko varnost. Poleg tega Komisija upošteva tudi vsa stališča ENISA v zvezi z istimi zahtevki.

Člen 20

Usklajevanje z mehanizmi Unije za krizno upravljanje

1. Kadar je pomemben kibernetski incident, kibernetski incident velikih razsežnosti ali kibernetski incident, enakovreden incidentu velikih razsežnosti, posledica nesreče ali povzroči nesrečo, kakor je opredeljena v členu 4, točka 1, Sklepa št. 1313/2013/EU, podpora, zagotovljena na podlagi te uredbe za odzivanje na tak incident, dopolnjuje ukrepe iz navedenega sklepa in ne posega vanj.

2. V primeru kibernetskega incidenta velikih razsežnosti ali kibernetskega incidenta, enakovrednega incidentu velikih razsežnosti, pri katerem se uporabi enotna ureditev EU za politično odzivanje na krize na podlagi Izvedbenega sklepa (EU) 2018/1993 (ureditve IPCR), se podpora, zagotovljena na podlagi te uredbe za odzivanje na tak incident, obravnava v skladu z ustreznimi postopki v okviru ureditve IPCR.

POGLAVJE IV

EVROPSKI MEHANIZEM ZA PREGLEDOVANJE KIBERNETSKIH INCIDENTOV

Člen 21

Evropski mehanizem za pregledovanje kibernetskih incidentov

1. ENISA na zahtevo Komisije ali mreže EU-CyCLONe ter s podporo mreže skupin CSIRT in odobritvijo zadevnih držav članic pregleda in oceni kibernetske grožnje, znane ranljivosti, ki jih je mogoče izrabiti, in blažitvene ukrepe v zvezi s posameznim pomembnim kibernetskim incidentom ali kibernetskim incidentom velikih razsežnosti. ENISA po zaključku pregleda in ocene incidenta in z namenom predstavitve pridobljenih spoznanj za preprečevanje ali ublažitev prihodnjih incidentov mreži EU-CyCLONe, mreži skupin CSIRT, zadevnim državam članicam 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. Kadar incident vpliva na tretjo državo, pridruženo programu Digitalna Evropa, ENISA poročilo zagotovi Svetu. V takih primerih Komisija poročilo po potrebi zagotovi visokemu predstavniku.

2. ENISA pri pripravi poročila o pregledu incidenta iz odstavka 1 tega člena sodeluje z vsemi ustreznimi deležniki in od njih zbira povratne informacije, vključno s predstavniki držav članic, Komisijo, drugimi ustreznimi institucijami, organi, uradi in agencijami Unije, industrijo, med drugim ponudniki upravljanih varnostnih storitev in uporabniki kibernetskih storitev. ENISA po potrebi v sodelovanju s skupinami CSIRT in, kadar je to ustrezno, pristojnimi organi, imenovanimi ali ustanovljenimi na podlagi člena 8(1) Direktive (EU) 2022/2555, sodeluje tudi s subjekti, ki so jih prizadeli pomembni kibernetski incidenti ali kibernetski incidenti velikih razsežnosti. Predstavniki, s katerimi se opravi posvetovanje, razkrijejo vsako morebitno nasprotje interesov.

3. Poročilo o pregledu incidenta iz odstavka 1 tega člena zajema pregled in analizo posameznega pomembnega kibernetskega incidenta ali kibernetskega incidenta velikih razsežnosti, vključno z glavnimi vzroki, znanimi ranljivostmi, ki jih je mogoče izrabiti, in pridobljenimi spoznanji. ENISA zagotovi, da je poročilo v skladu s pravom Unije ali nacionalnim pravom v zvezi z varstvom občutljivih ali tajnih podatkov. Na zahtevo zadevnih držav članic ali drugih uporabnikov iz člena 14(3), ki jih je incident prizadel, so podatki in informacije v poročilu anonimizirani. Ne zajema pa podrobnosti o aktivno izrabljenih ranljivostih, ki so še neodpravljene.

4. Poročilo o pregledu incidenta po potrebi vsebuje priporočila za izboljšanje kibernetske drže Unije in vključuje primere najboljših praks ter pridobljena spoznanja zadevnih deležnikov.

5. ENISA lahko izda javno dostopno različico poročila o pregledu incidenta. Ta različica poročila vsebuje le zanesljive javne informacije, ali druge zanesljive informacije s soglasjem zadevnih držav članic, in kar zadeva informacije, ki se nanašajo na uporabnika iz člena 14(3), točka (b) ali (c), s privolitvijo tega uporabnika.

POGLAVJE V

KONČNE DOLOČBE

Člen 22

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) podpora razvoju evropskega sistema za opozarjanje na področju kibernetske varnosti, vzpostavljenega na podlagi člena 3 Uredbe (EU) 2025/38 Evropskega parlamenta in Sveta (*)(v nadaljnjem besedilu: evropski sistem za opozarjanje na področju kibernetske varnosti), vključno z razvojem, uvedbo in delovanjem nacionalnih kibernetskih vozlišč in čezmejnih kibernetskih vozlišč, ki prispevajo k situacijskemu zavedanju v Uniji in krepitvi zmogljivosti Unije za pridobivanje analitike kibernetskih groženj;

(*) Uredba (EU) 2025/38 Evropskega parlamenta in Sveta z dne 19. decembra 2024 o določitvi ukrepov za okrepitev solidarnosti in zmogljivosti v Uniji za odkrivanje kibernetskih groženj in incidentov ter pripravo in odzivanje nanje ter spremembi Uredbe (EU) 2021/694 (Akt o kibernetski solidarnosti) (UL L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).“;

(ii) doda se naslednja točka:

„(g) vzpostavitev in upravljanje mehanizma za izredne razmere na področju kibernetske varnosti, vzpostavljenega na podlagi člena 10 Uredbe (EU) 2025/38, vključno z EU rezervo za kibernetsko varnost, vzpostavljeno s členom 14 navedene uredbe (v nadaljnjem besedilu: EU rezerva za kibernetsko varnost), za podporo državam članicam pri pripravi na pomembne kibernetske incidente in kibernetske incidente velikih razsežnosti ter odzivanju nanje, pri čemer mehanizem dopolnjuje nacionalne vire in zmogljivosti ter druge oblike podpore, ki so na voljo na ravni Unije, ter za podporo drugih uporabnikov pri odzivanju na pomembne kibernetske incidente in kibernetske incidente, enakovredne incidentom velikih razsežnosti.“;

(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 (*). EU rezervo za kibernetsko varnost pa izvaja Komisija in v skladu s členom 14(6) Uredbe (EU) 2025/38 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).“;

(2) člen 9 se spremeni:

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

„(b) 1 760 806 000 EUR za specifični cilj 2 – umetna inteligenca;

(c) 1 372 020 000 EUR za specifični cilj 3 – kibernetska varnost in zaupanje;

(d) 482 640 000 EUR za specifični cilj 4 – napredne digitalne veščine;“;

(b) doda se naslednji odstavek:

„8. Z odstopanjem od člena 12(1) finančne uredbe se neporabljene odobritve za prevzem obveznosti in odobritve plačil za ukrepe v okviru izvajanja EU rezerve za kibernetsko varnost in ukrepe, ki podpirajo medsebojno pomoč na podlagi Uredbe (EU) 2025/38, 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. Evropski parlament in Svet se obvestita o odobritvah, prenesenih na podlagi člena 12(6) finančne uredbe.“;

(3) člen 12 se spremeni:

(a) vstavita se naslednja odstavka:

„5a. Odstavek 5 se v zvezi s pravnimi subjekti, ki so ustanovljeni v Uniji, nadzirani pa so iz tretjih držav, ne uporablja za kateri koli ukrep za izvajanje evropskega sistema za opozarjanje na področju kibernetske varnosti, kadar sta v zvezi z zadevnim ukrepom izpolnjena oba naslednja pogoja:

(a) obstaja dejansko tveganje ob upoštevanju rezultatov pregleda, izvedenega na podlagi člena 9(4) Uredbe (EU) 2025/38, da orodja, infrastruktura ali storitve, ki so potrebni in zadostni, da bi navedeni ukrep ustrezno prispeval k cilju evropskega sistema za opozarjanje na področju kibernetske varnosti, ne bodo na voljo od pravnih subjektov, ki so ustanovljeni ali za katere se šteje, da so ustanovljeni v državah članicah ter jih nadzirajo države članice ali državljani držav članic;

(b) je varnostno tveganje javnega naročanja od takih pravnih subjektov v okviru evropskega sistema za opozarjanje na področju kibernetske varnosti sorazmerno s koristmi in ne ogroža bistvenih varnostnih interesov Unije in njenih držav članic.

5b. Odstavek 5 se v zvezi s pravnimi subjekti, ki so ustanovljeni v Uniji, nadzirani pa so iz tretjih držav, ne uporablja za kateri koli ukrep za izvajanje EU rezerve za kibernetsko varnost, kadar sta v zvezi z zadevnim ukrepom izpolnjena oba naslednja pogoja:

(a) obstaja dejansko tveganje ob upoštevanju rezultatov pregleda, izvedenega na podlagi člena 14(6) Uredbe (EU) 2025/38, da tehnologija, strokovno znanje ali zmogljivost, ki je potrebna in zadostna za ustrezno opravljanje funkcij EU rezerve za kibernetsko varnost, ne bo na voljo od pravnih subjektov, ki so ustanovljeni ali za katere se šteje, da so ustanovljeni v državah članicah ter jih nadzirajo države članice ali državljani držav članic;

(b) je varnostno tveganje vključitve takih pravnih subjektov v EU rezervo za kibernetsko varnost sorazmerno s koristmi in ne ogroža bistvenih varnostnih interesov Unije in njenih držav članic.“;

(b) odstavek 6 se nadomesti z naslednjim:

„6. Če je to ustrezno utemeljeno iz varnostnih razlogov, je v programu dela lahko določeno, da so pravni subjekti, ustanovljeni v pridruženih državah, in pravni subjekti, ustanovljeni v Uniji, ki pa so nadzirani iz tretjih držav, lahko upravičeni do sodelovanja pri vseh ali nekaterih ukrepih v okviru specifičnih ciljev 1 in 2 le, če izpolnjujejo zahteve, ki jih morajo navedeni pravni subjekti izpolnjevati za jamstvo varstva bistvenih varnostnih interesov Unije in držav članic, ter za zagotavljanje varstva informacij v tajnih dokumentih. Te zahteve se določijo v programu dela.

Prvi pododstavek se v zvezi s pravnimi subjekti, ustanovljeni v Uniji, ki pa so nadzirani iz tretjih držav, uporablja tudi za ukrepe v okviru specifičnega cilja 3:

(a) izvajanje evropskega sistema za opozarjanje na področju kibernetske varnosti, kadar se uporablja odstavek 5a, in

(b) izvajanje EU rezerve za kibernetsko varnost, kadar se uporablja odstavek 5b.“;

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

„2. Program lahko zagotovi financiranje v kateri koli obliki, določeni v finančni uredbi, 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, kakor so opredeljeni v direktivah 2014/24/EU (*) in 2014/25/EU (**) Evropskega parlamenta in Sveta.

Kadar je za doseganje ciljev ukrepa treba 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 ENISA lahko pri izvajanju postopkov javnega naročanja za EU rezervo za kibernetsko varnost delujeta kot osrednji nabavni organ za javno naročanje v imenu ali za račun tretjih držav, pridruženih Programu v skladu s členom 10 te uredbe. Komisija in ENISA delujeta lahko tudi kot trgovec na debelo, tako da kupujeta, skladiščita in

nadalje prodajata ali darujeta blago in storitve, vključno z najemi, navedenim tretjim državam. Z odstopanjem od člena 168(3) Uredbe (EU, Euratom) 2024/2509 Evropskega parlamenta in Sveta (***) za pooblastitev Komisije ali ENISA za ukrepanje zadostuje zahtevek ene same tretje države.

Komisija in ENISA lahko pri izvajanju postopkov javnega naročanja za EU rezervo za kibernetsko varnost delujeta kot osrednji nabavni organ za javno naročanje v imenu ali za račun institucij, organov, uradov ali agencij Unije. Komisija in ENISA delujeta lahko tudi kot trgovec na debelo, tako da kupujeta, skladiščita in nadalje prodajata ali darujeta blago in storitve, vključno z najemi, institucijam, organom, uradom ali agencijam Unije. Z odstopanjem od člena 168(3) Uredbe (EU, Euratom) 2024/2509 za pooblastitev Komisije ali ENISA za ukrepanje zadostuje zahtevek ene same institucije, organa, urada ali agencije Unije.

Program lahko zagotovi tudi financiranje v obliki finančnih instrumentov v okviru operacij mešanega financiranja.

(*) 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).
(**) Direktiva 2014/25/EU Evropskega parlamenta in Sveta z dne 26. februarja 2014 o javnem naročanju naročnikov, ki opravljajo dejavnosti v vodnem, energetskem in prometnem sektorju ter sektorju poštnih storitev ter o razveljavitvi Direktive 2004/17/ES (UL L 94, 28.3.2014, str. 243).
(***) Uredba (EU, Euratom) 2024/2509 Evropskega parlamenta in Sveta z dne 23. septembra 2024 o finančnih pravilih, ki se uporabljajo za splošni proračun Unije (UL L, 2024/2509, 26.9.2024, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).“;

(5) vstavi se naslednji člen:

„*Člen 16a*

Neskladja pravil

V primeru ukrepov za izvajanje evropskega sistema za opozarjanje na področju kibernetske varnosti se uporabljajo pravila iz členov 4, 5 in 9 Uredbe 2025/38. V primeru neskladja med določbami te uredbe ter členi 4, 5 in 9 Uredbe (EU) 2025/38 imajo prednost navedeni členi, ki se uporabljajo za te specifične ukrepe.“;

V primeru EU rezerve za kibernetsko varnost se posebna pravila za sodelovanje tretjih držav, pridruženih programu, določijo v členu 19 Uredbe (EU) 2025/38. V primeru neskladja med določbami te uredbe in členom 19 Uredbe (EU) 2025/38 ima prednost navedeni člen, ki se uporablja za te specifične ukrepe.“;

(6) člen 19 se nadomesti z naslednjim:

„*Člen 19*

Nepovratna sredstva

Nepovratna sredstva v okviru Programa se dodeljujejo in upravljajo v skladu z naslovom VIII finančne uredbe ter lahko krijejo do 100 % upravičenih stroškov brez poseganja v načelo sofinanciranja, kot je določeno v členu 190 finančne uredbe. Taka nepovratna sredstva se dodeljujejo in upravljajo, kot je določeno za vsak specifičen cilj.

Podporo v obliki nepovratnih sredstev lahko ECCC dodeli neposredno, brez razpisa za zbiranje predlogov, državam članicam, izbranim na podlagi člena 9 Uredbe (EU) 2025/38, in gostiteljskemu konzorciju iz člena 5 Uredbe (EU) 2025/38 v skladu s členom 195(1), točka (d), finančne uredbe.

Podporo v obliki nepovratnih sredstev za mehanizem za izredne razmere na področju kibernetske varnosti lahko ECCC dodeli neposredno, brez razpisa za zbiranje predlogov, državam članicam v skladu s členom 195(1), točka (d), finančne uredbe.

Kar zadeva ukrepe, ki podpirajo medsebojno pomoč, iz člena 18 Uredbe (EU) 2025/38, ECCC Komisijo in ENISA obvesti o zahtevkih držav članic za neposredna nepovratna sredstva, ki se dodelijo brez razpisa za zbiranje predlogov.

Kar zadeva ukrepe, ki podpirajo medsebojno pomoč, iz člena 18 Uredbe (EU) 2025/38 in v skladu s členom 193(2), drugi pododstavek, točka (a), finančne uredbe, se lahko v ustrezno utemeljenih primerih stroški štejejo za upravičene, tudi če so nastali pred vložitvijo zahtevka za nepovratna sredstva.“;

(7) prilogi I in II se spremenita v skladu s Prilogo k tej uredbi.

Člen 23

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 člena 14(7) se prenese na Komisijo za obdobje petih let od 5. februarja 2025. Komisija pripravi poročilo o prenosu pooblastila najpozneje devet mesecev pred koncem petletnega 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 člena 14(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 14(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 24

Postopek v odboru

1. Komisiji pomaga odbor za usklajevanje programa Digitalna Evropa iz člena 31(1) Uredbe (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 25

Ocena in pregled

1. Komisija do 5. februarja 2027, nato pa najmanj vsaka štiri leta oceni delovanje ukrepov iz te uredbe ter Evropskemu parlamentu in Svetu predloži poročilo.

2. V oceni iz odstavka 1 se oceni zlasti:

(a) število vzpostavljenih nacionalnih kibernetskih vozlišč in čezmejnih kibernetskih vozlišč, obseg deljenih informacij, po možnosti vključno z vplivom na delo mreže skupin CSIRT, ter obseg, v katerem so te prispevale h krepitvi skupnega odkrivanja kibernetskih groženj in incidentov v Uniji ter situacijskemu zavedanju o njih ter razvoju najsodobnejših tehnologij; uporaba financiranja programa Digitalna Evropa za skupno nabavljena orodja za kibernetsko varnost,

infrastrukturo ali storitve, ter, če so te informacije na voljo, raven sodelovanja med nacionalnimi kibernetskimi vozlišči ter sektorskimi in medsektorskimi skupnostmi bistvenih in pomembnih subjektov iz člena 3 Direktive (EU) 2022/2555;

(b) uporaba in učinkovitost ukrepov v okviru mehanizma za izredne razmere na področju kibernetske varnosti za podporo pripravljenosti, vključno z usposabljanjem in odzivanjem na pomembne kibernetske incidente, kibernetske incidente velikih razsežnosti in kibernetske incidente, enakovredne incidentom velikih razsežnosti, ter začetno obnovitvijo po njih, vključno z uporabo financiranja programa Digitalna Evropa ter pridobljenimi spoznanji in priporočili pri izvajanju mehanizma za izredne razmere na področju kibernetske varnosti;

(c) uporaba in učinkovitost EU rezerve za kibernetsko varnost glede na vrste uporabnikov, vključno z uporabo sredstev programa Digitalna Evropa, uporaba storitev, vključno z vrsto storitev, povprečni odzivni čas na zahteve in za uporabo EU rezerve za kibernetsko varnost, delež storitev, pretvorjenih v storitve za pripravljenost v zvezi s preprečevanjem incidentov in odzivanjem nanje ter pridobljena spoznanja in priporočila pri izvajanju EU rezerve za kibernetsko varnost;

(d) prispevek te uredbe h krepitvi konkurenčnega položaja industrije in storitev v Uniji v celotnem digitalnem gospodarstvu, vključno z mikropodjetji, malimi in srednjimi podjetji ter zagonskimi podjetji, ter prispevek k splošnemu cilju krepitve znanja in veščin delovne sile na področju kibernetske varnosti.

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

Člen 26

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 Bruslju, 19. decembra 2024

Za Evropski parlament	*Za Svet*
predsednica	*predsednik*
R. METSOLA	BÓKA J.

PRILOGA

Uredba (EU) 2021/694 se spremeni:

(1) v Prilogi I se oddelek „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, infrastrukturo ter tehnične izkušnje, ki so ključnega pomena za zaščito kritičnih infrastruktur in enotnega digitalnega 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 kibernetskimi vozlišči in čezmejnimi kibernetskimi vozlišči, ki sestavljajo evropski sistem za opozarjanje na področju kibernetske varnosti, 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, ob upoštevanju uravnotežene zastopanosti spolov, na primer z usklajevanjem programov za razvoj takih veščin, njihovo prilagajanje specifičnim sektorskim potrebam in olajšanje dostopa do specializiranih, ciljno usmerjenih usposabljanj.
5. Spodbujanje solidarnosti med državami članicami pri pripravi na pomembne kibernetske incidente in kibernetske incidente velikih razsežnosti ter 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 „Specifični cilj 3 – Kibernetska varnost in zaupanje“ nadomesti z naslednjim:

„Specifični cilj 3 – Kibernetska varnost in zaupanje

3.1. Število skupno naročenih infrastruktur ali orodij za kibernetsko varnost ali obojega, tudi v okviru evropskega sistema za opozarjanje na področju kibernetske varnosti

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

3.3. Število ukrepov za podporo pripravljenosti in odzivanju na kibernetske incidente v okviru mehanizma za izredne razmere na področju kibernetske varnosti“.

V zvezi s tem aktom je bila podana izjava, ki je na voljo v UL C, C/2025/308, 15.1.2025, ELI: http://data.europa.eu/eli/C/2025/308/oj.