Evropski parlament
2019-2024

Dokument zasedanja

A9-0426/2023

8.12.2023

***I
POROČILO

o predlogu uredbe Evropskega parlamenta in Sveta o določitvi ukrepov za okrepitev solidarnosti in zmogljivosti v Uniji za odkrivanje kibernetskovarnostnih groženj in incidentov ter pripravo in odzivanje nanje
(COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

Odbor za industrijo, raziskave in energijo

Poročevalka: Lina Gálvez Muñoz

Oznake postopkov

*	Postopek posvetovanja
***	Postopek odobritve
***I	Redni zakonodajni postopek (prva obravnava)
***II	Redni zakonodajni postopek (druga obravnava)
***III	Redni zakonodajni postopek (tretja obravnava)

(Vrsta postopka je odvisna od pravne podlage, ki je predlagana v osnutku akta.)

Predlogi sprememb k osnutku akta

Spremembe, ki jih predlaga Parlament, v dveh stolpcih

Izbrisano besedilo je označeno s ***krepkim poševnim tiskom*** v levem stolpcu, zamenjano besedilo s ***krepkim poševnim tiskom*** v obeh stolpcih, novo besedilo pa s ***krepkim poševnim tiskom*** v desnem stolpcu.

Prva in druga vrstica glave vsakega predloga spremembe navajata zadevni del besedila v obravnavanem osnutku akta. Če predlog spremembe zadeva obstoječi akt, ki se ga želi spremeniti z osnutkom akta, glava poleg tega vsebuje še tretjo in četrto vrstico, ki navajata obstoječi akt oziroma zadevno določbo tega akta.

Spremembe, ki jih predlaga Parlament, v obliki konsolidiranega besedila

Novo besedilo je označeno s ***krepkim poševnim tiskom***. Izbrisano besedilo je označeno s simbolom ▌ ali prečrtano. Zamenjano besedilo je izbrisano ali prečrtano, besedilo, ki ga nadomešča, pa je označeno s ***krepkim poševnim tiskom***.
Izjema so spremembe izključno tehnične narave, ki so jih vnesle službe z namenom priprave končnega besedila in niso označene.

VSEBINA

Stran

OSNUTEK ZAKONODAJNE RESOLUCIJE EVROPSKEGA PARLAMENTA

o predlogu uredbe Evropskega parlamenta in Sveta o določitvi ukrepov za okrepitev solidarnosti in zmogljivosti v Uniji za odkrivanje kibernetskovarnostnih groženj in incidentov ter pripravo in odzivanje nanje
(COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

(Redni zakonodajni postopek: prva obravnava)

Evropski parlament,

– ob upoštevanju predloga Komisije Evropskemu parlamentu in Svetu (COM(2023)0209),

– ob upoštevanju člena 294(2), člena 173(3) in člena 322(1), točka (a), Pogodbe o delovanju Evropske unije, na podlagi katerih je Komisija podala predlog Parlamentu (C9-0136/2023),

– ob upoštevanju člena 294(3) Pogodbe o delovanju Evropske unije,

– ob upoštevanju mnenja Evropskega ekonomsko-socialnega odbora z dne 13. julija 2023[1],

– ob upoštevanju člena 59 Poslovnika,

– ob upoštevanju mnenj Odbora za zunanje zadeve in Odbora za promet in turizem,

– ob upoštevanju poročila Odbora za industrijo, raziskave in energetiko (A9-0426/2023),

1. sprejme stališče v prvi obravnavi, kakor je določeno v nadaljevanju;

2. odobri svojo izjavo, priloženo tej resoluciji;

3. poziva Komisijo, naj mu zadevo ponovno predloži, če svoj predlog nadomesti, ga bistveno spremeni ali ga namerava bistveno spremeniti;

4. naroči svoji predsednici, naj stališče Parlamenta posreduje Svetu in Komisiji ter nacionalnim parlamentom.

[1] UL C 349, 29.9.2023, str. 167.

Predlog spremembe 1

PREDLOGI SPREMEMB EVROPSKEGA PARLAMENTA*

k predlogu Komisije

2023/0109(COD)

Predlog

UREDBA EVROPSKEGA PARLAMENTA IN SVETA

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

EVROPSKI PARLAMENT IN SVET EVROPSKE UNIJE STA –

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

ob upoštevanju predloga Evropske komisije,

po posredovanju osnutka zakonodajnega akta nacionalnim parlamentom,

ob upoštevanju mnenja Računskega sodišča[2],

ob upoštevanju mnenja Evropskega ekonomsko-socialnega odbora[3],

ob upoštevanju mnenja Odbora regij[4],

v skladu z rednim zakonodajnim postopkom,

ob upoštevanju naslednjega:

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

(2) Obseg, pogostost in posledice kibernetskovarnostnih incidentov se ***po vsej Uniji in tudi na svetovni ravni*** povečujejo ***tako z vidika njihovih metod kot z vidika posledic***, vključno z napadi na oskrbovalno verigo, katerih cilj je kibernetsko vohunjenje,

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

2 UL C […], […], str. […].

3 UL C , , str. .

4 UL C , , str. .

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

(3) Okrepiti je treba konkurenčni položaj industrijskega in storitvenega sektorja v Uniji v celotnem spletnem gospodarstvu ter podpreti njuno digitalno preobrazbo, in sicer z okrepitvijo ravni kibernetske varnosti na enotnem digitalnem trgu. Kot je priporočeno v treh različnih predlogih Konference o prihodnosti Evrope[5], je treba povečati odpornost državljanov, podjetij***, zlasti mikro-, malih in srednjih podjetij (v nadaljnjem besedilu: MSP), vključno z zagonskimi podjetji,*** in subjektov, ki upravljajo kritične infrastrukture, ***vključno z lokalnimi ali regionalnimi organi,*** proti vse večjim kibernetskovarnostnim grožnjam, ki lahko imajo uničujoče družbene in gospodarske posledice. Zato so potrebne naložbe v infrastrukture in storitve ***ter krepitev zmogljivosti za razvoj kibernetskovarnostnih veščin***, ki bodo podpirale hitrejše odkrivanje kibernetskovarnostnih groženj in incidentov ter odzivanje nanje, države članice pa potrebujejo pomoč pri boljši pripravi na pomembne kibernetskovarnostne incidente in take incidente velikih razsežnosti ter odzivanju nanje. Unija bi tudi morala povečati svoje zmogljivosti na teh področjih, zlasti kar zadeva zbiranje in analizo podatkov o kibernetskovarnostnih grožnjah in incidentih.

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

[5] https://futureu.europa.eu/sl/

(4) Unija je že sprejela več ukrepov za zmanjšanje ranljivosti in povečanje odpornosti kritičnih infrastruktur in subjektov proti tveganjem za kibernetsko varnost, zlasti Direktivo (EU) 2022/2555 Evropskega parlamenta in Sveta[6], Priporočilo Komisije (EU) 2017/1584[7], Direktivo 2013/40/EU Evropskega parlamenta in Sveta[8] ter Uredbo (EU) 2019/881 Evropskega parlamenta in Sveta[9]. Poleg tega so države članice v priporočilu Sveta o usklajenem vseevropskem pristopu za krepitev odpornosti kritične infrastrukture pozvane, naj sprejmejo nujne in učinkovite ukrepe ter zvesto, učinkovito, solidarno in usklajeno sodelujejo med seboj, s Komisijo in drugimi ustreznimi javnimi organi ter zadevnimi subjekti, da bi se okrepila odpornost kritične infrastrukture, ki se uporablja za zagotavljanje bistvenih storitev na notranjem trgu.

(5) Zaradi vse večjih tveganj za kibernetsko varnost in na splošno zapletene krajine groženj, pa tudi zaradi jasnega tveganja hitrega prelivanja kibernetskih incidentov iz ene države članice v druge in iz tretje države v Unijo je potrebna okrepljena solidarnost na ravni Unije za boljše odkrivanje kibernetskovarnostnih groženj in incidentov ter pripravo in odzivanje nanje ***in boljšo obnovitev po njih***. Države članice so Komisijo v sklepih Sveta o kibernetski drži EU pozvale tudi, naj predstavi predlog o novem skladu za odzivanje na izredne kibernetskovarnostne razmere[10].

(6) V skupnem sporočilu o politiki EU za kibernetsko obrambo[11], sprejetem 10. novembra 2022, je bila napovedana pobuda EU za kibernetsko solidarnost z naslednjimi cilji: okrepitev skupnih zmogljivosti EU za odkrivanje, situacijsko zavedanje in odzivanje s spodbujanjem uvedbe ***unijske mreže*** centrov za varnostne operacije ▌, podpiranje postopne vzpostavitve kibernetskovarnostne rezerve na ravni EU s storitvami zaupanja vrednih zasebnih ponudnikov in preskušanje kritičnih subjektov glede morebitnih ranljivosti na podlagi ocen tveganja EU.

(7) Po vsej Uniji je treba izboljšati odkrivanje kibernetskih groženj in incidentov ter situacijsko zavedanje o njih, hkrati pa je treba okrepiti solidarnost s povečanjem pripravljenosti in zmogljivosti držav članic in Unije za odzivanje na pomembne kibernetskovarnostne incidente in take incidente velikih razsežnosti ***ter za njihovo preprečevanje***. Zato bi bilo treba vzpostaviti vseevropsko ***mrežo*** centrov za varnostne operacije (evropski kibernetski ščit), da bi se oblikovale in okrepile skupne zmogljivosti za odkrivanje in situacijsko zavedanje ***in tako okrepile zmogljivosti Unije za odkrivanje groženj in izmenjavo informacij***; vzpostaviti bi bilo treba mehanizem za izredne

---

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

7 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 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).

9 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).

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

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

kibernetskovarnostne razmere, da bi države članice podprli pri pripravi na pomembne kibernetskovarnostne incidente in take incidente velikih razsežnosti, odzivanju nanje in takojšnji obnovitvi po njih; vzpostaviti bi bilo treba mehanizem za pregledovanje kibernetskovarnostnih incidentov za pregledovanje in ocenjevanje posameznih pomembnih kibernetskovarnostnih incidentov ali incidentov velikih razsežnosti. Ti ukrepi ne posegajo v člena 107 in 108 Pogodbe o delovanju Evropske unije (PDEU).

(8) Za dosego teh ciljev je treba tudi spremeniti nekatere dele Uredbe (EU) 2021/694 Evropskega parlamenta in Sveta[12]. Zlasti bi bilo treba s to uredbo spremeniti Uredbo (EU) 2021/694, kar zadeva dodajanje novih operativnih ciljev v zvezi z evropskim kibernetskim ščitom in mehanizmom za izredne ***kibernetskovarnostne*** razmere v okviru specifičnega cilja 3 programa Digitalna Evropa, katerega cilj je zagotoviti odpornost, celovitost in zanesljivost enotnega digitalnega trga, okrepiti zmogljivosti za spremljanje kibernetskih napadov in groženj in odzivanje nanje ter izboljšati čezmejno sodelovanje na področju kibernetske varnosti. To bo dopolnjeno s posebnimi pogoji, pod katerimi se lahko za te ukrepe dodeli finančna podpora, pri čemer bi bilo treba opredeliti mehanizme upravljanja in usklajevanja, ki so potrebni za doseganje zastavljenih ciljev. Druge spremembe Uredbe (EU) 2021/694 bi morale vključevati opise predlaganih ukrepov v okviru novih operativnih ciljev in merljive kazalnike za spremljanje izvajanja teh novih operativnih ciljev.

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

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

(10) Za to uredbo se uporabljajo horizontalna finančna pravila, ki sta jih Evropski parlament in Svet sprejela na podlagi člena 322 PDEU. Ta pravila so navedena v Uredbi ***(EU, Euratom) 2018/1046 Evropskega parlamenta in Sveta[13]*** in določajo zlasti postopek za določitev in izvrševanje proračuna Unije ter urejajo nadzor nad odgovornostmi finančnih udeležencev. Pravila, sprejeta na podlagi člena 322 PDEU, vključujejo tudi

---

[12] 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).

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

splošni režim pogojenosti za zaščito proračuna Unije, kot je določen v Uredbi (EU, Euratom) 2020/2092 Evropskega parlamenta in Sveta[14].

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

(11a) Mehanizem za izredne kibernetskovarnostne razmere in kibernetskovarnostna rezerva EU, vzpostavljena s to uredbo, sta novi pobudi in pri pripravi večletnega finančnega okvira za obdobje 2021–2027 še nista bila predvidena, pri čemer bi moralo biti zmanjšanje financiranja drugih prednostnih nalog programa Digitalna Evropa kot posledica financiranja teh dveh pobud čim bolj omejeno. Znesek finančnih sredstev, namenjenih kibernetskovarnostni rezervi EU, bi bilo zato treba zmanjšati in črpati predvsem iz nedodeljenih razlik do zgornjih mej večletnega finančnega okvira ali mobilizirati prek netematskih posebnih instrumentov večletnega finančnega okvira. Če se sredstva dodelijo ali prerazporedijo iz obstoječih programov, bi morala biti ta sredstva omejena na absolutni minimum, da to ne bi negativno vplivalo na obstoječe programe, zlasti Erasmus+, in da bi zagotovili, da bodo lahko ti programi dosegli svoje zastavljene cilje.

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

[14] ***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).***

boljšemu odkrivanju kibernetskovarnostnih groženj in incidentov ter tako dopolnjevati in podpirati subjekte in omrežja Unije, pristojne za krizno upravljanje v Uniji, zlasti organizacijsko mrežo EU za povezovanje v kibernetski krizi (v nadaljnjem besedilu: mreža EU-CyCLONe), kot je opredeljena v Direktivi (EU) 2022/2555 Evropskega parlamenta in Sveta[15].

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

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

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

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

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

(17) Skupno situacijsko zavedanje med ustreznimi organi je nujen osnovni pogoj za pripravljenost in usklajevanje na ravni Unije v zvezi s pomembnimi kibernetskovarnostnimi incidenti in takimi incidenti velikih razsežnosti. Z Direktivo (EU) 2022/2555 je ustanovljena mreža EU-CyCLONe za podporo usklajenemu obvladovanju kibernetskovarnostnih incidentov velikih razsežnosti in kriz na operativni ravni ter zagotovitev redne izmenjave ustreznih informacij med državami članicami ter institucijami, organi in agencijami Unije. V Priporočilu (EU) 2017/1584 o usklajenem odzivu na velike kibernetske incidente in krize je obravnavana vloga vseh ustreznih akterjev. V Direktivi (EU) 2022/2555 je tudi opozorjeno na odgovornosti Komisije v okviru mehanizma Unije na področju civilne zaščite, vzpostavljenega s Sklepom 1313/2013/EU Evropskega parlamenta in Sveta[16], ter za pripravo analitičnih poročil o enotni ureditvi za politično odzivanje na krize (IPCR) v skladu z Izvedbenim sklepom ***Sveta*** (EU) 2018/1993[17]. Zato bi morali čezmejni centri za varnostne operacije v primerih, ko pridobijo informacije v zvezi z morebitnim ali tekočim

---

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

17 ***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).***

kibernetskovarnostnim incidentom velikih razsežnosti, mreži EU-CyCLONe, mreži skupin CSIRT in Komisiji ***v skladu z Direktivo (EU) 2022/2555*** zagotoviti ustrezne informacije. Glede na okoliščine bi lahko informacije, ki jih je treba izmenjati, vključevale zlasti tehnične informacije, informacije o naravi in motivih napadalca ali morebitnega napadalca ter netehnične informacije na višji ravni o morebitnem ali tekočem kibernetskovarnostnem incidentu velikih razsežnosti. V zvezi s tem bi bilo treba ustrezno upoštevati načelo potrebe po seznanitvi in morda občutljivo naravo izmenjanih informacij.

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

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

(20) Evropski kibernetski ščit bi moral z zbiranjem, deljenjem in izmenjavanjem podatkov okrepiti tehnološko suverenost***, odprto strateško avtonomijo, konkurenčnost in odpornost*** Unije***, pa tudi pomemben kibernetskovarnostni ekosistem EU***. Zbiranje visokokakovostnih pripravljenih podatkov bi moralo prispevati tudi k razvoju naprednih tehnologij umetne inteligence in podatkovne analitike. ***Umetna inteligenca deluje najbolj učinkovito v kombinaciji s človeško analizo. Zato ima usposobljena delovna sila še vedno ključno vlogo pri zbiranju visokokakovostnih podatkov.*** Olajšati bi ga bilo treba tako, da se evropski kibernetski ščit poveže z infrastrukturo vseevropskega visokozmogljivostnega računalništva, vzpostavljenega z Uredbo Sveta (EU) 2021/1173[18].

(21) Čeprav je evropski kibernetski ščit civilni projekt, bi lahko imela skupnost za kibernetsko obrambo koristi od okrepljenih zmogljivosti civilnega odkrivanja in situacijskega zavedanja, ki so bile razvite za zaščito kritične infrastrukture. Čezmejni centri za varnostne operacije bi morali ob podpori Komisije in Evropskega kompetenčnega centra za kibernetsko varnost (v nadaljnjem besedilu: ECCC) ter v sodelovanju z visokim predstavnikom Unije za zunanje zadeve in varnostno politiko (v nadaljnjem besedilu: visoki predstavnik) postopoma razviti namenske ***pogoje dostopa*** ter protokole in standarde ***zaščitnih ukrepov***, da se omogoči sodelovanje s skupnostjo za kibernetsko obrambo, vključno s pogoji preverjanja in varnostnimi pogoji***, pri čemer morajo upoštevati civilni značaj institucij in namembnost financiranja, posledično pa***

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

uporabljati sredstva, ki so na voljo obrambni skupnosti. Razvoj evropskega kibernetskega ščita bi moral spremljati razmislek, na podlagi katerega bi bilo v tesnem sodelovanju z visokim predstavnikom omogočeno prihodnje sodelovanje z mrežami in platformami, odgovornimi za izmenjavo informacij v skupnosti za kibernetsko obrambo***, pri čemer morajo biti v celoti spoštovane pravice in svoboščine***.

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

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

(24) Glede na vse večja tveganja in število kibernetskovarnostnih incidentov, ki prizadenejo države članice, je treba vzpostaviti instrument podpore ob krizi, da se izboljša odpornost Unije proti pomembnim kibernetskovarnostnim incidentom in takim incidentom velikih razsežnosti ter da se ukrepi držav članic dopolnijo z nujno finančno podporo za pripravljenost, odzivanje in takojšnjo obnovitev bistvenih storitev. Ta instrument bi moral omogočiti hitro ***in učinkovito*** zagotavljanje pomoči v določenih okoliščinah in pod jasnimi pogoji ter skrbno spremljanje in ocenjevanje porabe sredstev. Čeprav so za preprečevanje kibernetskovarnostnih incidentov in kriz ter pripravo in odzivanje nanje v prvi vrsti odgovorne države članice, mehanizem za izredne ***kibernetskovarnostne*** razmere spodbuja solidarnost med državami članicami v skladu s členom 3(3) Pogodbe o Evropski uniji (PEU).

(25) Mehanizem za izredne ***kibernetskovarnostne*** razmere bi moral državam članicam zagotoviti podporo z dopolnjevanjem njihovih ukrepov in virov ter druge obstoječe možnosti podpore v primeru odziva na pomembne kibernetskovarnostne incidente in take incidente velikih razsežnosti ter takojšnje obnovitve po njih, kot so storitve, ki jih zagotavlja Agencija Evropske unije za kibernetsko varnost (ENISA) v skladu s svojim mandatom, usklajen odziv in pomoč mreže skupin CSIRT, podpora mreže EU-CyCLONe pri ublažitvi posledic ter medsebojna pomoč med državami članicami, med drugim v okviru člena 42(7) PEU, enot za hitro odzivanje na kibernetske grožnje v okviru stalnega strukturnega sodelovanja (PESCO)[19] in skupin za hitro odzivanje na hibridne grožnje. Obravnavati bi moral potrebo po zagotavljanju razpoložljivosti specializiranih sredstev za podporo pripravljenosti in odzivanju na kibernetskovarnostne incidente po vsej Uniji in v tretjih državah.

(26) Ta instrument ne posega v postopke in okvire za usklajevanje odzivanja na krize na ravni Unije, zlasti mehanizem Unije na področju civilne zaščite[20], enotno ureditev za

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

[20] 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).

političnо odzivanje na krize[21] in Direktivo (EU) 2022/2555. Prispeva lahko k ukrepom, ki se izvajajo v okviru člena 42(7) PEU ali v primerih, opredeljenih v členu 222 PDEU, ali jih dopolnjuje. Uporabo tega instrumenta bi bilo treba po potrebi uskladiti tudi z izvajanjem ukrepov iz zbirke orodij za kibernetsko diplomacijo.

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

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

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

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

izvede skupina za sodelovanje na področju varnosti omrežnih in informacijskih sistemov ob podpori Komisije in agencije ENISA ter v sodelovanju z Organom evropskih regulatorjev za elektronske komunikacije (BEREC), usklajene ocene tveganja, ki se izvedejo v skladu s členom 22 Direktive (EU) 2022/2555, in testiranje digitalne operativne odpornosti, kot je določeno v Uredbi (EU) 2022/2554 Evropskega parlamenta in Sveta[22]. Pri izbiri sektorjev bi bilo treba upoštevati tudi priporočilo Sveta o usklajenem vseevropskem pristopu za krepitev odpornosti kritične infrastrukture.

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

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

(32) Mehanizem za izredne ***kibernetskovarnostne*** razmere bi moral podpreti pomoč, ki jo države članice zagotovijo državi članici, ki jo je prizadel pomemben kibernetskovarnostni incident ali tak incident velikih razsežnosti, med drugim pomoč mreže skupin CSIRT iz člena 15 Direktive (EU) 2022/2555. Državam članicam, ki zagotovijo pomoč, bi bilo treba dovoliti, da vložijo zahtevke za kritje stroškov, povezanih s pošiljanjem strokovnih skupin v okviru medsebojne pomoči. Upravičeni stroški bi lahko vključevali potne stroške, stroške nastanitve in dnevnice strokovnjakov na področju kibernetske varnosti.

(33) Postopno bi bilo treba vzpostaviti kibernetskovarnostno rezervo na ravni Unije, ki bi zajemala storitve zasebnih ponudnikov upravljanih varnostnih storitev za podporo ukrepom odzivanja in takojšnje obnovitve v primeru pomembnih kibernetskovarnostnih incidentov ali takih incidentov velikih razsežnosti. Kibernetskovarnostna rezerva EU bi morala zagotoviti razpoložljivost in pripravljenost storitev***, hkrati pa krepiti odpornost Unije, vključno s sodelovanjem evropskih ponudnikov upravljanih varnostnih storitev, ki so MSP, in zagotavljanjem vzpostavitve ekosistema kibernetske varnosti, zlasti mikropodjetij, MSP, vključno z zagonskimi podjetji, z naložbami v raziskave in inovacije za razvoj najsodobnejših tehnologij, kot so tehnologije, povezane z računalništvom v oblaku in umetno inteligenco***. ***Zaupanja vredni ponudniki, vključno z MSP, bi morali imeti možnost, da za namene izpolnitve zgoraj navedenih meril sodelujejo drug z drugim.*** Storitve iz kibernetskovarnostne rezerve EU bi morale biti kot dopolnitev ukrepov nacionalnih organov na nacionalni ravni namenjene podpori tem organom pri zagotavljanju pomoči prizadetim subjektom, ki delujejo v kritičnih ali visoko kritičnih sektorjih. ***Zato bi bilo treba v sklopu kibernetskovarnostne rezerve spodbujati naložbe v raziskave in inovacije, da bi pospešili razvoj teh tehnologij. Po potrebi bi se lahko izvedle skupne vaje z zaupanja vrednimi ponudniki in***

[22] 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.

potencialnimi uporabniki kibernetskovarnostne rezerve, da bi po potrebi zagotovili njeno učinkovito delovanje. Države članice bi morale ob vložitvi zahtevka za podporo iz kibernetskovarnostne rezerve EU opredeliti podporo, zagotovljeno prizadetemu subjektu na nacionalni ravni, ki bi jo bilo treba upoštevati pri oceni zahtevka države članice. Storitve iz kibernetskovarnostne rezerve EU se lahko pod podobnimi pogoji uporabljajo tudi za podporo institucijam, organom, uradom in agencijam Unije. ***Komisija bi morala poskrbeti za vključenost držav članic in obsežne izmenjave z njimi, da ne bi prišlo do podvajanja s podobnimi pobudami, tudi v okviru Organizacije Severnoatlantske pogodbe (NATO).***

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

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

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

(37) Ob upoštevanju nepredvidljive narave kibernetskih napadov in dejstva, da ti pogosto niso omejeni na določeno geografsko območje in da predstavljajo veliko tveganje prelivanja, krepitev odpornosti sosednjih držav in njihove zmogljivosti za učinkovito odzivanje na pomembne kibernetskovarnostne incidente in take incidente velikih

razsežnosti prispeva k zaščiti Unije kot celote. Zato lahko podporo iz kibernetskovarnostne rezerve EU prejmejo tretje države, pridružene programu Digitalna Evropa, če je to določeno v ustreznih sporazumih o pridružitvi programu Digitalna Evropa. Unija bi morala financiranje za pridružene tretje države podpreti v okviru ustreznih partnerstev in instrumentov financiranja za te države. Podpora bi morala zajemati storitve na področju odzivanja na pomembne kibernetskovarnostne incidente ali take incidente velikih razsežnosti in takojšnje obnovitve po njih. Pri zagotavljanju podpore tretjim državam, pridruženim programu Digitalna Evropa, bi morali veljati pogoji, določeni za kibernetskovarnostno rezervo EU in zaupanja vredne ponudnike v tej uredbi.

(37a) Tretje države bi lahko prek podpore pri odzivanju na incidente iz kibernetskovarnostne rezerve EU dostopale do virov in podpore v skladu s to uredbo. Poleg tega utegnejo biti za zagotavljanje specifičnih storitev v sklopu kibernetskovarnostne rezerve EU potrebni ponudniki storitev odzivanja na incidente iz tretjih držav, vključno s tretjimi državami, pridruženimi programu Digitalna Evropa, ali drugih mednarodnih partnerskih držav in članic Nata. Z odstopanjem od Uredbe (EU, Euratom) 2018/1046 ter da bi okrepili tehnološko suverenost, odprto strateško avtonomijo, konkurenčnost in odpornost Unije ter zaščitili njena strateška sredstva, interese ali varnost, subjektom s sedežem v tretjih državah, ki niso pogodbenice Sporazuma o javnih naročilih in v zvezi s katerimi ni bil izveden pregled v smislu Uredbe (EU) 2019/452 Evropskega parlamenta in Sveta[23] in po potrebi v zvezi s katerimi niso bili izvedeni ukrepi za zmanjšanje tveganj, ob upoštevanju ciljev iz te uredbe ne bi smelo biti dovoljeno sodelovati. Zunanja razsežnost te uredbe bi morala biti skladna z določbami iz pridružitvenega sporazuma v okviru programa Digitalna Evropa. Da se zagotovi, da lahko državljani sodelujejo pri tem procesu, bi morala nadzor nad sodelovanjem tretjih držav izvajati javnost skupaj z akterji z zakonodajnimi pooblastili.

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

---

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

---

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

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

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

(38c) Namen krepitve raziskav in inovacij na področju kibernetske varnosti je povečati odpornost in odprto strateško avtonomijo Unije. Prav tako je pomembno ustvariti sinergije s programi za raziskave in inovacije in obstoječimi instrumenti ter institucijami in povečati sodelovanje ter usklajevanje med različnimi deležniki, vključno z zasebnim sektorjem, civilno družbo, akademskim svetom, državami članicami, Komisijo in agencijo ENISA;

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

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

(38f) Za dopolnitev nekaterih nebistvenih elementov te uredbe bi bilo treba na Komisijo prenesti pooblastilo, da v skladu s členom 290 PDEU sprejme akte, s katerimi določi pogoje za interoperabilnost med čezmejnimi centri za varnostne operacije, določi postopkovne ureditve za izmenjavo informacij med čezmejnimi centri za varnostne operacije na eni strani ter mrežo skupin CSIRT in Komisijo na drugi strani, določi vrste in število storitev za odzivanje, potrebnih za kibernetskovarnostno rezervo EU,

ter natančneje opredeli podrobne ureditve za dodelitev podpornih storitev iz kibernetskovarnostne rezerve EU. Zlasti je pomembno, da se Komisija pri pripravljalnem delu ustrezno posvetuje, tudi na ravni strokovnjakov, in da se ta posvetovanja izvedejo v skladu z načeli, določenimi v Medinstitucionalnem sporazumu z dne 13. aprila 2016 o boljši pripravi zakonodaje*. Za zagotovitev enakopravnega sodelovanja pri pripravi delegiranih aktov Evropski parlament in Svet zlasti prejmeta vse dokumente sočasno s strokovnjaki iz držav članic, njuni strokovnjaki pa se sistematično lahko udeležujejo sestankov strokovnih skupin Komisije, ki zadevajo pripravo delegiranih aktov.

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

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

SPREJELA NASLEDNJO UREDBO:

Poglavje I

SPLOŠNI CILJI, PREDMET UREJANJA IN OPREDELITVE POJMOV

Člen 1

Predmet urejanja in cilji

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

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

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

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

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

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

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

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

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

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

Člen 2

Opredelitev pojmov

V tej uredbi se uporabljajo naslednje opredelitve pojmov:

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

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

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

[24] 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).

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

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

(4a) „kritični subjekt“ pomeni kritični subjekt, kot je opredeljen v členu 2(1) Direktive (EU) 2022/2557 Evropskega parlamenta in Sveta[25];

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

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

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

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

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

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

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

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

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

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

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

---

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

Poglavje II

EVROPSKI KIBERNETSKI ŠČIT

Člen 3

Vzpostavitev evropskega kibernetskega ščita

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

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

2. Evropski kibernetski ščit:

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

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

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

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

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

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

Člen 4

Nacionalni centri za varnostne operacije

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

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

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

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

3. Nacionalni center za varnostne operacije, izbran v skladu z odstavkom 2, se zaveže, da bo za sodelovanje v čezmejnem centru za varnostne operacije zaprosil v dveh letih od datuma pridobitve orodij in infrastruktur ali datuma prejema nepovratnih sredstev, kateri koli nastopi prej. Če nacionalni center za varnostne operacije do takrat ne sodeluje v čezmejnem centru za varnostne operacije, ni upravičen do dodatne podpore Unije v skladu s to uredbo.

Člen 5

Čezmejni centri za varnostne operacije

1. Gostiteljski konzorcij, ki ga sestavljajo vsaj tri države članice, ki jih zastopajo nacionalni centri za varnostne operacije, ki so se zavezali skupnemu usklajevanju dejavnosti odkrivanja in spremljanja kibernetskih groženj, je upravičen do sodelovanja pri ukrepih za ustanovitev

čezmejnega centra za varnostne operacije. ***Čezmejni centri za varnostne operacije so zasnovani za odkrivanje in analiziranje kibernetskih groženj, preprečevanje incidentov ter podpiranje priprave visokokakovostnih obveščevalnih podatkov, zlasti z izmenjavo podatkov iz različnih virov, javnih in zasebnih, pa tudi z izmenjavo najsodobnejših orodij in skupnim razvijanjem kibernetskih zmogljivosti za odkrivanje, analizo, preprečevanje in zaščito v zaupanja vrednem in varnem okolju.***

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

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

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

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

Člen 6

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

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

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

(b) zvišuje raven kibernetske varnosti, zlasti z ozaveščanjem v zvezi s kibernetskimi grožnjami, omejevanjem ali oviranjem zmožnosti širjenja takih groženj, podpiranjem vrste obrambnih zmogljivosti, odpravljanjem in razkrivanjem ranljivosti, tehnikami

odkrivanja, omejevanja in preprečevanja groženj, strategijami za zmanjšanje tveganja ali fazami odzivanja in okrevanja ali spodbujanjem sodelovanja med javnimi in zasebnimi subjekti pri raziskovanju kibernetskih groženj.

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

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

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

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

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

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

Člen 7

Sodelovanje in izmenjava informacij z mrežo skupin CSIRT

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

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

Člen 8

Varnost

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

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

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

Poglavje III

MEHANIZEM ZA IZREDNE KIBERNETSKE VARNOSTNE RAZMERE

Člen 9

Vzpostavitev mehanizma za izredne kibernetske *varnostne* razmere

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

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

Člen 10

Vrsta ukrepov

1. Mehanizem podpira naslednje vrste ukrepov:

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

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

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

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

Člen 11

Usklajeno preskušanje pripravljenosti subjektov

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

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

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

Člen 12

Vzpostavitev kibernetskovarnostne rezerve EU

1. Vzpostavi se kibernetskovarnostna rezerva EU za pomoč uporabnikom iz odstavka 3 pri odzivanju ali zagotavljanju podpore pri odzivanju na pomembne

kibernetskovarnostne incidente ali take incidente velikih razsežnosti ter pri takojšnjem okrevanju po takih incidentih.

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

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

3. Uporabniki storitev iz kibernetskovarnostne rezerve EU so:

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

(b) Institucije, organi in agencije Unije, ***kot so opredeljeni v členu 3(1) Uredbe (EU) .../2023 Evropskega parlamenta in Sveta[26] ter skupine CERT-EU***.

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

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

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

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

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

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

Člen 13

Zahtevki za podporo iz kibernetskovarnostne rezerve EU

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

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

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

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

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

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

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

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

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

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

Člen 14

Izvajanje podpore iz kibernetskovarnostne rezerve EU

1. Zahtevke za podporo iz kibernetskovarnostne rezerve EU oceni Komisija ob podpori agencije ENISA ali kot je opredeljeno v sporazumih o prispevku iz člena 12(6) in uporabnikom iz

člena 12(3) se odgovor na zahtevke pošlje ***brez nepotrebnega odlašanja, v vsakem primeru pa v 24 urah*.**

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

(a) resnost kibernetskovarnostnega incidenta;

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

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

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

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

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

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

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

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

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

Člen 15

Usklajevanje z mehanizmi kriznega upravljanja

1. Kadar pomembni kibernetskovarnostni incidenti ali taki incidenti velikih razsežnosti izvirajo iz nesreč, kot so opredeljene v Sklepu št. 1313/2013/EU[27], ali povzročijo take nesreče, podpora

[27] 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).

za odzivanje na take incidente na podlagi te uredbe dopolnjuje ukrepe na podlagi Sklepa št. 1313/2013/EU in brez poseganja vanj.

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

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

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

Člen 16

Zaupanja vredni ponudniki

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

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

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

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

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

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

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

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

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

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

(f) ponudnik je opremljen ***s sodobno*** tehnično strojno in programsko opremo, potrebno za podporo zahtevani storitvi***, in po potrebi izpolnjuje zahteve iz Uredbe (EU) .../... Evropskega parlamenta in Sveta[28] (2022/0272(COD))***;

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

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

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

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

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

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

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

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

Člen 17

Podpora tretjim državam

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

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

---

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

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

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

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

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

Poglavje IV

MEHANIZEM ZA PREGLEDOVANJE KIBERNETSKOVARNOSTNIH INCIDENTOV

Člen 18

Mehanizem za pregledovanje kibernetskovarnostnih incidentov

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

2. Agencija ENISA pri pripravi poročila o pregledu incidenta iz odstavka 1 sodeluje z vsemi ustreznimi deležniki, vključno s predstavniki držav članic, Komisijo, drugimi ustreznimi institucijami, organi, uradi in agencijami EU, ponudniki upravljanih varnostnih storitev ***v nacionalnih in čezmejnih centrih za varnostne operacije*** in uporabniki kibernetskih storitev***, in od teh deležnikov zbere povratne informacije, kar se dopolni z jamstvi in spremljanjem, ki zadostujejo za zagotovitev, da bodo akterji s področja kibernetskovarnostnih storitev upoštevali pridobljene izkušnje in prepoznane primere dobre prakse***. Po potrebi sodeluje tudi s subjekti, ki so jih prizadeli pomembni kibernetskovarnostni incidenti ali taki incidenti velikih razsežnosti. Za podporo pregledu se lahko posvetuje tudi z drugimi vrstami deležnikov. Predstavniki, s katerimi se opravi posvetovanje, razkrijejo vsako morebitno nasprotje interesov.

3. Poročilo zajema pregled in analizo posameznega pomembnega kibernetskovarnostnega incidenta ali takega incidenta velikih razsežnosti, vključno z glavnimi vzroki, ranljivostmi in pridobljenimi spoznanji. V njem so zaupne informacije zavarovane v skladu s pravom Unije ali

nacionalnim pravom v zvezi z varstvom občutljivih ali tajnih podatkov. ***Ne zajema podrobnosti o aktivno izrabljenih ranljivostih, ki so še neodpravljene.***

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

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

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

Poglavje V

KONČNE DOLOČBE

Člen 19

Spremembe Uredbe (EU) 2021/694

Uredba (EU) 2021/694 se spremeni:

(1) člen 6 se spremeni:

(a) odstavek 1 se spremeni:

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

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

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

vzpostavitev in upravljanje mehanizma za izredne ***kibernetskovarnostne*** razmere za podporo državam članicam pri pripravi na pomembne kibernetskovarnostne incidente in odzivanju nanje, pri čemer mehanizem dopolnjuje nacionalne vire in zmogljivosti ter druge oblike podpore, ki so na voljo na ravni Unije, vključno z vzpostavitvijo kibernetskovarnostne rezerve EU.“;

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

„2. Ukrepi v okviru specifičnega cilja 3 se izvajajo predvsem prek Evropskega industrijskega, tehnološkega in raziskovalnega kompetenčnega centra za kibernetsko varnost ter mreže nacionalnih koordinacijskih centrov v skladu z Uredbo (EU) 2021/887

Evropskega parlamenta in Sveta*, razen ukrepov za izvajanje kibernetskovarnostne rezerve EU, ki jih izvajata Komisija in agencija ENISA.“;

_____

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

(2) člen 9 se spremeni:

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

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

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

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

(aa) vstavi se naslednji nov odstavek 2a:

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

(ab) vstavi se naslednji nov odstavek 2b:

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

(b) doda se naslednji odstavek 8:

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

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

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

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

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

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

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

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

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

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

(4) doda se naslednji člen 16a:

„***Člen 16a***

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

(5) člen 19 se nadomesti z naslednjim:

„Nepovratna sredstva v okviru Programa se dodeljujejo in upravljajo v skladu z naslovom VIII ***Uredbe (EU, Euratom) 2018/1046*** ter lahko krijejo do 100 % upravičenih

stroškov brez poseganja v načelo sofinanciranja, kot je določeno v členu 190 ***Uredbe (EU, Euratom) 2018/1046***. Taka nepovratna sredstva se dodeljujejo in upravljajo, kot je določeno za vsak specifični cilj.

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

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

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

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

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

Člen 19a
Dodatna sredstva za agencijo ENISA

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

Člen 20

Ocena *in pregled*

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

2. Pri tem se zlasti ocenijo:

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

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

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

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

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

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

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

Člen 20a

Izvajanje prenosa pooblastila

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

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

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

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

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

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

Člen 21

Postopek v odboru

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

Člen 22

Začetek veljavnosti

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

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

V Strasbourgu,

Za Evropski parlament	*Za Svet*
predsednica	*predsednik*

PRILOGA

Uredba (EU) 2021/694 se spremeni:

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

„Specifični cilj 3 – kibernetska varnost in zaupanje

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

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

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

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

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

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

5. Spodbujanje solidarnosti med državami članicami pri pripravi na pomembne kibernetskovarnostne incidente in odzivanju nanje z uvedbo čezmejnih storitev kibernetske varnosti, med drugim s podporo za medsebojno pomoč med javnimi organi in vzpostavitvijo rezerve zaupanja vrednih ponudnikov ***upravljanih varnostnih*** storitev na ravni Unije.“;

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

„Specifični cilj 3 – kibernetska varnost in zaupanje

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

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

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

OBRAZLOŽITEV

OZADJE

Kibernetska varnost je v središču naših demokracij, kot bi tudi morala biti. Kadar je ogrožena, se med prebivalstvom in podjetji širi negotovost, pa tudi dezinformacij je več. To spodkopava demokratična načela, ki so temelj spoštovanja človekovih pravic. Da bi to preprečili, naše demokracije nujno potrebujejo varno digitalno okolje, ki je pod javnim nadzorom.

Kibernetski napadi so v EU v porastu tako z vidika metod kot z vidika njihovih posledic. Poleg tega je ruski napad na Ukrajino prinesel korenite spremembe že pred invazijo, z njim pa se je po navedbah poročila agencije ENISA o naravi groženj za leto 2022 začela tudi nova doba **kibernetske programske opreme**[1]. Ugotovljeno je bilo, da je treba v zvezi s tem kibernetskim konfliktom v sklopu **večstranskih programov** in projektov prednostno **okrepiti zmogljivosti** ter hitro **razviti veščine**. Da bi postali odpornejši, je nujno potreben skupen evropski odziv, ki bo poleg sodelovanja na nacionalni ravni temeljil na tesnejšem sodelovanju na evropski ravni.

Za uspešno izvajanje te uredbe bo ključnega pomena okrepiti kulturo kibernetske varnosti, ki varnost, med drugim tudi varnost digitalnega okolja, razume kot javno dobro.

Poleg tega so tarča kibernetskih napadov pogosto **lokalne, regionalne ali nacionalne javne storitve** in infrastruktura (npr. zdravstveni sektor, ki je še vedno ena glavnih tarč[2]). Dokazi tudi kažejo, da so **lokalni organi** zaradi pomanjkanja finančnih in človeških virov med najranljivejšimi tarčami. Zlasti je pomembno, da se voditelji na lokalni ravni zavedajo, da je treba povečati digitalno odpornost[3]. Napade predvsem in neposredno občutijo državljani in zatorej, tudi z dezinformacijskimi kampanjami, ogrožajo naše demokracije. Občutek negotovosti, ki se lahko med prebivalstvom porodi zaradi teh razmer, lahko privede do političnih preferenc, ki se ravnajo po radikalni zavezanosti varnosti na račun spoštovanja temeljnih pravic. A je dejansko ravno obratno: varnost je bistven del naših demokracij, ki je združljiv z vsemi drugimi pravicami in potreben zanje.

Tudi **podjetja in MSP** v EU se spoprijemajo s kibernetsko kriminaliteto, in ker se za poslovanje v vse večji meri uporablja digitalno okolje, so tudi skrbi v zvezi s kibernetsko varnostjo vse večje. MSP so manj pripravljena, saj imajo na voljo manj sredstev za lastno zaščito, še manj pa se zavedajo, da lahko postanejo žrtve kibernetskih napadov.

Pričakuje se, da bo do tovrstnih napadov prihajalo tudi v prihodnje in da se bodo še povečali, zlasti v razmerah politične nestabilnosti, še posebej pa v vojnih razmerah. Digitalni prehod vsak dan napreduje, zato postaja digitalna odpornost vse pomembnejša za naš vsakdan in za **odprto strateško avtonomijo EU**.

---

[1] *ENISA Threat Landscape 2022* (Poročilo agencije ENISA o naravi groženj za leto 2022), oktober 2022, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@@download/fullReport.
[2] *ENISA Threat Landscape: Health Sector* (Poročilo agencije ENISA o naravi groženj: zdravstveni sektor), julij 2023. https://www.enisa.europa.eu/publications/health-threat-landscape/@@download/fullReport
[3] Evropski odbor regij: *Digital Resilience* (Digitalna odpornost), 2023, https://cor.europa.eu/en/engage/studies/Documents/Digital%20resilience.pdf.

PREDLOGI POROČEVALKE

Poročevalka meni, da mora biti EU bolje pripravljena na prihodnost, in pozdravlja ta nujni zakonodajni akt, da se združijo viri, informacije in znanje in tako zagotovi solidarnost med državami članicami, poveča industrijska zmogljivost v EU ter **na usklajen način razvijajo veščine in zmogljivosti**, ki zagotavljajo kibernetsko varnost. Tako bomo postali bolj odporni na prihodnje napade in naše demokracije zaščitili pred tem, da bi se varnostne potrebe koristoljubno instrumentalizirale. Poleg tega je pomembno zaščititi integriteto naših volilnih procesov. Ta zakonodajni akt je bistvena zaveza dosegi cilja **odprte strateške avtonomije**.

Iz teh razlogov EU potrebuje močno in **usklajeno upravljanje** ter strukturirano sodelovanje z zasebnim sektorjem, da bi spodbudila razvoj evropske kibernetske industrije. To bo dopolnjevalo sodelovanje s podobno mislečimi mednarodnimi partnerji, pa tudi z drugimi državami, ki nimajo enakih zmogljivosti in bodo morda potrebovale pomoč, ko bodo tarča kibernetskih napadov. V aktu EU o kibernetski solidarnosti mora biti dobro opredeljeno, kako naj se upravlja z njim, in ne sme priti do prekrivanja z že obstoječimi pobudami in zakonodajnimi akti, kot je direktiva NIS 2.

Predlog v veliki meri temelji na tem, da si države članice informacije izmenjujejo prostovoljno. Poročevalka zato predlaga, naj se povečajo jamstva za krepitev zaupanja med državami članicami, da bi povečali njihovo udeležbo in sodelovanje, na primer pri skupni nabavi v zvezi z infrastrukturo, pa tudi vključevanje zakonodajnih pooblastil, da bi zagotovili zaupanje državljanov in **demokratična jamstva**.

Predlaga tudi, naj se **proračun** za to pobudo **zagotovi** iz prihodnjih večletnih finančnih okvirov, skupaj z zavezo držav članic, da bodo poskrbele za to, da se bodo dejavnosti, razvite v sklopu akta EU o kibernetski solidarnosti, izvajale tudi po letu 2027.

Poročevalka predlaga, naj se **struktura upravljanja** izboljša, upravljanje pa jasno opredeli in poveže z veljavno zakonodajo.

Poleg tega naj se izboljša **usklajevanje** med različnimi subjekti držav članic, pristojnimi za kibernetsko varnost, da bi omogočili skupni kibernetski ščit. Agencija ENISA pa naj bolj prispeva k usklajevanju in interakciji med različnimi akterji nacionalnih skupnosti.

Kar zadeva **novo kibernetskovarnostno rezervo**, poročevalka meni, da se lahko z naložbami v raziskave in inovacije za razvoj najsodobnejših tehnologij, kot so tehnologije v oblaku in tehnologije umetne inteligence, spodbudi razvijanje industrijskih zmogljivosti v EU, tudi za MSP. Poleg tega predlaga, naj pri tem še naprej sodeluje industrija, naj se okrepijo merila za njeno sodelovanje in zaupanje vanj (tj. da se sodelovanje industrije poveže z nacionalnim ali lokalnim podjetjem), tako da se pojasnijo **merila** in natančneje opredeli **tehnološka suverenost** ter poskrbi za ravnovesje med akterji iz tretjih držav in akterji EU. Predlaga pa tudi, naj se za zasebne ponudnike v sklopu **mehanizma za izredne kibernetske razmere** uporablja **certifikacijska shema**, da bi vzpostavili dolgoročno in na zaupanju temelječo partnerstvo.

Kar zadeva **mehanizem za pregledovanje incidentov**, poročevalka predlaga, naj se okrepi vloga agencije ENISA in zasebnega sektorja v sklopu centrov za varnostne operacije, in sicer

s pravimi jamstvi in spremljanjem, da bi se prepričali, ali pridobljene izkušnje upoštevajo tudi akterji iz industrije. Prav tako predlaga, naj se vključijo izkušnje, pridobljene v okviru medsebojnih strokovnih pregledov, kot je navedeno v direktivi NIS 2, in agenciji ENISA da na voljo več finančnih sredstev, da bi zagotovili učinkovito uporabo zakonodaje in ustrezno zaščito pred kibernetskimi grožnjami.

Poleg tega ima ta predlog že po definiciji zelo pomembno **zunanjo razsežnost**, saj lahko, po eni strani, tretje države prek podpore pri odzivanju na incidente iz kibernetskovarnostne rezerve EU dostopajo do virov in podpore iz akta EU o kibernetski solidarnosti, po drugi strani pa, ker so za kibernetsko rezervo še vedno potrebni akterji iz zasebnega sektorja, ki niso iz EU. Da bi lahko državljani sodelovali pri tem procesu, bi morala nadzor nad zunanjo razsežnostjo izvajati tudi javnost skupaj z akterji z zakonodajnimi pooblastili. Kibernetsko varnost bi bilo treba obravnavati kot javno dobro.

Eden od osrednjih stebrov tega predloga je razvoj veščin in kompetenc, ki ne bi vključeval zgolj naložb v razvoj znanja, temveč naložbe v to, da bi imeli vsi državljani dostop do usposabljanja za te veščine. Poročevalka predlaga, da bi se tesneje povezali z **akademijo EU za kibernetske veščine**, ki namerava odpraviti pomanjkanje strokovnjakov za kibernetsko varnost, in sicer z združitvijo zasebnih in javnih pobud ter zagotavljanjem usposabljanja in certificiranja za državljane. To pa bodo morali spremljati zaščitni ukrepi, da se prepreči beg možganov, hkrati pa ne bi smela vplivati negativno na mobilnost delovne sile.

Glede na to, da je leto 2023 evropsko leto spretnosti, poročevalka predlaga, naj se vlaga v ta sektor in vključijo aktivni ukrepi za razvoj veščin v njem, hkrati pa veča ozaveščenost državljanov. Ukrepi bodo zasnovani tako, da zaradi naložb ne bo prišlo do neravnovesij med državami članicami, saj lahko aktualno veliko povpraševanje in visoke plače v tem sektorju privedejo do določene vrste bega možganov pri iskanju najbolje plačanih možnosti.

Zato poročevalka predlaga, naj se po vsej EU okrepijo specializirane, interdisciplinarne in splošne veščine in kompetence, s posebnim poudarkom na ženskah, saj so pri kibernetski varnosti na svetovni ravni v povprečju zastopane z 20 %, kar pomeni, da tu še vedno obstajajo razlike med spoloma.[4] Ženske morajo biti zastopane ter vključene v oblikovanje digitalne prihodnosti in njeno upravljanje.

Poročevalka predlaga, naj se pri razvoju veščin in kompetenc okrepi trikotnik med nacionalnimi kompetenčnimi centri, Evropskim kompetenčnim centrom za kibernetsko varnost (ECCC) in agencijo ENISA. Poveča naj se tudi vloga **industrije** pri **razvoju veščin** ter vzpostavijo partnerstva z akterji iz **akademskega sveta** in civilne družbe, pri tem pa upoštevajo regionalne izkušnje, znanja in specializacija ter zavezništva iz tretjih držav, in sicer v sodelovanju s podobno mislečimi partnerji, da bi povečali izmenjavo in zagotovili globalni pristop v pomoč državljanom, podjetjem in institucijam.

[4] Resolucija Evropskega parlamenta z dne 10. junija 2021 o spodbujanju enakosti spolov v izobraževanju in karierah na področju naravoslovja, tehnologije, inženirstva in matematike (2019/2164(INI)) https://www.europarl.europa.eu/doceo/document/TA-9-2021-0296_SL.html#def_1_22.

Poročevalka predlaga tudi sodelovanje na področju strokovnjakov in merjenja škode, ki jo kibernetski napadi povzročajo ljudem (npr. posledic napada z izsiljevalskim programjem na zdravstveni sektor).

Predlaga tudi ukrepe, s katerimi bi kot še en ukrep za zagotavljanje zaščite naših demokracij in temeljnih vrednot vključili vidik ozaveščenosti državljanov in to brez alarmizma večali, pa tudi okrepitev **kulture kibernetske varnosti**, ki varnost, vključno z varnostjo digitalnega okolja, razume kot javno dobro. Tako bomo lahko s preglednostjo, demokracijo in gotovostjo, ki jo lahko prinese razvoj vnaprejšnje zakonodaje, zagotovili model digitalne demokracije in ne model digitalnega avtoritarizma.

Poročevalka meni, da se bosta s krepitvijo **raziskav in inovacij** na področju kibernetske varnosti povečali odpornost in odprta strateška avtonomija EU. Podobno bo k temu prispevalo tudi ustvarjanje sinergij s programi za raziskave in inovacije ter obstoječimi instrumenti in institucijami ter krepitev trikotnika znanja za zapolnitev vrzeli v veščinah po vsej EU.

Poleg tega bo ta zakonodajni akt povečal odpornost EU in njenih držav članic, ne le neposredno z zakonodajo o kibernetski varnosti in kibernetski odpornosti, temveč tudi z učinkom, ki ga lahko ima na eksponentni razvoj umetne inteligence, in učinkom, ki ga lahko ima urejanje podatkov in zasebnosti podatkov na kibernetsko varnost.

Ta zakonodajni akt bo tudi pomagal izpolniti zavezo, ki je bila v **evropski deklaraciji o digitalnih pravicah in načelih za digitalno desetletje** dana v zvezi z zaščito interesov našega prebivalstva, podjetij in javnih institucij pred tveganji za kibernetsko varnost in kibernetsko kriminaliteto, vključno s kršitvami varstva podatkov in krajo identitete ali poseganjem vanjo.

Poročevalka glede na navedeno meni, da bi se moral ta predlog, skupaj z evropskim kibernetskim ščitom in mehanizmom za izredne kibernetske razmere, začeti izvajati čim prej, da bomo dobili splošen okvir in preprečili podatkovne silose glede na brezmejnost kibernetskega prostora.

PRILOGA: SUBJEKTI ALI OSEBE, OD KATERIH JE POROČEVALKA PREJELA PRISPEVEK

V skladu s členom 8 Priloge I Poslovnika poročevalka izjavlja, da je pri pripravi poročila do njegovega sprejetja v odboru prejela prispevke od naslednjih subjektov ali oseb:

Subjekt in/ali oseba
CorwdStrike
CyberPeace institute
Microsoft Corporation
Romanian National Cyber Security Directorate
ENISA
Centro Criptológico Nacional
Permanent Representation of Spain
Trellix
Palo Alto Networks Inc
Committee of the regions rapporteur

Priprava tega seznama je v izključni pristojnosti poročevalke.

27.10.2023

MNENJE ODBORA ZA ZUNANJE ZADEVE

za Odbor za industrijo, raziskave in energetiko

o predlogu uredbe Evropskega parlamenta in Sveta o določitvi ukrepov za okrepitev solidarnosti in zmogljivosti v Uniji za odkrivanje kibernetskovarnostnih groženj in incidentov ter pripravo in odzivanje nanje
(COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

Pripravljavec mnenja: Dragoş Tudorache

Predlog spremembe 1

Predlog uredbe
Uvodna izjava 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(1) Uporaba informacijskih in komunikacijskih tehnologij ter odvisnost od njih sta postali ključna vidika v vseh sektorjih gospodarske dejavnosti, saj so naše javne uprave, podjetja in državljani v različnih sektorjih in prek meja tesneje medsebojno povezani in bolj odvisni drug od drugega kot kdaj koli prej.	(1) Uporaba informacijskih in komunikacijskih tehnologij ter odvisnost od njih sta postali ključna vidika v vseh sektorjih gospodarske ***in vojaške*** dejavnosti, saj so naše javne uprave, podjetja in državljani ***ter vojaški in obrambni akterji*** v različnih sektorjih in prek meja tesneje medsebojno povezani in bolj odvisni drug od drugega kot kdaj koli prej.

Predlog spremembe 2

Predlog uredbe
Uvodna izjava 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(2) Obseg, pogostost in posledice kibernetskovarnostnih incidentov se povečujejo, vključno z napadi na	(2) Obseg, pogostost in posledice kibernetskovarnostnih incidentov se povečujejo, vključno z napadi na

oskrbovalno verigo, katerih cilj je kibernetsko vohunjenje, izsiljevalsko programje ali povzročanje motenj. Ti predstavljajo veliko grožnjo za delovanje omrežja in informacijskih sistemov. Glede na hitro razvijajočo se krajino groženj je treba zaradi nevarnosti morebitnih incidentov velikih razsežnosti, ki povzročajo velike motnje ali škodo na kritičnih infrastrukturah, povečati pripravljenost na vseh ravneh okvira Unije za kibernetsko varnost. ***Ta nevarnost presega*** rusko vojaško agresijo na Ukrajino in se ***bo verjetno nadaljevala,*** glede na številne na državni ravni usklajene, kriminalne in hektivistične akterje, vpletene v trenutne geopolitične napetosti. Taki incidenti lahko ovirajo zagotavljanje javnih storitev in opravljanje gospodarskih dejavnosti, tudi v kritičnih ali visoko kritičnih sektorjih, povzročijo znatne finančne izgube, spodkopljejo zaupanje uporabnikov, povzročijo veliko škodo gospodarstvu Unije in imajo lahko celo zdravstvene ali življenjsko nevarne posledice. Poleg tega so kibernetskovarnostni incidenti nepredvidljivi, saj pogosto nastanejo in se razvijejo v zelo kratkem času, niso omejeni na določeno geografsko območje in se zgodijo hkrati ali se takoj razširijo po številnih državah.

oskrbovalno verigo, katerih cilj je kibernetsko vohunjenje, izsiljevalsko programje ali povzročanje motenj. Ti predstavljajo veliko grožnjo za delovanje omrežja in informacijskih sistemov. Glede na hitro razvijajočo se krajino groženj je treba zaradi nevarnosti morebitnih incidentov velikih razsežnosti, ki povzročajo velike motnje ali škodo na kritičnih infrastrukturah, povečati pripravljenost na vseh ravneh okvira Unije za kibernetsko varnost. ***Te grožnje postajajo vse pomembnejše zaradi ponovnega izbruha vojne na naši celini. Tovrstne nevarnosti sežejo dosti širše od ruske vojaške agresije*** na Ukrajino in se ***bodo*** glede na številne na državni ravni usklajene, kriminalne in hektivistične akterje, vpletene v trenutne geopolitične napetosti***, verjetno nadaljevale***. Taki incidenti lahko ovirajo zagotavljanje javnih storitev in opravljanje gospodarskih dejavnosti, tudi v kritičnih ali visoko kritičnih sektorjih, povzročijo znatne finančne izgube, spodkopljejo zaupanje uporabnikov, povzročijo veliko škodo gospodarstvu ***in varnosti*** Unije in imajo lahko celo zdravstvene ali življenjsko nevarne posledice***, saj lahko ogrozijo lokalne ali nacionalne naprave, povezane z varnostjo***. Poleg tega so kibernetskovarnostni incidenti nepredvidljivi, saj pogosto nastanejo in se razvijejo v zelo kratkem času, niso omejeni na določeno geografsko območje in se zgodijo hkrati ali se takoj razširijo po številnih državah. ***Kibernetska varnost je pomembna za zaščito naših evropskih vrednot, in s tem, ko varuje našo volilno infrastrukturo in demokratične postopke pred morebitnim tujim vmešavanjem, zagotavlja delovanje naših demokracij.***

Predlog spremembe 3

Predlog uredbe
Uvodna izjava 2 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(2a) Kibernetska varnost je odločilnega pomena za zagotavljanje varnosti Unije in za preprečevanje, da bi zlonamerni državni in nedržavni akterji spodkopavali našo demokracijo, gospodarstvo in varnost. Pomembno je preprečiti razdrobljeno okolje, saj to ne bi pomenile ustreznega pristopa, zlasti če bi bili v prihodnosti soočeni z grozečimi obsežnimi kibernetskimi napadi, usmerjenimi proti več državam članicam naenkrat ali proti mednarodni kritični infrastrukturi. Zato je treba določiti organ Unije, ki bo deloval kot platforma za usklajevanje dosedanjih in tudi prihodnjih instrumentov, finančnih sredstev in mehanizmov za kibernetsko varnost.

Predlog spremembe 4

Predlog uredbe
Uvodna izjava 3

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(3) ***Okrepiti*** je treba konkurenčni položaj industrijskega in storitvenega sektorja v Uniji ***v celotnem spletnem 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[16], je treba povečati odpornost državljanov, podjetij in subjektov, ki upravljajo kritične infrastrukture, proti vse večjim kibernetskovarnostnim grožnjam, ki imajo lahko uničujoče družbene in gospodarske posledice. ***Zato*** so potrebne naložbe v infrastrukture in storitve, ki bodo podpirale hitrejše odkrivanje kibernetskovarnostnih groženj in incidentov ter odzivanje nanje, države članice pa potrebujejo pomoč pri boljši pripravi na pomembne	(3) ***V celotnem spletnem gospodarstvu*** je treba ***okrepiti*** konkurenčni položaj industrijskega in storitvenega sektorja v Uniji 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[16], je treba povečati odpornost državljanov, podjetij in subjektov, ki upravljajo kritične infrastrukture, proti vse večjim kibernetskovarnostnim grožnjam, ki imajo lahko uničujoče družbene in gospodarske posledice. ***Za to*** so potrebne naložbe v infrastrukture in storitve, ki bodo podpirale hitrejše odkrivanje kibernetskovarnostnih groženj in incidentov ter odzivanje nanje, države članice pa potrebujejo pomoč pri boljši pripravi na pomembne

kibernetskovarnostne incidente in take incidente velikih razsežnosti ter odzivanju nanje. Unija bi tudi morala povečati svoje zmogljivosti na teh področjih, zlasti kar zadeva zbiranje in analizo podatkov o kibernetskovarnostnih grožnjah in incidentih.

[16] https://futureu.europa.eu/en/

kibernetskovarnostne incidente in take incidente velikih razsežnosti ter odzivanju nanje. Unija bi tudi morala povečati svoje zmogljivosti na teh področjih, zlasti kar zadeva zbiranje in analizo podatkov o kibernetskovarnostnih grožnjah in incidentih***, ter zmožnost proaktivnega ukrepanja in odločnega odzivanja na kibernetskovarnostne grožnje in incidente***.

[16] https://futureu.europa.eu/en/

Predlog spremembe 5

Predlog uredbe
Uvodna izjava 4

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(4) Unija je že sprejela več ukrepov za zmanjšanje ranljivosti in povečanje odpornosti kritičnih infrastruktur in subjektov proti tveganjem za kibernetsko varnost, zlasti Direktivo (EU) 2022/2555 Evropskega parlamenta in Sveta[17], Priporočilo Komisije (EU) 2017/1584[18], Direktivo 2013/40/EU Evropskega parlamenta in Sveta[19] ter Uredbo (EU) 2019/881 Evropskega parlamenta in Sveta[20]. Poleg tega so države članice v priporočilu Sveta o usklajenem vseevropskem pristopu za krepitev odpornosti kritične infrastrukture pozvane, naj sprejmejo nujne in učinkovite ukrepe ter ***zvesto***, učinkovito, solidarno in usklajeno sodelujejo med seboj, s Komisijo in drugimi ustreznimi javnimi organi ter zadevnimi subjekti, da bi se okrepila odpornost kritične infrastrukture, ki se uporablja za zagotavljanje bistvenih storitev na notranjem trgu.	(4) Unija je že sprejela več ukrepov za zmanjšanje ranljivosti in povečanje odpornosti kritičnih infrastruktur in subjektov proti tveganjem za kibernetsko varnost, zlasti Direktivo (EU) 2022/2555 Evropskega parlamenta in Sveta[17], Priporočilo Komisije (EU) 2017/1584[18], Direktivo 2013/40/EU Evropskega parlamenta in Sveta[19] ter Uredbo (EU) 2019/881 Evropskega parlamenta in Sveta[20]. Poleg tega so države članice v priporočilu Sveta o usklajenem vseevropskem pristopu za krepitev odpornosti kritične infrastrukture pozvane, naj sprejmejo nujne in učinkovite ukrepe ter ***lojalno***, učinkovito***, proaktivno***, solidarno in usklajeno sodelujejo med seboj, s Komisijo in drugimi ustreznimi javnimi organi ter zadevnimi subjekti, da bi se okrepila odpornost kritične infrastrukture, ki se uporablja za zagotavljanje bistvenih storitev na notranjem trgu. ***Unija je marca 2022 odobrila in začela izvajati tudi strateški kompas za varnost in obrambo, ki je med drugim osredotočen zlasti na povečanje kibernetske varnosti in poglobitev***

mednarodnega sodelovanja na tem področju s podobno mislečimi zavezniki in demokratičnimi partnerji. Sodelovanje na področju kibernetske varnosti je bilo posebej omenjeno tudi v nedavni tretji skupni izjavi o sodelovanju med EU in Natom iz januarja 2023. V končnem poročilu o oceni projektne skupine EU-NATO je bilo priporočeno, naj se v celoti izkoristijo sinergije med EU in Natom[1], vključno z izmenjavo dobre prakse med civilnimi in vojaškimi akterji pri izvajanju ustreznih kibernetskih politik in zakonodaje.

[1] https://commission.europa.eu/document/34209534-3c59-4b01-b4f0-b2c6ee2df736_en

---

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

[18] 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).

[19] 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).

[20] 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).

---

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

[18] 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).

[19] 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).

[20] 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).

Predlog spremembe 6

Predlog uredbe
Uvodna izjava 6

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(6) V skupnem sporočilu o politiki EU za kibernetsko obrambo[22], sprejetem 10. novembra 2022, je bila napovedana pobuda EU za kibernetsko solidarnost z naslednjimi cilji: okrepitev skupnih zmogljivosti EU za odkrivanje, situacijsko zavedanje in odzivanje s spodbujanjem uvedbe infrastrukture centrov za varnostne operacije v EU, podpiranje postopne vzpostavitve kibernetskovarnostne rezerve na ravni EU s storitvami zaupanja vrednih zasebnih ponudnikov in preskušanje kritičnih subjektov glede morebitnih ranljivosti na podlagi ocen tveganja EU.	(6) V skupnem sporočilu o politiki EU za kibernetsko obrambo[22], sprejetem 10. novembra 2022, je bila napovedana pobuda EU za kibernetsko solidarnost z naslednjimi cilji: okrepitev skupnih zmogljivosti EU za odkrivanje, situacijsko zavedanje in odzivanje s spodbujanjem uvedbe infrastrukture centrov za varnostne operacije v EU, podpiranje postopne vzpostavitve kibernetskovarnostne rezerve na ravni EU s storitvami zaupanja vrednih zasebnih ponudnikov in preskušanje kritičnih subjektov glede morebitnih ranljivosti na podlagi ocen tveganja EU. ***Poleg tega sta zaradi hitro razvijajočega se okolja kibernetskih groženj in hitrega tehnološkega razvoja potrebna tudi okrepljeno civilno-vojaško usklajevanje in sodelovanje, kot je poudaril Svet v svojih sklepih o politiki EU za kibernetsko obrambo[1].***
	[1] Sklepi Sveta o oblikovanju kibernetske drže Evropske unije, ki jih je Svet odobril na seji 23. maja 2022 (9618/23).
[22] Skupno sporočilo Evropskemu parlamentu in Svetu, Politika EU za kibernetsko obrambo, JOIN(2022) ***49 final***.	[22] Skupno sporočilo Evropskemu parlamentu in Svetu, Politika EU za kibernetsko obrambo, JOIN(2022)***0049***.

Predlog spremembe 7

Predlog uredbe
Uvodna izjava 6 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(6a) Zaradi zabrisane meje med civilnimi in vojaškimi zadevami in zaradi dvojne rabe kibernetskih orodij in tehnologij je potreben celovit in celosten pristop do digitalnega sveta. V primeru velikega kibernetskega incidenta in krize, ki bi prizadela več kot eno državo članico, bi moralo biti vzpostavljeno ustrezno krizno upravljanje in vodenje. Te strukture bi morale skrbeti za izmenjavo informacij, usklajevanje in sodelovanje s strukturami Unije za zunanjo varnost in vojaško krizno upravljanje ter z organi držav članic, pristojnimi za varnost in obrambo (skupnost za kibernetsko obrambo). To bi moralo veljati tudi za operacije in misije skupne varnostne in obrambne politike, ki jih Unija izvaja za zagotavljanje miru in stabilnosti v svojem sosedstvu in širše.

Predlog spremembe 8

Predlog uredbe
Uvodna izjava 7

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(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 odzivanje na pomembne kibernetskovarnostne incidente in take incidente velikih razsežnosti. Zato bi bilo treba vzpostaviti vseevropsko infrastrukturo centrov za varnostne operacije (evropski kibernetski ščit), da bi se oblikovale in okrepile skupne zmogljivosti za odkrivanje in situacijsko zavedanje; vzpostaviti bi bilo treba mehanizem za izredne kibernetske razmere, da bi države članice podprli pri pripravi na pomembne	(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 odzivanje na pomembne kibernetskovarnostne incidente in take incidente velikih razsežnosti. Zato bi bilo treba vzpostaviti vseevropsko infrastrukturo centrov za varnostne operacije (evropski kibernetski ščit), da bi se oblikovale in okrepile skupne zmogljivosti za odkrivanje in situacijsko zavedanje; vzpostaviti bi bilo treba mehanizem za izredne kibernetske razmere, da bi države članice podprli pri pripravi na pomembne

kibernetskovarnostne incidente in take incidente velikih razsežnosti, odzivanju nanje in takojšnjem okrevanju po njih***;*** vzpostaviti bi bilo treba mehanizem za pregledovanje kibernetskovarnostnih incidentov za pregledovanje in ocenjevanje posameznih pomembnih kibernetskovarnostnih incidentov ali incidentov velikih razsežnosti. Ti ukrepi ne posegajo v člena 107 in 108 Pogodbe o delovanju Evropske unije (PDEU).	kibernetskovarnostne incidente in take incidente velikih razsežnosti, ***tudi za primer incidentov, ki bi prizadeli več kot eno državo članico,*** odzivanju nanje in takojšnjem okrevanju po njih***. Kadar je to izvedljivo in potrebno, bi moral mehanizem za izredne kibernetske razmere organizirati izmenjavo informacij in sodelovanje z obrambnimi organi držav članic, pri tem pa bi ga morale podpirati institucije, organi in agencije EU (skupnost EU za kibernetsko obrambo).*** Vzpostaviti bi bilo treba mehanizem za pregledovanje kibernetskovarnostnih incidentov za pregledovanje in ocenjevanje posameznih pomembnih kibernetskovarnostnih incidentov ali incidentov velikih razsežnosti***. Tovrstne nove strukture bi morale podpirati tudi operacije in misije SVOP EU***. Ti ukrepi ne posegajo v člena 107 in 108 Pogodbe o delovanju Evropske unije (PDEU).

Predlog spremembe 9

Predlog uredbe
Uvodna izjava 11

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(11) Za dobro finančno poslovodenje bi bilo treba določiti posebna pravila za prenos neporabljenih odobritev za prevzem obveznosti in odobritev plačil. Ob upoštevanju načela, da se proračun Unije določi vsako leto, bi bilo treba s to uredbo zaradi nepredvidljive, izjemne in posebne narave kibernetske krajine zagotoviti možnosti za prenos neporabljenih sredstev, ki presegajo tiste iz finančne uredbe, s čimer bi se čim bolj povečala zmogljivost mehanizma za izredne kibernetske razmere za podporo državam članicam pri učinkovitem boju proti kibernetskim grožnjam.	(11) Za dobro finančno poslovodenje bi bilo treba določiti posebna pravila za prenos neporabljenih odobritev za prevzem obveznosti in odobritev plačil. Ob upoštevanju načela, da se proračun Unije določi vsako leto, bi bilo treba s to uredbo zaradi nepredvidljive, izjemne in posebne narave kibernetske krajine zagotoviti možnosti za prenos neporabljenih sredstev, ki presegajo tiste iz finančne uredbe, s čimer bi se čim bolj povečala zmogljivost mehanizma za izredne kibernetske razmere za podporo državam članicam pri učinkovitem boju proti kibernetskim grožnjam. ***Tovrstna posebna pravila bi omogočila tudi dolgoročnejšo finančno podporo za skupno naročanje izjemno varnih orodij in infrastrukture naslednje***

generacije, da bi z uporabo najsodobnejše umetne inteligence in podatkovne analitike izboljšali skupne zmogljivosti za odkrivanje.

Predlog spremembe 10

Predlog uredbe
Uvodna izjava 13

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(13) Vsaka država članica bi morala imenovati javni organ na nacionalni ravni, ki bi bil zadolžen za usklajevanje dejavnosti odkrivanja kibernetskih groženj v tej državi članici. Ti nacionalni centri za varnostne operacije bi morali delovati kot referenčna točka in točka dostopa na nacionalni ravni za sodelovanje v evropskem kibernetskem ščitu ter zagotoviti, da se informacije o kibernetskih grožnjah, ki jih predložijo javni in zasebni subjekti, na nacionalni ravni izmenjujejo in zbirajo na učinkovit in poenostavljen način.	(13) Vsaka država članica bi morala imenovati javni organ na nacionalni ravni, ki bi bil zadolžen za usklajevanje dejavnosti odkrivanja kibernetskih groženj v tej državi članici. Ti nacionalni centri za varnostne operacije bi morali delovati kot referenčna točka in točka dostopa na nacionalni ravni za sodelovanje v evropskem kibernetskem ščitu ter zagotoviti, da se informacije o kibernetskih grožnjah, ki jih predložijo javni in zasebni subjekti, na nacionalni ravni izmenjujejo in zbirajo na učinkovit in poenostavljen način. ***Kadar je to izvedljivo in potrebno, bi morali centri za varnostne operacije omogočati tudi sodelovanje subjektov s področja obrambe in vzpostaviti steber obrambe v smislu upravljanja in vrste informacij, ki se izmenjujejo, kot je določeno v skupnem sporočilu o politiki EU za kibernetsko obrambo[1], ki ga je podprl tudi visoki predstavnik.*** ***[1] Skupno sporočilo Evropskemu parlamentu in Svetu, Politika EU za kibernetsko obrambo, JOIN(2022)0049.***

Predlog spremembe 11

Predlog uredbe
Uvodna izjava 14

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(14) V okviru evropskega kibernetskega	(14) V okviru evropskega kibernetskega

ščita bi bilo treba ustanoviti več čezmejnih centrov za varnostne operacije na področju kibernetske varnosti. ***Ti*** bi morali ***združevati*** nacionalne centre za varnostne operacije iz vsaj treh držav članic, da bi lahko v celoti izkoristili prednosti čezmejnega odkrivanja groženj ter izmenjave in upravljanja informacij. Splošna cilja čezmejnih centrov za varnostne operacije bi morala biti okrepitev zmogljivosti za analizo, preprečevanje in odkrivanje kibernetskovarnostnih groženj ter podpora pripravi visokokakovostnih obveščevalnih podatkov o kibernetskovarnostnih grožnjah, zlasti z izmenjavo podatkov iz različnih virov, javnih ali zasebnih, pa tudi izmenjavo in skupno uporabo najsodobnejših orodij ter skupnim razvojem zmogljivosti za odkrivanje, analizo in preprečevanje v zaupanja vrednem okolju. Ti centri bi morali zagotoviti nove dodatne zmogljivosti, ki bi temeljile na obstoječih centrih za varnostne operacije in skupinah za odzivanje na incidente na področju računalniške varnosti (v nadaljnjem besedilu: skupine CSIRT) ter drugih ustreznih akterjih in jih dopolnjevale.	ščita bi bilo treba ustanoviti več čezmejnih centrov za varnostne operacije na področju kibernetske varnosti. ***Združevati*** bi morali nacionalne centre za varnostne operacije iz vsaj treh držav članic***, vključno s stebrom obrambe***, da bi lahko v celoti izkoristili prednosti čezmejnega odkrivanja groženj ter izmenjave in upravljanja informacij. Splošna cilja čezmejnih centrov za varnostne operacije bi morala biti okrepitev zmogljivosti za analizo, preprečevanje in odkrivanje kibernetskovarnostnih groženj ter podpora pripravi visokokakovostnih obveščevalnih podatkov o kibernetskovarnostnih grožnjah, zlasti z izmenjavo podatkov iz različnih virov, javnih ali zasebnih ***ter, če je to potrebno in izvedljivo, vojaških virov z zadostnimi navodili za izmenjavo informacij***, pa tudi z izmenjavo in skupno uporabo najsodobnejših orodij ter skupnim razvojem zmogljivosti za odkrivanje, analizo in preprečevanje v zaupanja vrednem okolju. Ti centri bi morali zagotoviti nove dodatne zmogljivosti, ki bi temeljile na obstoječih centrih za varnostne operacije in skupinah za odzivanje na incidente na področju računalniške varnosti (v nadaljnjem besedilu: skupine CSIRT) ter drugih ustreznih akterjih in jih dopolnjevale.

Predlog spremembe 12

Predlog uredbe
Uvodna izjava 15

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(15) Spremljanje, odkrivanje in analizo kibernetskih groženj na nacionalni ravni običajno zagotavljajo centri za varnostne operacije, ki jih sestavljajo javni in zasebni subjekti, v povezavi s skupinami CSIRT. Poleg tega si skupine CSIRT informacije izmenjujejo v okviru mreže skupin CSIRT v skladu z Direktivo (EU) 2022/2555. Čezmejni centri za varnostne operacije bi	(15) Spremljanje, odkrivanje in analizo kibernetskih groženj na nacionalni ravni običajno zagotavljajo centri za varnostne operacije, ki jih sestavljajo javni in zasebni subjekti, v povezavi s skupinami CSIRT. Poleg tega si skupine CSIRT informacije izmenjujejo v okviru mreže skupin CSIRT v skladu z Direktivo (EU) 2022/2555. Čezmejni centri za varnostne operacije bi

morali predstavljati novo zmogljivost, ki dopolnjuje mrežo skupin CSIRT, in sicer z zbiranjem in izmenjavo podatkov javnih in zasebnih subjektov o kibernetskovarnostnih grožnjah, povečevanjem vrednosti takih podatkov s strokovno analizo ter skupno pridobljenimi infrastrukturami in najsodobnejšimi orodji ter prispevanjem k razvoju zmogljivosti in ***tehnološke suverenosti*** Unije.	morali predstavljati novo zmogljivost, ki dopolnjuje mrežo skupin CSIRT, in sicer z zbiranjem in izmenjavo podatkov javnih in zasebnih subjektov o kibernetskovarnostnih grožnjah, povečevanjem vrednosti takih podatkov s strokovno analizo ter skupno pridobljenimi infrastrukturami in najsodobnejšimi orodji ter prispevanjem k razvoju zmogljivosti in ***odpornosti*** Unije.

Predlog spremembe 13

Predlog uredbe
Uvodna izjava 16

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(16) Čezmejni centri za varnostne operacije bi morali delovati kot osrednja točka, ki bi omogočala obsežno zbiranje ustreznih podatkov in obveščevalnih podatkov o kibernetskih grožnjah ter širjenje informacij o grožnjah med velikim in raznolikim naborom akterjev (npr. skupinami za odzivanje na računalniške grožnje (v nadaljnjem besedilu: skupine CERT), skupinami CSIRT, centri za izmenjavo in analizo informacij, upravljavci kritičnih infrastruktur). Informacije, ki si jih izmenjujejo sodelujoči v čezmejnem centru za varnostne operacije, bi lahko vključevale podatke iz omrežij in senzorjev, obveščevalne podatke o grožnjah, kazalnike ogroženosti ter kontekstualizirane informacije o incidentih, grožnjah in ranljivostih. Poleg tega bi morali čezmejni centri za varnostne operacije skleniti tudi sporazume o sodelovanju z drugimi čezmejnimi centri za varnostne operacije.	(16) Čezmejni centri za varnostne operacije bi morali delovati kot osrednja točka, ki bi omogočala obsežno zbiranje ustreznih podatkov in obveščevalnih podatkov o kibernetskih grožnjah ter širjenje informacij o grožnjah med velikim in raznolikim naborom akterjev (npr. skupinami za odzivanje na računalniške grožnje (v nadaljnjem besedilu: skupine CERT), skupinami CSIRT, centri za izmenjavo in analizo informacij, upravljavci kritičnih infrastruktur ***ter skupnostjo za kibernetsko obrambo***). Informacije, ki si jih izmenjujejo sodelujoči v čezmejnem centru za varnostne operacije, bi lahko vključevale podatke iz omrežij in senzorjev, obveščevalne podatke o grožnjah, kazalnike ogroženosti ter kontekstualizirane informacije o incidentih, grožnjah in ranljivostih. Poleg tega bi morali čezmejni centri za varnostne operacije skleniti tudi sporazume o sodelovanju z drugimi čezmejnimi centri za varnostne operacije ***in operativno mrežo vojaških skupin za odzivanje na izredne računalniške razmere (MICNET), ko bo vzpostavljena***.

Predlog spremembe 14

Predlog uredbe
Uvodna izjava 17

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

seznanitvi in morda občutljivo naravo izmenjanih informacij.	ustrezno upoštevati načelo potrebe po seznanitvi in morda občutljivo naravo izmenjanih informacij.

Predlog spremembe 15

Predlog uredbe
Uvodna izjava 19

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(19) Da bi omogočili obsežno izmenjavo podatkov o kibernetskovarnostnih grožnjah iz različnih virov v zaupanja vrednem okolju, bi morali biti subjekti, ki sodelujejo v evropskem kibernetskem ščitu, opremljeni z najsodobnejšimi in izjemno varnimi orodji, opremo in infrastrukturami. 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.	(19) Da bi omogočili obsežno izmenjavo podatkov o kibernetskovarnostnih grožnjah iz različnih virov v zaupanja vrednem okolju, bi morali biti subjekti, ki sodelujejo v evropskem kibernetskem ščitu, opremljeni z najsodobnejšimi in izjemno varnimi orodji, opremo in infrastrukturami***, a je treba izključiti dobavitelje z visokim tveganjem, ki dobavljajo kritične izdelke z digitalnimi elementi***. 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. Pri uporabi umetne inteligence bi bilo treba zagotoviti človekov nadzor, poskrbeti pa bi bilo treba tudi za zadostno raven umetnointeligenčne pismenosti, potrebno podporo in pooblastila za opravljanje te funkcije.

Predlog spremembe 16

Predlog uredbe
Uvodna izjava 19 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(19a) V skladu z Uredbo [XX/XXXX (akt o kibernetski odpornosti)] bi morali subjekti, ki sodelujejo v evropskem kibernetskem ščitu, izpolnjevati zahteve iz te uredbe tudi pri vseh izdelkih, ki vsebujejo digitalne elemente. Zaradi vse večjih tveganj, ki nastanejo kot rezultat

	gospodarske odvisnosti, je treba s skupnim strateškim okvirom za gospodarsko varnost EU čim bolj zmanjšati izpostavljenost dobaviteljev z visokim tveganjem, ki dobavljajo kritične izdelke. Odvisnost od tovrstnih dobaviteljev je strateško tveganje, ki bi ga bilo treba odpravljati na ravni Unije, zlasti če katera država izvaja gospodarsko vohunjenje ali gospodarsko prisilo in njena zakonodaja zahteva poljuben dostop do vseh vrst dejavnosti ali podatkov podjetja, zlasti kadar so kritični izdelki namenjeni temu, da jih bodo uporabljali bistveni subjekti iz Direktive (EU) 2022/2555.

Predlog spremembe 17

Predlog uredbe
Uvodna izjava 20

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(20) Evropski kibernetski ščit bi moral z zbiranjem, deljenjem in izmenjavanjem podatkov okrepiti tehnološko suverenost Unije. Zbiranje visokokakovostnih pripravljenih podatkov bi moralo prispevati tudi k razvoju naprednih tehnologij umetne inteligence in podatkovne analitike. Olajšati bi ga bilo treba tako, da se evropski kibernetski ščit poveže z infrastrukturo vseevropskega visokozmogljivostnega računalništva, vzpostavljenega z Uredbo Sveta (EU) 2021/1173[25].	(20) Evropski kibernetski ščit bi moral z zbiranjem, deljenjem in izmenjavanjem podatkov okrepiti tehnološko suverenost**,** ***strateško avtonomnost, konkurenčnost in odpornost*** Unije. Zbiranje visokokakovostnih pripravljenih podatkov bi moralo prispevati tudi k razvoju naprednih tehnologij umetne inteligence in podatkovne analitike. Olajšati bi ga bilo treba tako, da se evropski kibernetski ščit poveže z infrastrukturo vseevropskega visokozmogljivostnega računalništva, vzpostavljenega z Uredbo Sveta (EU) 2021/1173[25].
[25] Uredba Sveta (EU) 2021/1173 z dne 13. julija 2021 o ustanovitvi Skupnega podjetja za evropsko visokozmogljivostno računalništvo in razveljavitvi Uredbe (EU) 2018/1488 (UL L 256, 19.7.2021, str. 3).	[25] Uredba Sveta (EU) 2021/1173 z dne 13. julija 2021 o ustanovitvi Skupnega podjetja za evropsko visokozmogljivostno računalništvo in razveljavitvi Uredbe (EU) 2018/1488 (UL L 256, 19.7.2021, str. 3).

Predlog spremembe 18

Predlog uredbe
Uvodna izjava 25

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(25) Mehanizem za izredne kibernetske razmere bi moral državam članicam zagotoviti podporo z dopolnjevanjem njihovih ukrepov in virov ter druge obstoječe možnosti podpore v primeru odziva na pomembne kibernetskovarnostne incidente in take incidente velikih razsežnosti ter takojšnjega okrevanja po njih, kot so storitve, ki jih zagotavlja Agencija Evropske unije za kibernetsko varnost (ENISA) v skladu s svojim mandatom, usklajen odziv in pomoč mreže skupin CSIRT, podpora mreže EU-CyCLONe pri ublažitvi posledic ter medsebojna pomoč med državami članicami, med drugim v okviru člena 42(7) PEU, enot za hitro odzivanje na kibernetske grožnje v okviru stalnega strukturnega sodelovanja (PESCO)***26*** in skupin za hitro odzivanje na hibridne grožnje. Obravnavati bi moral potrebo po zagotavljanju razpoložljivosti specializiranih sredstev za podporo pripravljenosti in odzivanju na kibernetskovarnostne incidente po vsej Uniji in v tretjih državah.	(25) Mehanizem za izredne kibernetske razmere bi moral državam članicam zagotoviti podporo z dopolnjevanjem njihovih ukrepov in virov ter druge obstoječe možnosti podpore v primeru odziva na pomembne kibernetskovarnostne incidente in take incidente velikih razsežnosti ter takojšnjega okrevanja po njih, kot so storitve, ki jih zagotavlja Agencija Evropske unije za kibernetsko varnost (ENISA) v skladu s svojim mandatom, usklajen odziv in pomoč mreže skupin CSIRT, podpora mreže EU-CyCLONe pri ublažitvi posledic ter medsebojna pomoč med državami članicami, med drugim v okviru člena 42(7) PEU, enot za hitro odzivanje na kibernetske grožnje v okviru stalnega strukturnega sodelovanja (PESCO)***[1], novega centra za usklajevanje na kibernetskem*** in ***informacijskem področju (CIDCC) v okviru stalnega in strukturnega sodelovanja in njegovega predlaganega naslednika – koordinacijskega centra EU za kibernetsko obrambo (EUCDCC), ter*** skupin za hitro odzivanje na hibridne grožnje. Obravnavati bi moral potrebo po zagotavljanju razpoložljivosti specializiranih sredstev za podporo pripravljenosti in odzivanju na kibernetskovarnostne incidente po vsej Uniji in v tretjih državah***, zlasti v državah kandidatkah za članstvo v EU, ki so usklajene s skupno zunanjo in varnostno politiko ter skupno varnostno in obrambno politiko, zato da se jih podpre pri krepitvi kibernetskih zmogljivosti ter da se izboljša čezmejno in regionalno sodelovanje na kibernetskem področju med temi državami kandidatkami***.

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

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

Predlog spremembe 19

Predlog uredbe
Uvodna izjava 26

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(26) Ta instrument ne posega v postopke in okvire za usklajevanje odzivanja na krize na ravni Unije, zlasti mehanizem Unije na področju civilne zaščite[27], enotno ureditev za politično odzivanje na krize[28], in Direktivo (EU) 2022/2555. Prispeva lahko k ukrepom, ki se izvajajo v okviru člena 42(7) PEU ali v primerih, opredeljenih v členu 222 PDEU, ali jih dopolnjuje. Uporabo tega instrumenta bi bilo treba ***po potrebi*** uskladiti tudi z izvajanjem ukrepov iz zbirke orodij za kibernetsko diplomacijo.	(26) Ta instrument ne posega v postopke in okvire za usklajevanje odzivanja na krize na ravni Unije, zlasti mehanizem Unije na področju civilne zaščite[27], enotno ureditev za politično odzivanje na krize[28], in Direktivo (EU) 2022/2555. Prispeva lahko k ukrepom, ki se izvajajo v okviru člena 42(7) PEU ali v primerih, opredeljenih v členu 222 PDEU, ali jih dopolnjuje Uporabo tega instrumenta bi bilo treba uskladiti tudi z izvajanjem ukrepov iz zbirke orodij za kibernetsko diplomacijo***, zlasti za poglobitev sodelovanja med skupnostjo za kibernetsko obrambo in drugimi skupnostmi na strateški, operativni in tehnični ravni, zato da se okrepijo zmogljivosti za zaščito pred kibernetskimi grožnjami iz držav zunaj EU, vključno z omejevalnimi ukrepi, ki se lahko uporabijo za preprečevanje zlonamernih kibernetskih dejavnosti in za odzivanje nanje***.

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

[27] 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).

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

20.12.2013, str. 924).

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

Predlog spremembe 20

Predlog uredbe
Uvodna izjava 28

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

takojšnje okrevanje in/ali ponovno vzpostavili delovanje bistvenih storitev.

takojšnje okrevanje in/ali ponovno vzpostavili delovanje bistvenih storitev ***z ustrezno uporabo vseh obrambnih možnosti, ki so na voljo civilnim in vojaškim skupnostim***.

Predlog spremembe 21

Predlog uredbe
Uvodna izjava 29

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(29) V okviru ukrepov pripravljenosti bi bilo treba za spodbujanje doslednega pristopa ter krepitev varnosti po vsej Uniji in na njenem notranjem trgu zagotoviti podporo za usklajeno preskušanje in ocenjevanje kibernetske varnosti subjektov, ki delujejo v visoko kritičnih sektorjih, opredeljenih v skladu z Direktivo (EU) 2022/2555. V ta namen bi morala Komisija ob podpori agencije ENISA in v sodelovanju s skupino za sodelovanje na področju varnosti omrežnih in informacijskih sistemov, ustanovljeno z Direktivo (EU) 2022/2555, redno določati ustrezne sektorje ali podsektorje, ki bi morali biti upravičeni do finančne podpore za usklajeno preskušanje na ravni Unije. Sektorje ali podsektorje bi bilo treba izbrati iz Priloge I k Direktivi (EU) 2022/2555 (v nadaljnjem besedilu: visoko kritični sektorji). Usklajeno preskušanje bi moralo temeljiti na skupnih scenarijih tveganja in metodologijah. Pri izbiri sektorjev in razvoju scenarijev tveganja bi bilo treba upoštevati ustrezne ocene tveganja in scenarije tveganja po vsej Uniji, vključno s potrebo po preprečevanju podvajanja, kot so ocena tveganja in scenariji tveganja, h katerim poziva Svet v svojih sklepih o oblikovanju kibernetske drže Evropske unije in ki jih morajo izvesti Komisija, visoki predstavnik in skupina za sodelovanje na področju varnosti omrežnih in informacijskih sistemov v sodelovanju z ustreznimi civilnimi in vojaškimi organi in	(29) V okviru ukrepov pripravljenosti bi bilo treba za spodbujanje doslednega pristopa ter krepitev varnosti po vsej Uniji in na njenem notranjem trgu zagotoviti podporo za usklajeno preskušanje in ocenjevanje kibernetske varnosti subjektov, ki delujejo v visoko kritičnih sektorjih, opredeljenih v skladu z Direktivo (EU) 2022/2555. V ta namen bi morala Komisija ob podpori agencije ENISA in v sodelovanju s skupino za sodelovanje na področju varnosti omrežnih in informacijskih sistemov, ustanovljeno z Direktivo (EU) 2022/2555, redno določati ustrezne sektorje ali podsektorje, ki bi morali biti upravičeni do finančne podpore za usklajeno preskušanje na ravni Unije. ***Po potrebi bi se morala v zagotavljanje ažurnih ocen vključiti Evropska služba za zunanje delovanje (ESZD), zlasti prek Obveščevalnega in situacijskega centra EU (INTCEN) in njegove hibridne fuzijske celice ter ob podpori direktorata za obveščevalno dejavnost Vojaškega štaba Evropske unije (EUMS) v okviru Enotne zmogljivosti za analize obveščevalnih podatkov (SIAC), in tako pomagati opredeliti*** sektorje ali podsektorje***, ki*** bi ***jih*** bilo treba izbrati iz Priloge I k Direktivi (EU) 2022/2555 (v nadaljnjem besedilu: visoko kritični sektorji). Usklajeno preskušanje bi moralo temeljiti na skupnih scenarijih tveganja in metodologijah***. Te dejavnosti bi morale imeti tudi pomembno vlogo pri***

agencijami ter vzpostavljenimi mrežami, med drugim mrežo EU-CyCLONe, pa tudi ocena tveganja komunikacijskih omrežij in infrastruktur, ki se zahteva na podlagi skupnega ministrskega poziva iz Neversa ter jo izvede skupina za sodelovanje na področju varnosti omrežnih in informacijskih sistemov ob podpori Komisije in agencije ENISA ter v sodelovanju z Organom evropskih regulatorjev za elektronske komunikacije (BEREC), usklajene ocene tveganja, ki se izvedejo v skladu s členom 22 Direktive (EU) 2022/2555, in testiranje digitalne operativne odpornosti, kot je določeno v Uredbi (EU) 2022/2554 Evropskega parlamenta in ***Sveta[29]***. Pri izbiri sektorjev bi bilo treba upoštevati tudi priporočilo Sveta o usklajenem vseevropskem pristopu za krepitev odpornosti kritične infrastrukture.

izboljševanju sodelovanja med civilnimi in vojaškimi subjekti. Zato bi morale Komisija, ESZD in ENISA pri organiziranju vaj sistematično razmisliti o tem, da bi pritegnile udeležence iz drugih kibernetskih skupnosti, kot je Evropska obrambna agencija (EDA), in drugih ustreznih subjektov. Pri izbiri sektorjev in razvoju scenarijev tveganja bi bilo treba upoštevati ustrezne ocene tveganja in scenarije tveganja po vsej Uniji, vključno s potrebo po preprečevanju podvajanja, kot so ocena tveganja in scenariji tveganja, h katerim poziva Svet v svojih sklepih o oblikovanju kibernetske drže Evropske unije in ki jih morajo izvesti Komisija, visoki predstavnik in skupina za sodelovanje na področju varnosti omrežnih in informacijskih sistemov v sodelovanju z ustreznimi civilnimi in vojaškimi organi in agencijami ter vzpostavljenimi mrežami, med drugim mrežo EU-CyCLONe, pa tudi ocena tveganja komunikacijskih omrežij in infrastruktur, ki se zahteva na podlagi skupnega ministrskega poziva iz Neversa ter jo izvede skupina za sodelovanje na področju varnosti omrežnih in informacijskih sistemov ob podpori Komisije in agencije ENISA ter v sodelovanju z Organom evropskih regulatorjev za elektronske komunikacije (BEREC), usklajene ocene tveganja, ki se izvedejo v skladu s členom 22 Direktive (EU) 2022/2555, in testiranje digitalne operativne odpornosti, kot je določeno v Uredbi (EU) 2022/2554 Evropskega parlamenta in ***Sveta[1]***. Pri izbiri sektorjev bi bilo treba upoštevati tudi priporočilo Sveta o usklajenem vseevropskem pristopu za krepitev odpornosti kritične infrastrukture.

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

[29] 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.

[29] 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.

Predlog spremembe 22

Predlog uredbe
Uvodna izjava 32

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(32) Mehanizem za izredne kibernetske razmere bi moral podpreti pomoč, ki jo države članice zagotovijo državi članici, ki jo je prizadel pomemben kibernetskovarnostni incident ali tak incident velikih razsežnosti, med drugim pomoč mreže skupin CSIRT iz člena 15 Direktive (EU) 2022/2555. Državam članicam, ki zagotovijo pomoč, bi bilo treba dovoliti, da vložijo zahtevke za kritje stroškov, povezanih s pošiljanjem strokovnih skupin v okviru medsebojne pomoči. Upravičeni stroški bi lahko vključevali potne stroške, stroške nastanitve in dnevnice strokovnjakov na področju kibernetske varnosti.	(32) Mehanizem za izredne kibernetske razmere bi moral podpreti pomoč, ki jo države članice zagotovijo državi članici, ki jo je prizadel pomemben kibernetskovarnostni incident ali tak incident velikih razsežnosti, med drugim pomoč mreže skupin CSIRT iz člena 15 Direktive (EU) 2022/2555. Državam članicam, ki zagotovijo pomoč, bi bilo treba dovoliti, da ***pri zagotavljanju pomoči tretjim državam, zlasti Ukrajini in Moldaviji,*** vložijo zahtevke za kritje stroškov, povezanih s pošiljanjem strokovnih skupin v okviru medsebojne pomoči***, s čimer se zagotovi učinkovito usklajevanje ustreznih programov in instrumentov EU, vključno z Evropskim mirovnim instrumentom, skupno zunanjo in varnostno politiko ter Instrumentom za sosedstvo ter razvojno in mednarodno sodelovanje***. Upravičeni stroški bi lahko vključevali potne stroške, stroške nastanitve in dnevnice strokovnjakov na področju kibernetske varnosti.

Predlog spremembe 23

Predlog uredbe
Uvodna izjava 33

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(33) Postopno bi bilo treba vzpostaviti kibernetskovarnostno rezervo na ravni Unije, ki bi zajemala storitve zasebnih ponudnikov upravljanih varnostnih storitev za podporo ukrepom odzivanja in takojšnjega okrevanja v primeru pomembnih kibernetskovarnostnih incidentov ali takih incidentov velikih razsežnosti. Kibernetskovarnostna rezerva EU bi morala zagotoviti razpoložljivost in pripravljenost storitev. Storitve iz kibernetskovarnostne rezerve EU bi morale biti namenjene podpori nacionalnim organom pri zagotavljanju pomoči prizadetim subjektom, ki delujejo v kritičnih ali visoko kritičnih sektorjih, kot dopolnitev njihovih ukrepov na nacionalni ravni. Države članice bi morale ob vložitvi zahtevka za podporo iz kibernetskovarnostne rezerve EU opredeliti podporo, zagotovljeno prizadetemu subjektu na nacionalni ravni, ki bi jo bilo treba upoštevati pri oceni zahtevka države članice. Storitve iz kibernetskovarnostne rezerve EU se lahko pod podobnimi pogoji uporabljajo tudi za podporo institucijam, organom, uradom in agencijam Unije.	(33) Postopno bi bilo treba vzpostaviti kibernetskovarnostno rezervo na ravni Unije, ki bi zajemala storitve zasebnih ponudnikov upravljanih varnostnih storitev za podporo ukrepom odzivanja in takojšnjega okrevanja v primeru pomembnih kibernetskovarnostnih incidentov ali takih incidentov velikih razsežnosti. Kibernetskovarnostna rezerva EU bi morala zagotoviti razpoložljivost in pripravljenost storitev. Storitve iz kibernetskovarnostne rezerve EU bi morale biti namenjene podpori nacionalnim organom pri zagotavljanju pomoči prizadetim subjektom, ki delujejo v kritičnih ali visoko kritičnih sektorjih, kot dopolnitev njihovih ukrepov na nacionalni ravni. Države članice bi morale ob vložitvi zahtevka za podporo iz kibernetskovarnostne rezerve EU opredeliti podporo, zagotovljeno prizadetemu subjektu na nacionalni ravni, ki bi jo bilo treba upoštevati pri oceni zahtevka države članice. Storitve iz kibernetskovarnostne rezerve EU se lahko pod podobnimi pogoji uporabljajo tudi za podporo institucijam, organom, uradom in agencijam Unije***, vključno z misijami SVOP***.

Predlog spremembe 24

Predlog uredbe
Uvodna izjava 34

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(34) Za izbor zasebnih ponudnikov storitev, ki bi storitve zagotavljali v okviru kibernetskovarnostne rezerve EU, je treba določiti sklop minimalnih meril, ki bi jih bilo treba vključiti v razpis za zbiranje ponudb za izbor teh ponudnikov, da se lahko izpolnijo potrebe organov držav članic in subjektov, ki delujejo v kritičnih	(34) Za izbor zasebnih ponudnikov storitev, ki bi storitve zagotavljali v okviru kibernetskovarnostne rezerve EU, je treba določiti sklop minimalnih meril, ki bi jih bilo treba vključiti v razpis za zbiranje ponudb za izbor teh ponudnikov, da se lahko izpolnijo potrebe organov držav članic in subjektov, ki delujejo v kritičnih ali visoko kritičnih sektorjih***, pri čemer je***

ali visoko kritičnih sektorjih.	***treba upoštevati tveganja, povezana s sodelovanjem ponudnikov iz strateško konkurenčnih držav, kar lahko povzroči tveganja za gospodarsko varnost ter negativno vpliva na strateško varnost Unije***.

Predlog spremembe 25

Predlog uredbe
Uvodna izjava 36

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(36) Za podporo ciljem te uredbe glede spodbujanja skupnega situacijskega zavedanja, krepitve odpornosti Unije ter omogočanja učinkovitega odziva na pomembne kibernetskovarnostne incidente in take incidente velikih razsežnosti bi bilo treba mreži EU-CyCLONe, mreži skupin CSIRT ali Komisiji omogočiti, da agencijo ENISA zaprosijo, naj pregleda in oceni grožnje, ranljivosti in blažitvene ukrepe v zvezi s posameznim pomembnim kibernetskovarnostnim incidentom ali takim incidentom velikih razsežnosti. ***Po zaključku pregleda*** in ***ocene incidenta*** bi morala agencija ENISA v sodelovanju z ustreznimi deležniki, vključno s predstavniki iz zasebnega sektorja, držav članic, Komisije in drugih ustreznih institucij, organov, uradov in agencij EU, pripraviti poročilo o pregledu incidenta. Kar zadeva zasebni sektor, agencija ENISA razvija kanale za izmenjavo informacij s specializiranimi ponudniki, vključno s ponudniki upravljanih varnostnih rešitev in prodajalci, da bi prispevala k svojemu poslanstvu doseganja visoke skupne ravni kibernetske varnosti po vsej Uniji. Cilj poročila o pregledu posameznih incidentov, ki temelji na sodelovanju z deležniki, vključno z zasebnim sektorjem, bi moral biti ocena vzrokov, posledic in blažitev incidenta po njegovem nastanku. Posebno pozornost bi bilo treba nameniti prispevku in	(36) Za podporo ciljem te uredbe glede spodbujanja skupnega situacijskega zavedanja, krepitve odpornosti Unije ter omogočanja učinkovitega odziva na pomembne kibernetskovarnostne incidente in take incidente velikih razsežnosti bi bilo treba mreži EU-CyCLONe, mreži skupin CSIRT ali Komisiji omogočiti, da agencijo ENISA zaprosijo, naj pregleda in oceni grožnje, ranljivosti in blažitvene ukrepe v zvezi s posameznim pomembnim kibernetskovarnostnim incidentom ali takim incidentom velikih razsežnosti. ***Da bi razvili sistem varne povezljivosti, ki bi temeljil na evropski infrastrukturi za kvantne komunikacije (EuroQCI) in satelitskih vladnih komunikacijah Evropske unije (GOVSATCOM), zlasti pa, da bi začeli izvajati vodilni program Galileo/GNSS za uporabnike na področju obrambe, bi morali pri morebitnem prihodnjem razvoju vedno upoštevati možnost tako imenovane „hipervojne“, kjer se hitrost*** in ***izpopolnjenost kvantnega računalništva združuje z visoko avtonomnimi vojaškimi sistemi,*** bi morala agencija ENISA v sodelovanju z ustreznimi deležniki, vključno s predstavniki iz zasebnega sektorja, držav članic, Komisije in drugih ustreznih institucij, organov, uradov in agencij EU, ***po zaključku pregleda in oceni incidenta*** pripraviti poročilo o pregledu incidenta. Kar zadeva zasebni sektor, agencija

spoznanjem, ki si jih izmenjujejo ponudniki upravljanih varnostnih storitev, ki izpolnjujejo pogoje največje poklicne integritete, nepristranskosti in potrebnega tehničnega strokovnega znanja, kot se zahtevajo s to uredbo. Poročilo bi bilo treba predložiti mreži EU-CyCLONe, mreži skupin CSIRT in Komisiji, ***pri čemer*** bi ga ***te*** morale upoštevati pri svojem delu. Če je incident povezan s tretjo državo, ***bo*** Komisija poročilo ***poslala*** tudi visokemu predstavniku.

ENISA razvija kanale za izmenjavo informacij s specializiranimi ponudniki, vključno s ponudniki upravljanih varnostnih rešitev in prodajalci, da bi prispevala k svojemu poslanstvu doseganja visoke skupne ravni kibernetske varnosti po vsej Uniji. Cilj poročila o pregledu posameznih incidentov, ki temelji na sodelovanju z deležniki, vključno z zasebnim sektorjem, bi moral biti ocena vzrokov, posledic in blažitev incidenta po njegovem nastanku. Posebno pozornost bi bilo treba nameniti prispevku in spoznanjem, ki si jih izmenjujejo ponudniki upravljanih varnostnih storitev, ki izpolnjujejo pogoje največje poklicne integritete, nepristranskosti in potrebnega tehničnega strokovnega znanja, kot se zahtevajo s to uredbo. Poročilo bi bilo treba predložiti mreži EU-CyCLONe, mreži skupin CSIRT in Komisiji, ***te pa*** bi ga morale upoštevati pri svojem delu. Če je incident povezan s tretjo državo, Komisija poročilo ***pošlje*** tudi visokemu predstavniku***, Evropski službi za zunanje delovanje in prek ustreznih štabov še misijam SVOP v državah, ki jih dani incident prizadene***.

Predlog spremembe 26

Predlog uredbe
Uvodna izjava 37

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(37) Ob upoštevanju nepredvidljive narave kibernetskih napadov in dejstva, da ti pogosto niso omejeni na določeno geografsko območje in da predstavljajo veliko tveganje prelivanja, krepitev odpornosti sosednjih držav in njihove zmogljivosti za učinkovito odzivanje na pomembne kibernetskovarnostne incidente in take incidente velikih razsežnosti prispeva k zaščiti Unije kot celote. Zato ***lahko*** podporo iz kibernetskovarnostne rezerve EU ***prejmejo*** tretje države,	(37) Ob upoštevanju nepredvidljive narave kibernetskih napadov in dejstva, da ti pogosto niso omejeni na določeno geografsko območje in da predstavljajo veliko tveganje prelivanja, krepitev odpornosti sosednjih držav***, zlasti Ukrajine in Moldavije,*** in njihove zmogljivosti za učinkovito odzivanje na pomembne kibernetskovarnostne incidente in take incidente velikih razsežnosti prispeva k zaščiti Unije kot celote. Zato ***bi morale*** podporo iz kibernetskovarnostne rezerve

pridružene programu Digitalna Evropa, ***če*** je ***to določeno v ustreznih sporazumih o pridružitvi programu Digitalna Evropa***. Unija bi morala financiranje za pridružene tretje države podpreti v okviru ustreznih partnerstev in instrumentov financiranja za te države. Podpora bi morala zajemati storitve na področju odzivanja na pomembne kibernetskovarnostne incidente ali take incidente velikih razsežnosti in takojšnjega okrevanja po njih. Pri zagotavljanju podpore tretjim državam, pridruženim programu Digitalna Evropa, bi se morali uporabljati pogoji, določeni za kibernetskovarnostno rezervo EU in zaupanja vredne ponudnike v tej uredbi.	EU ***prejeti tudi*** tretje države, pridružene programu Digitalna Evropa***. Podpora bi morala prav tako veljati za tiste tretje države***, ***v katere je napotena misija SVOP z izrecnim mandatom za povečanje odpornosti zoper hibridne grožnje, vključno s kibernetskimi, ali za katere*** je ***bil sprejet ukrep pomoči iz Evropskega mirovnega instrumenta za povečanje kibernetske odpornosti države***. Unija bi morala financiranje za pridružene tretje države podpreti v okviru ustreznih partnerstev in instrumentov financiranja za te države. Podpora bi morala zajemati storitve na področju odzivanja na pomembne kibernetskovarnostne incidente ali take incidente velikih razsežnosti in takojšnjega okrevanja po njih. Pri zagotavljanju podpore tretjim državam, pridruženim programu Digitalna Evropa, bi se morali uporabljati pogoji, določeni za kibernetskovarnostno rezervo EU in zaupanja vredne ponudnike v tej uredbi.

Predlog spremembe 27

Predlog uredbe
Člen 1 – odstavek 1 – točka c

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(c) vzpostavitvijo evropskega mehanizma za pregledovanje kibernetskovarnostnih incidentov za pregledovanje in ocenjevanje pomembnih ***incidentov*** ali incidentov ***velikih razsežnosti***.	(c) vzpostavitvijo evropskega mehanizma za pregledovanje kibernetskovarnostnih incidentov za pregledovanje in ocenjevanje pomembnih ali ***velikih*** incidentov ***ali groženj***.

Predlog spremembe 28

Predlog uredbe
Člen 1 – odstavek 2 – točka a

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(a) okrepiti skupno odkrivanje kibernetskih groženj in incidentov v Uniji	(a) okrepiti skupno odkrivanje kibernetskih groženj in incidentov v Uniji

ter situacijsko zavedanje o njih, da se tako okrepi konkurenčni položaj industrijskega in storitvenega sektorja v Uniji v celotnem spletnem gospodarstvu ter prispeva k tehnološki ***suverenosti*** Unije na področju kibernetske varnosti;	ter situacijsko zavedanje o njih, da se tako okrepi konkurenčni položaj industrijskega in storitvenega sektorja v Uniji v celotnem spletnem gospodarstvu ter prispeva k tehnološki ***odpornosti*** Unije na področju kibernetske varnosti;

Predlog spremembe 29

Predlog uredbe
Člen 1 – odstavek 2 – točka b

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(b) okrepiti pripravljenost subjektov, ki delujejo v kritičnih in visoko kritičnih sektorjih po vsej Uniji, ter solidarnost z razvijanjem skupnih zmogljivosti za odzivanje na pomembne kibernetskovarnostne incidente ali take incidente velikih razsežnosti, med drugim z omogočanjem podpore Unije pri odzivanju na kibernetskovarnostne incidente tretjim državam, pridruženim programu Digitalna Evropa***;***	(b) okrepiti pripravljenost subjektov, ki delujejo v kritičnih in visoko kritičnih sektorjih po vsej Uniji, ter solidarnost z razvijanjem skupnih zmogljivosti za odzivanje na pomembne kibernetskovarnostne incidente ali take incidente velikih razsežnosti, med drugim z omogočanjem podpore Unije pri odzivanju na kibernetskovarnostne incidente tretjim državam, pridruženim programu Digitalna Evropa***, ali tretjim državam, ki so kandidatke za pristop k Uniji in ne delujejo v nasprotju z varnostnimi in obrambnimi interesi Unije in njenih držav članic, kot je določeno v okviru SZVP na podlagi naslova V PEU. Države članice bi morale razmisliti o programu aktivne kibernetske obrambe, ki bi bil del njihove nacionalne strategije za kibernetsko varnost in bi zajemal tudi redno skupno urjenje med državami članicami in v mednarodnih organizacijah. Program bi moral omogočati, da bi se grožnje odkrivale, preiskovale, analizirale in blažile sinhronizirano in v realnem času.***

Predlog spremembe 30

Predlog uredbe
Člen 1 – odstavek 2 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	2a. zmanjšati sistemska kibernetskovarnostna tveganja, ki lahko nastanejo zaradi odvisnosti od kritične opreme iz držav, ki bi lahko delovale v nasprotju z varnostnimi in obrambnimi interesi Unije in njenih držav članic, kot so določeni v okviru SZVP na podlagi naslova V PEU.

Predlog spremembe 31

Predlog uredbe
Člen 2 – odstavek 2 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	„skupnost za kibernetsko obrambo“ tvorijo obrambni organi držav članic, podpirajo pa jih institucije, organi in agencije EU, kot je določeno v Skupnem sporočilu o politiki EU za kibernetsko obrambo[1];
	[1] Skupno sporočilo Evropskemu parlamentu in Svetu, Politika EU za kibernetsko obrambo, JOIN(2022)0049.

Predlog spremembe 32

Predlog uredbe
Člen 3 – odstavek 2 – pododstavek 1 – točka b a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(ba) pomaga pri posodobitvi celotnih sistemov kibernetske obrambe, in sicer poveča kakovost zmogljivosti kibernetske obrambe z uvajanjem umetnointeligenčnih sistemov ter pospeši izmenjavo informacij med nacionalnimi in čezmejnimi centri za varnostne operacije;

Predlog spremembe 33

Predlog uredbe
Člen 3 – odstavek 2 – pododstavek 1 – točka d a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(da) pregleda in oceni kritične kibernetskovarnostne tehnologije in opremo, ki jih centri za varnostne operacije uporabljajo pri odzivanju na kibernetskovarnostne incidente in zaradi katerih bi utegnilo priti do sistemskih tveganj, ker jih obvladujejo ponudniki z visokim tveganjem iz držav, ki bi lahko delovale v nasprotju z varnostnimi in obrambnimi interesi Unije in njenih držav članic, kot so določeni v okviru SZVP na podlagi naslova V PEU.

Predlog spremembe 34

Predlog uredbe
Člen 4 – odstavek 1 – pododstavek 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
Lahko deluje kot referenčna točka in točka dostopa do drugih javnih in zasebnih organizacij na nacionalni ravni za zbiranje in analiziranje informacij o kibernetskovarnostnih grožnjah in incidentih ter prispevanje k čezmejnim centrom za varnostne operacije. Opremljen je z najsodobnejšimi tehnologijami, ki so zmožne odkrivanja, združevanja in analiziranja podatkov v zvezi s kibernetskovarnostnimi grožnjami in incidenti.	Deluje ***lahko*** kot referenčna točka in točka dostopa do drugih javnih in zasebnih***, po potrebi pa tudi vojaških*** organizacij na nacionalni ravni za zbiranje in analiziranje informacij o kibernetskovarnostnih grožnjah in incidentih ter prispevanje k čezmejnim centrom za varnostne operacije. Opremljen je z najsodobnejšimi tehnologijami, ki so zmožne odkrivanja, združevanja in analiziranja podatkov v zvezi s kibernetskovarnostnimi grožnjami in incidenti.

Predlog spremembe 35

Predlog uredbe
Člen 4 – odstavek 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. 2. Evropski kompetenčni center za kibernetsko varnost (v nadaljnjem besedilu: ECCC) na podlagi razpisa za prijavo interesa izbere nacionalne centre za varnostne operacije, ki z njim sodelujejo pri skupnem javnem naročanju orodij in infrastruktur. Center ECCC lahko izbranim nacionalnim centrom za varnostne operacije dodeli nepovratna sredstva za financiranje delovanja teh orodij in infrastruktur. Finančni prispevek Unije krije do 50 % stroškov pridobitve orodij in infrastruktur ter do 50 % operativnih stroškov, preostale stroške pa krije država članica. Pred začetkom postopka za pridobitev orodij in infrastruktur center ECCC in nacionalni center za varnostne operacije skleneta sporazum o gostiteljstvu in uporabi, ki ureja uporabo orodij in infrastruktur.	2. 2. Evropski kompetenčni center za kibernetsko varnost (v nadaljnjem besedilu: ECCC) na podlagi razpisa za prijavo interesa izbere nacionalne centre za varnostne operacije, ki z njim sodelujejo pri skupnem javnem naročanju orodij in infrastruktur. Center ECCC lahko izbranim nacionalnim centrom za varnostne operacije dodeli nepovratna sredstva za financiranje delovanja teh orodij in infrastruktu ***pod strogim pogojem, da ta orodja in infrastrukturo zagotavljajo zaupanja vredni ponudniki v skladu s členom 16***. Finančni prispevek Unije krije do 50 % stroškov pridobitve orodij in infrastruktur ter do 50 % operativnih stroškov, preostale stroške pa krije država članica. Pred začetkom postopka za pridobitev orodij in infrastruktur center ECCC in nacionalni center za varnostne operacije skleneta sporazum o gostiteljstvu in uporabi, ki ureja uporabo orodij in infrastruktur.

Predlog spremembe 36

Predlog uredbe
Člen 5 – odstavek 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. Center ECCC na podlagi razpisa za prijavo interesa izbere gostiteljski konzorcij, ki z njim sodeluje pri skupnem javnem naročanju orodij in infrastruktur. Gostiteljskemu konzorciju lahko dodeli nepovratna sredstva za financiranje delovanja orodij in infrastruktur. Finančni prispevek Unije krije do 75 % stroškov pridobitve orodij in infrastruktur ter do 50 % operativnih stroškov, preostale stroške pa krije gostiteljski konzorcij. Pred začetkom postopka za pridobitev orodij in infrastruktur center ECCC in gostiteljski konzorcij skleneta sporazum o gostiteljstvu	2. Center ECCC na podlagi razpisa za prijavo interesa izbere gostiteljski konzorcij, ki z njim sodeluje pri skupnem javnem naročanju orodij in infrastruktur. Gostiteljskemu konzorciju lahko dodeli nepovratna sredstva za financiranje delovanja orodij in infrastruktur***, pod strogim pogojem, da ta orodja in infrastrukturo zagotavljajo zaupanja vredni ponudniki v skladu s členom 16***. Finančni prispevek Unije krije do 75 % stroškov pridobitve orodij in infrastruktur ter do 50 % operativnih stroškov, preostale stroške pa krije gostiteljski konzorcij. Pred

in uporabi, ki ureja uporabo orodij in infrastruktur.	začetkom postopka za pridobitev orodij in infrastruktur center ECCC in gostiteljski konzorcij skleneta sporazum o gostiteljstvu in uporabi, ki ureja uporabo orodij in infrastruktur.

Predlog spremembe 37

Predlog uredbe
Člen 5 – odstavek 2 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	2a. Samodejno se izključi vsaka infrastruktura ali ponudnik, ki izvira iz tretje države z visokim tveganjem.

Predlog spremembe 38

Predlog uredbe
Člen 6 – odstavek 1 – točka b a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(ba) neposredno podpira povečevanje vojaških in obrambnih zmogljivosti sodelujočih članic ali preprečuje neposredno in takojšnjo grožnjo njihovi varnosti. Ker lahko izkoriščanje šibkih točk v obrambnem sektorju povzroči hude motnje in škodo, so za kibernetsko varnost obrambne industrije potrebni posebni ukrepi, s katerimi se zagotovi varnost dobavnih verig, zlasti subjektov, ki so nižje v dobavnih verigah in ne potrebujejo dostopa do tajnih podatkov, bi pa lahko predstavljali resno tveganje za ves sektor. Posebno pozornost bi bilo treba nameniti posledicam vsake morebitne kršitve in vsaki morebitni grozeči manipulaciji omrežnih podatkov, zaradi katerih ključna obrambna sredstva nenadoma ne bi bila več uporabna ali s čimer bi bilo mogoče celo nevtralizirati operativne sisteme, tako da bi jih bilo mogoče prevzeti ali ugrabiti.

Predlog spremembe 39

Predlog uredbe
Člen 6 – odstavek 1 – točka b a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(bb) podpira krepitev obrambnih zmogljivosti sodelujočih držav oziroma onemogoča neposredne grožnje njihovi varnosti, pomaga zagotavljati varnost dobavnih verig, zlasti subjektov, ki so nižje v dobavnih verigah in ne potrebujejo dostopa do tajnih podatkov, bi pa lahko bili vektor resnih tveganj za ves sektor.

Predlog spremembe 40

Predlog uredbe
Člen 7 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. Kadar čezmejni centri za varnostne operacije pridobijo informacije v zvezi z morebitnim ali tekočim kibernetskovarnostnim incidentom velikih razsežnosti, ustrezne informacije nemudoma zagotovijo mreži EU-CyCLONe, mreži skupin CSIRT in Komisiji glede na njihove vloge pri kriznem upravljanju v skladu z Direktivo (EU) 2022/2555.	1. Kadar čezmejni centri za varnostne operacije pridobijo informacije v zvezi z morebitnim ali tekočim kibernetskovarnostnim incidentom velikih razsežnosti, ustrezne informacije nemudoma zagotovijo mreži EU-CyCLONe, mreži skupin CSIRT in Komisiji***, vključno z visokim predstavnikom in Evropsko službo za zunanje delovanje, kadar gre za tretjo državo,*** glede na njihove vloge pri kriznem upravljanju v skladu z Direktivo (EU) 2022/2555.

Predlog spremembe 41

Predlog uredbe
Člen 8 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. Države članice, ki sodelujejo v evropskem kibernetskem ščitu, zagotovijo visoko raven varnosti podatkov in fizične	1. Države članice, ki sodelujejo v evropskem kibernetskem ščitu, zagotovijo visoko raven varnosti podatkov in fizične

varnosti infrastrukture evropskega kibernetskega ščita ter ustrezno upravljanje in nadzor infrastrukture, tako da je ta zaščitena pred grožnjami ter da sta zagotovljeni njena varnost in varnost sistemov, med drugim varnost podatkov, ki se izmenjujejo prek infrastrukture.

varnosti infrastrukture evropskega kibernetskega ščita ter ustrezno upravljanje in nadzor infrastrukture, tako da je ta zaščitena pred grožnjami ter da sta zagotovljeni njena varnost in varnost sistemov, ***zato da se zmanjša tveganje in spodbuja tehnološka prednost EU v kritičnih sektorjih,*** med drugim ***z ukrepi za omejitev ali izključitev dobaviteljev z visokim tveganjem, ter zato, da se zaščiti*** varnost podatkov, ki se izmenjujejo prek infrastrukture.

Predlog spremembe 42

Predlog uredbe
Člen 8 – odstavek 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. Države članice, ki sodelujejo v evropskem kibernetskem ščitu, zagotovijo, da izmenjava informacij v okviru evropskega kibernetskega ščita s subjekti, ki niso javni organi držav članic, nima negativnih posledic za varnostne interese Unije.	2. Države članice, ki sodelujejo v evropskem kibernetskem ščitu, zagotovijo, da izmenjava informacij v okviru evropskega kibernetskega ščita s subjekti, ki niso javni organi držav članic, nima negativnih posledic za varnostne interese Unije ***ter da je vsaka izmenjava informacij s ponudniki storitev z visokim tveganjem omejena in ne posega v varnostne in strateške interese Unije***.

Predlog spremembe 43

Predlog uredbe
Člen 8 – odstavek 3

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
3. Komisija lahko sprejme izvedbene akte, s katerimi določi tehnične zahteve za države članice glede izpolnjevanja njihove obveznosti iz odstavkov 1 in 2. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 21(2) te uredbe. Pri tem Komisija ob podpori visokega predstavnika upošteva ustrezne varnostne standarde na ravni obrambe, da	3. Komisija lahko sprejme izvedbene akte, s katerimi določi tehnične zahteve za države članice glede izpolnjevanja njihove obveznosti iz odstavkov 1 in 2. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 21(2) te uredbe. Pri tem Komisija ob podpori visokega predstavnika upošteva ustrezne varnostne standarde na ravni obrambe, da

bi se olajšalo sodelovanje z vojaškimi akterji.	bi se olajšalo sodelovanje z vojaškimi akterji ***in bi se ob tem uporabljal celoten nabor obrambnih možnosti, ki so na voljo civilnim in vojaškim skupnostim za splošno varnost in obrambo EU, ter o tem obvesti Evropski parlament***.

Predlog spremembe 44

Predlog uredbe
Člen 9 – odstavek 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. Ukrepi za izvajanje mehanizma za izredne kibernetske razmere se podprejo s sredstvi iz programa Digitalna Evropa***,*** ***izvajajo pa se*** v skladu z Uredbo (EU) 2021/694 in zlasti specifičnim ciljem 3 Uredbe.	2. Ukrepi za izvajanje mehanizma za izredne kibernetske razmere se podprejo s sredstvi iz programa Digitalna Evropa ***in se izvajajo*** v skladu z Uredbo (EU) 2021/694 in zlasti specifičnim ciljem 3 Uredbe***, medtem ko se pri zagotavljanju ukrepov pomoči tretjim državam, zlasti Ukrajini in Moldaviji, ukrepi podprejo tudi iz Evropskega mirovnega instrument***.

Predlog spremembe 45

Predlog uredbe
Člen 10 – odstavek 1 – točka a

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(a) ukrepe pripravljenosti, vključno z usklajenim preskušanjem pripravljenosti subjektov, ki delujejo v visoko kritičnih sektorjih po vsej Uniji;	(a) ukrepe pripravljenosti, vključno z usklajenim preskušanjem pripravljenosti subjektov, ki delujejo v visoko kritičnih sektorjih po vsej Uniji***, kot so javna infrastruktura, volilna infrastruktura, promet, zdravstvo, finančne storitve, telekomunikacije, oskrba s hrano in varnost;***

Predlog spremembe 46

Predlog uredbe
Člen 10 – odstavek 1 – točka c

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(c) ukrepe medsebojne pomoči, ki vključujejo pomoč, ki jo nacionalni organi ene države članice zagotovijo drugi državi članici, zlasti kot je določeno v členu 11(3), točka (f), Direktive (EU) 2022/2555**.**	(c) ukrepe medsebojne pomoči, ki vključujejo pomoč, ki jo nacionalni organi ene države članice zagotovijo drugi državi članici, zlasti kot je določeno v členu 11(3), točka (f), Direktive (EU) 2022/2555***, ter v okviru člena 42(7) PEU in člena 222 PDEU;***

Predlog spremembe 47

Predlog uredbe
Člen 10 – odstavek 1 – točka c a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(ca) nadomestitev in postopna opustitev kritične infrastrukture, ki prihaja od dobaviteljev z visokim tveganjem, ki bi lahko delovali v nasprotju z varnostnimi in obrambnimi interesi Unije in njenih držav članic, kot so določeni v okviru SZVP na podlagi naslova V PEU.

Predlog spremembe 48

Predlog uredbe
Člen 11 – odstavek 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. Skupina za sodelovanje na področju varnosti omrežnih in informacijskih sistemov v sodelovanju s Komisijo, agencijo ENISA in ***visokim predstavnikom*** razvije skupne scenarije tveganja in metodologije za usklajeno preskušanje.	2. Skupina za sodelovanje na področju varnosti omrežnih in informacijskih sistemov v sodelovanju s Komisijo, agencijo ENISA***, visokim predstavnikom, ESZD*** in ***po potrebi Evropsko obrambno agencijo*** razvije skupne scenarije tveganja in metodologije za usklajeno preskušanje.

Predlog spremembe 49

Predlog uredbe
Člen 12 – odstavek 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. Kibernetskovarnostno rezervo EU sestavljajo storitve za odzivanje na incidente, ki jih zagotovijo zaupanja vredni ponudniki, izbrani v skladu z merili iz člena 16. Rezerva vključuje storitve, k zagotavljanju katerih se ponudniki zavežejo vnaprej. Storitve se lahko uporabljajo v vseh državah članicah.	2. Kibernetskovarnostno rezervo EU sestavljajo storitve za odzivanje na incidente, ki jih zagotovijo zaupanja vredni ponudniki, izbrani v skladu z merili iz člena 16. Rezerva vključuje storitve, k zagotavljanju katerih se ponudniki zavežejo vnaprej. Storitve se lahko uporabljajo v vseh državah članicah ***in tretjih državah, ki izpolnjujejo veljavne zahteve te uredbe***.

Predlog spremembe 50

Predlog uredbe
Člen 12 – odstavek 3 – točka b

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(b) institucije, organi, uradi in agencije Unije.	(b) institucije, organi, uradi in agencije Unije***, vključno z misijami SVOP***.

Predlog spremembe 51

Predlog uredbe
Člen 12 – odstavek 4

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
4. Uporabniki iz odstavka 3, točka (a), storitve iz kibernetskovarnostne rezerve EU uporabljajo za odzivanje na pomembne incidente ali incidente velikih razsežnosti, ki prizadenejo subjekte, ki delujejo v kritičnih ali visoko kritičnih sektorjih, ali za podporo odzivanju ***nanje*** in takojšnjemu okrevanju po njih.	4. Uporabniki iz odstavka 3, točka (a), storitve iz kibernetskovarnostne rezerve EU uporabljajo za odzivanje na pomembne incidente ali incidente velikih razsežnosti, ki prizadenejo subjekte, ki delujejo v kritičnih ali visoko kritičnih sektorjih, ***kot so javna infrastruktura, volilna infrastruktura, promet, zdravstvo, finančne storitve, telekomunikacije, oskrba s hrano in varnost,*** ali za podporo odzivanju ***na tovrstne incidente*** in takojšnjemu okrevanju po njih.

Predlog spremembe 52

Predlog uredbe
Člen 12 – odstavek 5

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
5. Za izvajanje kibernetskovarnostne rezerve EU je v celoti odgovorna Komisija. Komisija določi prednostne naloge in razvoj kibernetskovarnostne rezerve EU 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**.**	5. Za izvajanje kibernetskovarnostne rezerve EU je v celoti odgovorna Komisija. Komisija določi prednostne naloge in razvoj kibernetskovarnostne rezerve EU 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***, programi*** in ***cilji*** Unije***, zlasti s strateškim ciljem zmanjšanja odvisnosti od dobaviteljev z visokim tveganjem, ki bi lahko delovali v nasprotju z varnostnimi in obrambnimi interesi Unije in njenih držav članic, kot so določeni v okviru SZVP na podlagi naslova V PEU;***

Predlog spremembe 53

Predlog uredbe
Člen 12 – odstavek 7

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
7. Da bi agencija ENISA podprla Komisijo pri vzpostavitvi kibernetskovarnostne rezerve EU, po posvetovanju z državami članicami in Komisijo pripravi pregled potrebnih storitev. Po posvetovanju s Komisijo pripravi podoben pregled za opredelitev potreb tretjih držav, upravičenih do podpore iz kibernetskovarnostne rezerve EU v skladu s členom 17. Komisija se po potrebi posvetuje z visokim predstavnikom.	7. Da bi agencija ENISA podprla Komisijo pri vzpostavitvi kibernetskovarnostne rezerve EU, po posvetovanju z državami članicami in Komisijo pripravi pregled potrebnih storitev. Po posvetovanju s Komisijo ***in ob podpori ESZD*** pripravi podoben pregled za opredelitev potreb tretjih držav, upravičenih do podpore iz kibernetskovarnostne rezerve EU v skladu s členom 17. Komisija se po potrebi posvetuje z visokim predstavnikom.

Predlog spremembe 54

Predlog uredbe
Člen 14 – odstavek 2 – točka a a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(aa) vpliv incidenta na varnost in obrambo Unije;

Predlog spremembe 55

Predlog uredbe
Člen 15 – odstavek 3

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
3. Na podlagi posvetovanja z visokim predstavnikom lahko podpora v okviru mehanizma za izredne kibernetske razmere dopolnjuje pomoč, zagotovljeno v okviru skupne zunanje in varnostne politike ter skupne varnostne in obrambne politike, med drugim prek enot za hitro odzivanje na kibernetske grožnje. Prav tako lahko dopolnjuje pomoč, ki jo ena država članica zagotavlja drugi državi članici, ali k njej prispeva v okviru člena 42(7) Pogodbe o Evropski uniji.	3. Na podlagi posvetovanja z visokim predstavnikom lahko podpora v okviru mehanizma za izredne kibernetske razmere dopolnjuje pomoč, zagotovljeno v okviru skupne zunanje in varnostne politike ter skupne varnostne in obrambne politike, med drugim prek enot za hitro odzivanje na kibernetske grožnje***, da bi bolje podprli države članice EU, misije in operacije SVOP ter tretje države, usklajene s skupno zunanjo in varnostno politiko ter skupno varnostno in obrambno politiko EU, zlasti Ukrajino in Moldavijo, pri njihovih prizadevanjih za krepitev zmogljivosti kibernetske obrambe***. Prav tako lahko dopolnjuje pomoč, ki jo ena država članica zagotavlja drugi državi članici, ali k njej prispeva v okviru člena 42(7) Pogodbe o Evropski uniji.

Predlog spremembe 56

Predlog uredbe
Člen 16 – odstavek 2 – točka b a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(aa) ponudnik dokaže, da njegove strukture odločanja in upravljanja niso pod neprimernim vplivom vlad držav, ki bi

lahko delovale v nasprotju z varnostnimi in obrambnimi interesi Unije in njenih držav članic, kot so določeni v okviru SZVP na podlagi naslova V PEU;

Predlog spremembe 57

Predlog uredbe
Člen 16 – odstavek 2 – točka f

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(f) ponudnik ***je opremljen s*** tehnično strojno in programsko opremo, potrebno za podporo zahtevani storitvi;	(f) ponudnik ***ima*** tehnično strojno in programsko opremo, potrebno za podporo zahtevani storitvi***, in izpolnjuje zahteve iz člena X Uredbe XX/XXXX (akt o kibernetski odpornosti)***;

Predlog spremembe 58

Predlog uredbe
Člen 16 – odstavek 2 – točka j a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(ja) ponudniki, ki izvirajo iz tretjih držav z visokim tveganjem, niso sprejemljivi;

Predlog spremembe 59

Predlog uredbe
Člen 16 – odstavek 2 – točka j b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(jb) ponudnik po možnosti tesno sodeluje z ustreznimi malimi in srednjimi podjetji;

Predlog spremembe 60

Predlog uredbe
Člen 17 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. Tretje države lahko zaprosijo za podporo iz kibernetskovarnostne rezerve EU, če ***je to določeno v pridružitvenih sporazumih, sklenjenih v zvezi z njihovim sodelovanjem v programu Digitalna Evropa.***	1. Tretje države lahko zaprosijo za podporo iz kibernetskovarnostne rezerve EU, če***:***
	(a) je to določeno v pridružitvenih sporazumih, sklenjenih v zvezi z njihovim sodelovanjem v programu Digitalna Evropa;
	(b) gre za tretje države, v katere je napotena misija SVOP z izrecnim mandatom za krepitev odpornosti proti hibridnim grožnjam, tudi kibernetskim, ali če je bil sprejet ukrep pomoči iz Evropskega mirovnega instrumenta za povečanje kibernetske odpornosti dane države.

Predlog spremembe 61

Predlog uredbe
Člen 17 – odstavek 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. Podpora iz kibernetskovarnostne rezerve EU je v skladu s to uredbo in izpolnjuje vse posebne pogoje, določene v pridružitvenih sporazumih iz odstavka 1.	2. Podpora iz kibernetskovarnostne rezerve EU je v skladu s to uredbo in izpolnjuje vse posebne pogoje, določene v pridružitvenih sporazumih iz odstavka***, razen za tretje države, za katere veljajo določbe iz odstavka*** 1***(b)***.

Predlog spremembe 62

Predlog uredbe
Člen 18 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. Agencija ENISA na zahtevo Komisije, mreže EU-CyCLONe ali mreže skupin CSIRT pregleda in oceni grožnje,	1. Agencija ENISA na zahtevo Komisije, mreže EU-CyCLONe ali mreže skupin CSIRT pregleda in oceni grožnje,

ranljivosti in blažitvene ukrepe v zvezi s posameznim pomembnim kibernetskovarnostnim incidentom ali takim incidentom velikih razsežnosti. Agencija ENISA po zaključku pregleda in ocene incidenta mreži skupin CSIRT, mreži EU-CyCLONe in Komisiji predloži poročilo o pregledu incidenta, da bi jih podprla pri izvajanju njihovih nalog, zlasti nalog iz členov 15 in 16 Direktive (EU) 2022/2555. Komisija poročilo po potrebi posreduje visokemu predstavniku.	ranljivosti in blažitvene ukrepe v zvezi s posameznim pomembnim kibernetskovarnostnim incidentom ali takim incidentom velikih razsežnosti. Agencija ENISA po zaključku pregleda in ocene incidenta mreži skupin CSIRT, mreži EU-CyCLONe in Komisiji predloži poročilo o pregledu incidenta, da bi jih podprla pri izvajanju njihovih nalog, zlasti nalog iz členov 15 in 16 Direktive (EU) 2022/2555. Komisija poročilo po potrebi***, zlasti če je incident povezan s tretjo državo,*** posreduje visokemu predstavniku ***in Evropski službi za zunanje delovanje***.

Predlog spremembe 63

Predlog uredbe
Člen 18 – odstavek 3 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	3a. Poročilo se posreduje Evropskemu parlamentu v skladu s pravom Unije ali nacionalnim pravom o varovanju občutljivih tajnih podatkov.

Predlog spremembe 64

Predlog uredbe
Člen 19 – odstavek 1 – točka 1 – točka a – točka 1
Uredba (EU) 2021/694
Člen 6 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(aa) podpora razvoju kibernetskega ščita EU, vključno z razvojem, uvedbo in delovanjem platform nacionalnih in čezmejnih centrov za varnostne operacije, ki prispevajo k situacijskemu zavedanju v Uniji in krepitvi zmogljivosti Unije za pridobivanje obveščevalnih podatkov o kibernetskih grožnjah;	(aa) podpora razvoju kibernetskega ščita EU, vključno z razvojem, uvedbo in delovanjem platform nacionalnih in čezmejnih centrov za varnostne operacije, ki prispevajo k situacijskemu zavedanju v Uniji in krepitvi zmogljivosti Unije za pridobivanje obveščevalnih podatkov o kibernetskih grožnjah ***ter zmanjšujejo odvisnost Unije od ponudnikov z visokim tveganjem, ki ponujajo kritično opremo***

	ali komponente za kibernetsko varnost, a bi lahko delovali v nasprotju z varnostnimi in obrambnimi interesi Unije in njenih držav članic, kot so določeni v okviru SZVP na podlagi naslova V PEU;

Predlog spremembe 65

Predlog uredbe
Člen 20 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
Komisija do ***[štiri*** leta po datumu začetka uporabe te ***uredbe]*** Evropskemu parlamentu in Svetu predloži poročilo o oceni in pregledu te uredbe.	Komisija do ***[tri*** leta po datumu začetka uporabe te ***uredbe in nato vsaki dve leti]*** Evropskemu parlamentu in Svetu predloži poročilo o oceni in pregledu te uredbe.

POSTOPEK V ODBORU, ZAPROŠENEM ZA MNENJE

Naslov	Določitev ukrepov za okrepitev solidarnosti in zmogljivosti v Uniji za odkrivanje kibernetskovarnostnih groženj in incidentov ter pripravo in odzivanje nanje
Referenčni dokumenti	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)
Pristojni odbor Datum razglasitve na zasedanju	ITRE 1.6.2023
Mnenje pripravil Datum razglasitve na zasedanju	AFET 1.6.2023
Pripravljavec/-ka mnenja Datum imenovanja	Dragoş Tudorache 16.6.2023
Obravnava v odboru	18.9.2023
Datum sprejetja	24.10.2023
Izid končnega glasovanja	+: 39 –: 4 0: 0
Poslanci, navzoči pri končnem glasovanju	Aleksander Aleksandrov Jordanov (Alexander Alexandrov Yordanov), Petras Auštrevičius, Traian Băsescu, Anna Bonfrisco, Włodzimierz Cimoszewicz, Katalin Cseh, Michael Gahler, Jorgos Jeorjiu (Giorgos Georgiou), Sunčana Glavak, Bernard Guetta, Sandra Kalniete, Dietmar Köster, Andrius Kubilius, David Lega, Leopoldo López Gil, Jaak Madison, Pedro Marques, David McAllister, Vangelis Meimarakis, Sven Mikser, Francisco José Millán Mon, Matjaž Nemec, Dimitris Papadakis (Demetris Papadakis), Kostas Papadakis, Tonino Picula, Thijs Reuten, Nacho Sánchez Amor, Andreas Schieder, Jordi Solé, Sergej Stanišev (Sergei Stanishev), Tineke Strik, Dominik Tarczyński, Dragoş Tudorache, Thomas Waitz, Bernhard Zimniok, Željana Zovko
Namestniki, navzoči pri končnem glasovanju	Attila Ara-Kovács, Lars Patrick Berg, Andrej Kovačev (Andrey Kovatchev), Georgios Kircos (Georgios Kyrtsos), Sergey Lagodinsky, Giuliano Pisapia, Mick Wallace

POIMENSKO GLASOVANJE PRI KONČNEM GLASOVANJU V ODBORU, ZAPROŠENEM ZA MNENJE

39	+
ECR	Lars Patrick Berg, Dominik Tarczyński
ID	Anna Bonfrisco, Jaak Madison
PPE	Aleksander Aleksandrov Jordanov (Alexander Alexandrov Yordanov), Traian Băsescu, Michael Gahler, Sunčana Glavak, Sandra Kalniete, Andrej Kovačev (Andrey Kovatchev), Andrius Kubilius, David Lega, Leopoldo López Gil, David McAllister, Vangelis Meimarakis, Francisco José Millán Mon, Željana Zovko
Renew	Petras Auštrevičius, Katalin Cseh, Bernard Guetta, Georgios Kircos (Georgios Kyrtsos), Dragoş Tudorache
S&D	Attila Ara-Kovács, Włodzimierz Cimoszewicz, Dietmar Köster, Pedro Marques, Sven Mikser, Matjaž Nemec, Dimitris Papadakis (Demetris Papadakis), Tonino Picula, Giuliano Pisapia, Thijs Reuten, Nacho Sánchez Amor, Andreas Schieder, Sergej Stanišev (Sergei Stanishev)
Verts/ALE	Sergey Lagodinsky, Jordi Solé, Tineke Strik, Thomas Waitz

4	-
ID	Bernhard Zimniok
NI	Kostas Papadakis
The Left	Jorgos Jeorjiu (Giorgos Georgiou), Mick Wallace

0	0

Uporabljeni znaki:
+ : za
- : proti
0 : vzdržani

25.10.2023

MNENJE ODBORA ZA PROMET IN TURIZEM

za Odbor za industrijo, raziskave in energetiko

o predlogu uredbe Evropskega parlamenta in Sveta o določitvi ukrepov za okrepitev solidarnosti in zmogljivosti v Uniji za odkrivanje kibernetskovarnostnih groženj in incidentov ter pripravo in odzivanje nanje
(COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

Pripravljavec mnenja: Gheorghe Falcă

KRATKA OBRAZLOŽITEV

Organizacije, ki jih prizadenejo kibernetski napadi, tudi v prometnem sektorju, jih redko prijavijo, zlasti podjetja zasebnega sektorja, saj menijo, da gre za „slabo reklamo“. Večina organizacij se z njimi rajši spoprijema interno in napade pogosto objavijo kar napadalci. V Uniji je odjeknila dobra novica, da začetek veljavnosti Direktive (EU) 2022/2555 o varnosti omrežij (direktiva NIS 2), ki jo morajo države članice v nacionalno zakonodajo prenesti do oktobra 2024, harmonizira obveznosti poročanja o incidentih v državah članicah. Zato bo v prihodnjih letih verjetno prišlo do boljšega razumevanja narave in obsega tega problema.

Agencija Evropske unije za kibernetsko varnost (ENISA) je nedavno objavila poročilo1 s podatki o kibernetskovarnostnih grožnjah v prometnem sektorju, v katerem poudarja, da so bili kibernetski kriminalci odgovorni za več kot polovico incidentov v obdobju poročanja za leto 2022 (55 %) in da je bil glavni motiv za te napade finančna korist. Ugotavlja tudi, da je večina kibernetskih napadov v prometnem sektorju usmerjena v informacijske sisteme, kar povzroča motnje v delovanju.

Kar zadeva pripravljenost in odzivanje na kibernetskovarnostne incidente, sta podpora na ravni Unije in solidarnost med državami članicami trenutno omejeni. Svet je v sklepih iz maja 2022 poudaril, da je treba te vrzeli odpraviti, in pozval Komisijo, naj predstavi predlog o novem **skladu za odzivanje na izredne kibernetskovarnostne razmere**[2].

S to uredbo se izvaja **strategija EU za kibernetsko varnost**, sprejeta decembra 2020, v kateri je bila napovedana vzpostavitev **evropskega kibernetskega ščita**, ki krepi zmogljivosti za odkrivanje kibernetskih groženj in izmenjavo informacij o njih v Evropski uniji z združevanjem nacionalnih in čezmejnih centrov za varnostne operacije (SOC). Ukrepi iz te uredbe bodo podprti s **sredstvi, namenjenimi strateškemu cilju kibernetske varnosti v okviru programa Digitalna Evropa**.

[1] Understanding Cyber Threats in Transport (Razumevanje kibernetskih groženj v prometu), ENISA, objavljeno 21. marca 2023.
[2] Sklepi Sveta o oblikovanju stališča Evropske unije glede kibernetskih vprašanj z dne 23. maja 2022, (9364/22).

Skupni proračun vključuje povečanje sredstev v višini 100 milijonov EUR, za katero se v tej uredbi predlaga, da se prerazporedi iz drugih strateških ciljev programa Digitalna Evropa. Tako se bo novi skupni znesek, ki je na voljo za ukrepe na področju kibernetske varnosti v okviru programa Digitalna Evropa, povečal na 842,8 milijona EUR.

Z delom dodatnih 100 milijonov EUR se bo okrepil proračun, ki ga upravlja Evropski kompetenčni center za kibernetsko varnost (ECCC), za izvajanje ukrepov v zvezi s centri za varnostne operacije in pripravljenostjo v okviru njihovih delovnih programov. Poleg tega bodo dodatna sredstva namenjena podpori vzpostavitve kibernetskovarnostne rezerve EU. Ta sredstva dopolnjujejo proračun, ki je za podobne ukrepe že predviden v okviru delovnih programov osrednjega programa Digitalna Evropa in programa Digitalna Evropa za kibernetsko varnost za obdobje 2023–2027, s čimer bi se lahko skupni znesek za obdobje 2023–2027 povečal na 551 milijonov EUR, pri čemer je bilo za obdobje 2021–2022 že dodeljenih 115 milijonov EUR v obliki pilotnih projektov. Vključno s prispevki držav članic bi lahko skupni proračun znašal do 1,109 milijarde EUR.

Stališče pripravljavca mnenja

Pripravljavec mnenja pozdravlja novi predlog in meni, da bo različnim deležnikom prinesel znatne koristi. Poudarja, da je treba bolje razumeti potrebe in zahteve glede kibernetske varnosti pri prevozu ter da je treba kritičnim subjektom na področju prometa zagotoviti dostop do ustreznega financiranja za pripravljenost, odzivanje in reševanje incidentov.

Pripravljavec mnenja podpira nabor orodij za kibernetsko varnost v prometu, katerega namen je prispevati k višji ravni kibernetske ozaveščenosti in higiene s posebnim poudarkom na prometnem sektorju. Obravnava prometne organizacije, ne glede na njihovo velikost in področje dejavnosti, ter upošteva kritično prometno infrastrukturo in vojaško mobilnost, posebej z ozirom na vojno v Ukrajini, med drugim zlasti:

- letalske prevoznike, organe za upravljanje letališč, jedrna letališča, centre za upravljanje in nadzor zračnega prometa, Agencijo Evropske unije za varnost v letalstvu in Eurocontrol;
- upravljavce infrastrukture, prevoznike v železniškem prometu in evropski sistem za upravljanje železniškega prometa (ERTMS);
- prevozna podjetja za potniški in tovorni promet po kopenskih vodah, morju in obalnih vodah, upravne organe pristanišč, tudi njihove pristaniške objekte, subjekte, ki izvajajo dela in upravljajo opremo v pristaniščih, ter upravljavce sistemov za nadzor plovbe;
- organe za ceste, pristojne za nadzor upravljanja prometa, upravljavce inteligentnih prometnih sistemov;
- poštne in kurirske službe.

Pripravljavec mnenja meni, da bo njegov uspeh odvisen od obsega proračuna za delovanje **sklada za odzivanje na izredne kibernetskovarnostne razmere** (ERFC), zato bi moral biti dovolj velik, da bi države članice podprli pri **pripravi na** pomembne kibernetskovarnostne incidente in take incidente velikih razsežnosti, **odzivanju nanje in okrevanju po njih**. Podpora za odzivanje na incidente je na voljo tudi institucijam, organom, uradom in agencijam Unije.

Evropski kibernetski ščit bo izboljšal zmogljivosti držav članic za odkrivanje kibernetskih groženj, **mehanizem za izredne kibernetske razmere** pa bo dopolnjeval ukrepe držav članic z nujno pomočjo za pripravljenost, odzivanje in takojšnje okrevanje/ponovno vzpostavitev delovanja bistvenih storitev.

PREDLOGI SPREMEMB

Odbor za promet in turizem poziva Odbor za industrijo, raziskave in energetiko kot pristojni odbor, da upošteva:

Predlog spremembe 1

Predlog uredbe
Uvodna izjava 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(2) Obseg, pogostost in posledice kibernetskovarnostnih incidentov se povečujejo, vključno z napadi na oskrbovalno verigo, katerih cilj je kibernetsko vohunjenje, izsiljevalsko programje ali povzročanje motenj. Ti predstavljajo veliko grožnjo za delovanje omrežja in informacijskih sistemov. Glede na hitro razvijajočo se krajino groženj je treba zaradi nevarnosti morebitnih incidentov velikih razsežnosti, ki povzročajo velike motnje ali škodo na kritičnih infrastrukturah, povečati pripravljenost na vseh ravneh okvira Unije za kibernetsko varnost. Ta nevarnost presega rusko vojaško agresijo na Ukrajino in se bo verjetno nadaljevala, glede na številne na državni ravni usklajene, kriminalne in hektivistične akterje, vpletene v trenutne geopolitične napetosti. Taki incidenti lahko ovirajo zagotavljanje javnih storitev in opravljanje gospodarskih dejavnosti, tudi v kritičnih ali visoko kritičnih sektorjih, povzročijo znatne finančne izgube, spodkopljejo zaupanje uporabnikov, povzročijo veliko škodo gospodarstvu Unije in imajo lahko celo zdravstvene ali življenjsko nevarne posledice. Poleg tega so kibernetskovarnostni incidenti nepredvidljivi, saj pogosto nastanejo in se razvijejo v zelo kratkem času, niso omejeni na določeno geografsko območje in se zgodijo hkrati ali se takoj razširijo po številnih državah.	(2) Obseg, pogostost in posledice kibernetskovarnostnih incidentov se povečujejo, vključno z napadi na oskrbovalno verigo, katerih cilj je kibernetsko vohunjenje, izsiljevalsko programje ali povzročanje motenj. Ti predstavljajo veliko grožnjo za delovanje omrežja in informacijskih sistemov ***ter kritične informacijske in fizične infrastrukture***. Glede na hitro razvijajočo se krajino groženj je treba zaradi nevarnosti morebitnih incidentov velikih razsežnosti, ki povzročajo velike motnje ali škodo na kritičnih infrastrukturah, povečati pripravljenost na vseh ravneh okvira Unije za kibernetsko varnost. Ta nevarnost presega rusko vojaško agresijo na Ukrajino in se bo verjetno nadaljevala, glede na številne na državni ravni usklajene, kriminalne in hektivistične akterje, vpletene v trenutne geopolitične napetosti. Taki incidenti lahko ovirajo zagotavljanje javnih storitev***, javnega*** in ***zasebnega prometa ter*** opravljanje gospodarskih dejavnosti, tudi v kritičnih ali visoko kritičnih sektorjih, povzročijo znatne finančne izgube, spodkopljejo zaupanje uporabnikov, povzročijo veliko škodo gospodarstvu ***in mobilnosti*** Unije in imajo lahko celo zdravstvene ali življenjsko nevarne posledice. Poleg tega so kibernetskovarnostni incidenti nepredvidljivi, saj pogosto nastanejo in se razvijejo v zelo kratkem času, niso omejeni na določeno geografsko območje in se zgodijo hkrati ali se takoj razširijo po

številnih državah.

Predlog spremembe 2

Predlog uredbe
Uvodna izjava 2 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(2a) Akterji, ki jih podpirajo države, storilci kibernetskih kaznivih dejanj in hektivisti, katerih tarča so organi, operaterji, proizvajalci, dobavitelji in ponudniki storitev v letalskem, pomorskem, železniškem in cestnem prometu, predstavljajo vse resnejšo kibernetskovarnostno grožnjo prometnemu sektorju. Agencija Evropske unije za kibernetsko varnost (ENISA) je ugotovila, da se je v letu 2022 povprečno mesečno število sporočenih incidentov, ki so prizadeli prometni sektor, v primerjavi z ravnmi iz leta 2021 povečalo za 25 %. Tarča teh napadov na prometni sektor so večinoma sistemi informacijske tehnologije, posledično lahko pride do motenj v delovanju teh sistemov[14a].
	[14a] ENISA (2023), ENISA threat landscape: Transport sector (Poročilo agencije ENISA o naravi groženj: prometni sektor), str. 7 in 17.

Predlog spremembe 3

Predlog uredbe
Uvodna izjava 2 b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(2b) Z neizzvano invazijo Rusije na Ukrajino se je znatno povečalo število kibernetskovarnostnih incidentov, vključno s porazdeljenimi kibernetskimi napadi za zavrnitev storitve, katerih tarča so prometni sektor v EU in območja blizu

EU, zlasti letališča, železnice in prometni organi[14b]. Število teh napadov se bo zelo verjetno tudi v prihodnje še povečevalo.

[14b] ENISA (2023), ENISA threat landscape: Transport sector (Poročilo agencije ENISA o naravi groženj: prometni sektor), str. 9.

Predlog spremembe 4

Predlog uredbe
Uvodna izjava 2 c (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(2c) Tarča kibernetskih napadov so organi in telesa v vseh prometnih podsektorjih, pri čemer so prizadeti prevozniki v železniškem prometu ter upravljavci infrastrukture in pristanišč. Kar zadeva cestni sektor, pa so bili – poleg izvajalcev javnega prevoza – njihova tarča proizvajalci originalne opreme, dobavitelji in ponudniki storitev. V letalskem sektorju pa so bili glavna tarča letalski prevozniki in upravljavci letališč, sledili pa so jim ponudniki storitev, izvajalci površinskega prevoza in dobavna veriga[14c].

[14c] ENISA (2023), ENISA threat landscape: Transport sector (Poročilo agencije ENISA o naravi groženj: prometni sektor), str. 17.

Predlog spremembe 5

Predlog uredbe
Uvodna izjava 3

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(3) Okrepiti je treba konkurenčni položaj industrijskega in storitvenega sektorja v Uniji v celotnem spletnem	(3) Okrepiti je treba konkurenčni položaj industrijskega in storitvenega sektorja v Uniji v celotnem spletnem

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[16], je treba povečati odpornost državljanov, podjetij in subjektov, ki upravljajo kritične infrastrukture, proti vse večjim kibernetskovarnostnim grožnjam, ki imajo lahko uničujoče družbene in gospodarske posledice. Zato so potrebne naložbe v infrastrukture in storitve, ki bodo podpirale hitrejše odkrivanje kibernetskovarnostnih groženj in incidentov ter odzivanje nanje, države članice pa potrebujejo pomoč pri boljši pripravi na pomembne kibernetskovarnostne incidente in take incidente velikih razsežnosti ter odzivanju nanje. Unija bi tudi morala povečati svoje zmogljivosti na teh področjih, zlasti kar zadeva zbiranje in analizo podatkov o kibernetskovarnostnih grožnjah in incidentih.

[16] https://futureu.europa.eu/en/

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[16], je treba povečati odpornost državljanov, podjetij***,*** ***prevoznikov*** in subjektov, ki upravljajo kritične infrastrukture, proti vse večjim kibernetskovarnostnim grožnjam, ki imajo lahko uničujoče družbene in gospodarske posledice. Zato so potrebne naložbe v infrastrukture in storitve, ki bodo podpirale hitrejše odkrivanje kibernetskovarnostnih groženj in incidentov ter odzivanje nanje, države članice pa potrebujejo pomoč pri boljši pripravi na pomembne kibernetskovarnostne incidente in take incidente velikih razsežnosti ter odzivanju nanje. Unija bi tudi morala povečati svoje zmogljivosti na teh področjih, zlasti kar zadeva zbiranje in analizo podatkov o kibernetskovarnostnih grožnjah in incidentih ***ter o stanju in razvoju kibernetskovarnostnega trga dela, saj ima ključno vlogo pri zagotavljanju potrebnih storitev odkrivanja in odzivanja***.

[16] https://futureu.europa.eu/en/

Predlog spremembe 6

Predlog uredbe
Uvodna izjava 4

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(4) Unija je že sprejela več ukrepov za zmanjšanje ranljivosti in povečanje odpornosti kritičnih infrastruktur in subjektov proti tveganjem za kibernetsko varnost, zlasti Direktivo (EU) 2022/2555 Evropskega parlamenta in Sveta[17], Priporočilo Komisije (EU) 2017/1584[18], Direktivo 2013/40/EU Evropskega parlamenta in Sveta[19] ***ter*** Uredbo (EU) 2019/881 Evropskega parlamenta in	(4) Unija je že sprejela več ukrepov za zmanjšanje ranljivosti in povečanje odpornosti kritičnih infrastruktur in subjektov proti tveganjem za kibernetsko varnost, zlasti Direktivo (EU) 2022/2555 Evropskega parlamenta in Sveta[17], Priporočilo Komisije (EU) 2017/1584[18], Direktivo 2013/40/EU Evropskega parlamenta in Sveta[19] ***in*** Uredbo (EU) 2019/881 Evropskega parlamenta in

Sveta[20]. Poleg tega so države članice v priporočilu Sveta o usklajenem vseevropskem pristopu za krepitev odpornosti kritične infrastrukture pozvane, naj sprejmejo nujne in učinkovite ukrepe ter zvesto, učinkovito, solidarno in usklajeno sodelujejo med seboj, s Komisijo in drugimi ustreznimi javnimi organi ter zadevnimi subjekti, da bi se okrepila odpornost kritične infrastrukture, ki se uporablja za zagotavljanje bistvenih storitev na notranjem trgu.

Sveta[20] ***ter predlog uredbe o smernicah za razvoj vseevropskega prometnega omrežja in predlog uredbe o horizontalnih zahtevah glede kibernetske varnosti za izdelke z digitalnimi elementi (akt o kibernetski odpornosti)***. Poleg tega so države članice v priporočilu Sveta o usklajenem vseevropskem pristopu za krepitev odpornosti kritične infrastrukture pozvane, naj sprejmejo nujne in učinkovite ukrepe ter zvesto, učinkovito, solidarno in usklajeno sodelujejo med seboj, s Komisijo in drugimi ustreznimi javnimi organi ter zadevnimi subjekti, da bi se okrepila odpornost kritične infrastrukture, ki se uporablja za zagotavljanje bistvenih storitev na notranjem trgu.

---

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

[18] 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).

[19] 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).

[20] 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).

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

[18] 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).

[19] 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).

[20] 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).

Predlog spremembe 7

Predlog uredbe
Uvodna izjava 4 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(4a) Sicer pozdravlja zbirko orodij Evropske komisije za kibernetsko varnost v prometu[2a], ki vsebuje osnovne informacije o grožnjah, ki lahko vplivajo na prometne organizacije (razširjanje zlonamerne programske opreme, zavrnitev storitve, nepooblaščen dostop in kraja ter manipulacija programske opreme), in navaja primere dobre prakse za blažitev, a bi bilo treba prevoznikom zagotoviti ustrezno usposabljanje o kibernetski varnosti in ustrezna orodja za preprečevanje kibernetskih groženj. Iz proračuna Unije bi morala biti krita tudi podpora, kot je usposabljanje, ki ga zagotavlja agencija ENISA, da bi lahko prevozniki učinkovito izvajali primere dobre prakse za blažitev, vključene v zbirko orodij.
	[1a] ENISA threat landscape: transport sector (Poročilo agencije ENISA o naravi groženj: prometni sektor), ENISA, marec 2023.
	[2a] Evropska komisija, (2021). Transport Cybersecurity Toolkit (zbirka orodij za kibernetsko varnost v prometu), na voljo na spletnem naslovu https://transport.ec.europa.eu/transport-themes/security-safety/cybersecurity_en

Predlog spremembe 8

Predlog uredbe
Uvodna izjava 4 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(4a) Usklajen vseevropski pristop za povečanje pripravljenosti in odpornosti

kritične infrastrukture, na primer prometne infrastrukture, temelji na krepitvi zmogljivosti držav članic. Kot je priznano v nedavnem sporočilu Komisije Evropskemu parlamentu in Svetu o zapolnitvi vrzeli na področju strokovnjakov za kibernetsko varnost za povečanje konkurenčnosti, rasti in odpornosti EU[19a], varnosti EU ni mogoče zagotoviti brez njenega največjega bogastva: njenih državljanov.

[19a] Sporočilo Komisije Evropskemu parlamentu in Svetu o zapolnitvi vrzeli na področju strokovnjakov za kibernetsko varnost za povečanje konkurenčnosti, rasti in odpornosti EU („akademija za kibernetske veščine“) (COM(2023)0207).

Predlog spremembe 9

Predlog uredbe
Uvodna izjava 12

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(12) Za učinkovitejše preprečevanje in ocenjevanje kibernetskih groženj in incidentov ter odzivanje nanje je treba razviti celovitejše znanje o grožnjah za kritična sredstva in infrastrukture na ozemlju Unije, vključno z njihovo geografsko porazdelitvijo, medsebojno povezanostjo in morebitnimi učinki v primeru kibernetskih napadov na te infrastrukture. Vzpostaviti bi bilo treba obsežno infrastrukturo centrov za varnostne operacije (v nadaljnjem besedilu: evropski kibernetski ščit) v Uniji, ki bi jo sestavljalo več interoperabilnih čezmejnih platform, od katerih bi vsaka združevala več nacionalnih centrov za varnostne operacije. Ta infrastruktura bi morala služiti interesom in potrebam držav in Unije na področju kibernetske varnosti, spodbujati najsodobnejšo tehnologijo za napredno zbiranje podatkov in analitična	(12) Za učinkovitejše preprečevanje in ocenjevanje kibernetskih groženj in incidentov ter odzivanje nanje je treba razviti celovitejše znanje o grožnjah za kritična sredstva in infrastrukture na ozemlju Unije, vključno z njihovo geografsko porazdelitvijo, medsebojno povezanostjo in morebitnimi učinki v primeru kibernetskih napadov na te infrastrukture. ***Ta kritična sredstva in infrastrukture vključujejo inteligentne prometne sisteme, ki so sicer bistvenega pomena za avtomatizirano in večmodalno mobilnost, vendar je za njihovo delovanje potrebna izmenjava občutljivih podatkov.*** Vzpostaviti bi bilo treba obsežno infrastrukturo centrov za varnostne operacije (v nadaljnjem besedilu: evropski kibernetski ščit) v Uniji, ki bi jo sestavljalo več interoperabilnih čezmejnih platform, od katerih bi vsaka združevala več

orodja, okrepiti zmogljivosti kibernetskega odkrivanja in upravljanja ter zagotavljati situacijsko zavedanje v realnem času. Namenjena bi morala biti boljšemu odkrivanju kibernetskovarnostnih groženj in incidentov ter tako dopolnjevati in podpirati subjekte in omrežja Unije, odgovorne za krizno upravljanje v Uniji, zlasti organizacijsko mrežo EU za povezovanje v kibernetski krizi (v nadaljnjem besedilu: mreža EU-CyCLONe), kot je opredeljena v Direktivi (EU) 2022/2555 Evropskega parlamenta in Sveta[24].

nacionalnih centrov za varnostne operacije. Ta infrastruktura bi morala služiti interesom in potrebam držav in Unije na področju kibernetske varnosti, spodbujati najsodobnejšo tehnologijo za napredno zbiranje podatkov in analitična orodja, okrepiti zmogljivosti kibernetskega odkrivanja in upravljanja ter zagotavljati situacijsko zavedanje v realnem času. Namenjena bi morala biti boljšemu odkrivanju kibernetskovarnostnih groženj in incidentov ter tako dopolnjevati in podpirati subjekte in omrežja Unije, odgovorne za krizno upravljanje v Uniji, zlasti organizacijsko mrežo EU za povezovanje v kibernetski krizi (v nadaljnjem besedilu: mreža EU-CyCLONe), kot je opredeljena v Direktivi (EU) 2022/2555 Evropskega parlamenta in Sveta[24].

---

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

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

Predlog spremembe 10

Predlog uredbe
Uvodna izjava 14 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(14a) Prometni sektor v vse večji meri postaja eden najdonosnejših poslov za storilce kibernetskih kaznivih dejanj, pri čemer podatki o strankah veljajo za zelo dragoceno dobrino, prometna dobavna veriga pa postaja vse pogostejša tarča. Zato bi bilo treba prometno infrastrukturo, ki je čezmejne narave ali v sklopu katere se prek brezžičnih tehnologij izmenjujejo podatki,

obravnavati kot osrednji predmet, ki ga bi morali nacionalni in zlasti čezmejni centri za varnostne operacije analizirati in spremljati. V skladu z nedavnim predlogom za revizijo uredbe o omrežju TEN-T mora na primer biti izmenjava informacij o čezmejnih kibernetskih grožnjah, s katerimi se lahko to nadnacionalno omrežje sooča, v znamenju večje solidarnosti in sodelovanja. Podobno so inteligentni prometni sistemi sicer bistvenega pomena za varnejši, učinkovitejši in bolj trajnosten promet, a so zaradi njih prometni sistemi bolj izpostavljeni kibernetskim napadom, ki lahko povzročijo nesreče, prometne zastoje ali gospodarske izgube za zasebne in javne prevoznike. Da bi zagotovili varnost potnikov, varstvo podatkov uporabnikov in ponudnikov ter preprečili finančno škodo, je bistveno, da program izvajanja revidirane direktive o inteligentnih prometnih sistemih vključuje določbe in orodja za krepitev sodelovanja med državami članicami pri odkrivanju kibernetskovarnostnih groženj in incidentov ter pripravi in odzivanju nanje.

Predlog spremembe 11

Predlog uredbe
Uvodna izjava 15

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(15) Spremljanje, odkrivanje in analizo kibernetskih groženj na nacionalni ravni običajno zagotavljajo centri za varnostne operacije, ki jih sestavljajo javni in zasebni subjekti, v povezavi s skupinami CSIRT. Poleg tega si skupine CSIRT informacije izmenjujejo v okviru mreže skupin CSIRT v skladu z Direktivo (EU) 2022/2555. Čezmejni centri za varnostne operacije bi morali predstavljati novo zmogljivost, ki dopolnjuje mrežo skupin CSIRT, in sicer z zbiranjem in izmenjavo podatkov javnih in zasebnih subjektov o	(15) Spremljanje, odkrivanje in analizo kibernetskih groženj na nacionalni ravni običajno zagotavljajo centri za varnostne operacije, ki jih sestavljajo javni in zasebni subjekti, v povezavi s skupinami CSIRT. Poleg tega si skupine CSIRT informacije izmenjujejo v okviru mreže skupin CSIRT v skladu z Direktivo (EU) 2022/2555. Čezmejni centri za varnostne operacije bi morali predstavljati novo zmogljivost, ki dopolnjuje mrežo skupin CSIRT, in sicer z zbiranjem in izmenjavo podatkov javnih in zasebnih subjektov o

kibernetskovarnostnih grožnjah, povečevanjem vrednosti takih podatkov s strokovno analizo ter skupno pridobljenimi infrastrukturami in najsodobnejšimi orodji ter prispevanjem k razvoju zmogljivosti in tehnološke suverenosti Unije.	kibernetskovarnostnih grožnjah, povečevanjem vrednosti takih podatkov s strokovno analizo ter skupno pridobljenimi infrastrukturami in najsodobnejšimi orodji ter prispevanjem k razvoju zmogljivosti in tehnološke suverenosti Unije. ***V zvezi s tem je za okrepitev avtonomije Unije na kibernetskem področju in ob upoštevanju člena 47(4) predloga uredbe o smernicah za razvoj vseevropskega prometnega omrežja (COM(2021)0812) tudi treba preprečiti dostop do podatkov, ki vodijo do kibernetskih groženj, in sicer z izvrševanjem trdnega regulativnega okvira, ki ureja tuje lastništvo kritične infrastrukture in tuje naložbe vanjo, na primer na področju prometa.***

Predlog spremembe 12

Predlog uredbe
Uvodna izjava 21

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(21) Čeprav je evropski kibernetski ščit civilni projekt, bi lahko imela skupnost za kibernetsko obrambo koristi od okrepljenih zmogljivosti civilnega odkrivanja in situacijskega zavedanja, ki so bile razvite za zaščito kritične infrastrukture. Čezmejni centri za varnostne operacije bi morali ob podpori Komisije in Evropskega kompetenčnega centra za kibernetsko varnost (v nadaljnjem besedilu: ECCC) ter v sodelovanju z visokim predstavnikom Unije za zunanje zadeve in varnostno politiko (v nadaljnjem besedilu: visoki predstavnik) postopoma razviti namenske protokole in standarde, da se omogoči sodelovanje s skupnostjo za kibernetsko obrambo, vključno s pogoji preverjanja in varnostnimi pogoji. Razvoj evropskega kibernetskega ščita bi moral spremljati razmislek, na podlagi katerega bi bilo v tesnem sodelovanju z visokim predstavnikom omogočeno prihodnje sodelovanje z mrežami in platformami,	(21) Čeprav je evropski kibernetski ščit civilni projekt, bi lahko imela skupnost za kibernetsko obrambo koristi od okrepljenih zmogljivosti civilnega odkrivanja in situacijskega zavedanja, ki so bile razvite za zaščito kritične infrastrukture. Čezmejni centri za varnostne operacije bi morali ob podpori Komisije in Evropskega kompetenčnega centra za kibernetsko varnost (v nadaljnjem besedilu: ECCC) ter v sodelovanju z visokim predstavnikom Unije za zunanje zadeve in varnostno politiko (v nadaljnjem besedilu: visoki predstavnik) postopoma razviti namenske protokole in standarde, da se omogoči sodelovanje s skupnostjo za kibernetsko obrambo, vključno s pogoji preverjanja in varnostnimi pogoji. Razvoj evropskega kibernetskega ščita bi moral spremljati razmislek, na podlagi katerega bi bilo v tesnem sodelovanju z visokim predstavnikom omogočeno prihodnje sodelovanje z mrežami in platformami,

odgovornimi za izmenjavo informacij v skupnosti za kibernetsko obrambo.	odgovornimi za izmenjavo informacij v skupnosti za kibernetsko obrambo. ***Poleg tega bi moral omogočiti sinergije z akcijskim načrtom za vojaško mobilnost 2.0. Dobro delujoče omrežje vojaške mobilnosti mora biti odporno, tudi v kontekstu kibernetskih in drugih hibridnih groženj, ki bi lahko vplivale na kritična vozlišča z dvojno rabo v prometnem sistemu. Tako bi lahko na primer kibernetski napad na sisteme, ki se uporabljajo na letališčih, v pristaniščih ali železnicah, ali kibernetski napad na vojaška sredstva imel velike posledice. Da bi lahko digitalizirali procese in postopke, tudi za potrebno civilno in vojaško sodelovanje, bo zato treba okrepiti računalniške informacijske sisteme proti kibernetskim grožnjam.***

Predlog spremembe 13

Predlog uredbe
Uvodna izjava 21 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(21a) Ključnega pomena je, da se v primeru kibernetskovarnostne krize učinkovito izmenjujejo informacije, da se lahko v vojaškem in civilnem prometnem sektorju spremljajo razmere. Prek te izmenjave informacij bi se moralo spodbujati tudi sodelovanje med ustreznimi sektorskimi organi, pristojnimi za promet, organi, pristojnimi za kibernetsko varnost, centri za varnostne operacije in skupinami CSIRT.

Predlog spremembe 14

Predlog uredbe
Uvodna izjava 29

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(29) V okviru ukrepov pripravljenosti bi	(29) V okviru ukrepov pripravljenosti bi

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

bilo treba za spodbujanje doslednega pristopa ter krepitev varnosti po vsej Uniji in na njenem notranjem trgu zagotoviti podporo za usklajeno preskušanje in ocenjevanje kibernetske varnosti subjektov, ki delujejo v visoko kritičnih sektorjih, opredeljenih v skladu z Direktivo (EU) 2022/2555. V ta namen bi morala Komisija ob podpori agencije ENISA in v sodelovanju s skupino za sodelovanje na področju varnosti omrežnih in informacijskih sistemov, ustanovljeno z Direktivo (EU) 2022/2555, redno določati ustrezne sektorje ali podsektorje, ki bi morali biti upravičeni do finančne podpore za usklajeno preskušanje na ravni Unije. Sektorje ali podsektorje bi bilo treba izbrati iz Priloge I k Direktivi (EU) 2022/2555 (v nadaljnjem besedilu: visoko kritični sektorji). ***Posebno pozornost bi bilo treba nameniti prometnemu sektorju in njegovim podsektorjem (zračnemu, železniškemu, vodnemu, cestnemu), saj vključujejo kritično infrastrukturo, v sklopu katere bi lahko kibernetski incidenti in napadi resno ogrozili varnost potnikov in prevoznikov.*** Usklajeno preskušanje bi moralo temeljiti na skupnih scenarijih tveganja in metodologijah. Pri izbiri sektorjev in razvoju scenarijev tveganja bi bilo treba upoštevati ustrezne ocene tveganja in scenarije tveganja po vsej Uniji, vključno s potrebo po preprečevanju podvajanja, kot so ocena tveganja in scenariji tveganja, h katerim poziva Svet v svojih sklepih o oblikovanju kibernetske drže Evropske unije in ki jih morajo izvesti Komisija, visoki predstavnik in skupina za sodelovanje na področju varnosti omrežnih in informacijskih sistemov v sodelovanju z ustreznimi civilnimi in vojaškimi organi in agencijami ter vzpostavljenimi mrežami, med drugim mrežo EU-CyCLONe, pa tudi ocena tveganja komunikacijskih omrežij in infrastruktur, ki se zahteva na podlagi skupnega ministrskega poziva iz Neversa ter jo izvede skupina za sodelovanje na področju varnosti omrežnih in

Uredbi (EU) 2022/2554 Evropskega parlamenta in Sveta[29]. Pri izbiri sektorjev bi bilo treba upoštevati tudi priporočilo Sveta o usklajenem vseevropskem pristopu za krepitev odpornosti kritične infrastrukture.	informacijskih sistemov ob podpori Komisije in agencije ENISA ter v sodelovanju z Organom evropskih regulatorjev za elektronske komunikacije (BEREC), usklajene ocene tveganja, ki se izvedejo v skladu s členom 22 Direktive (EU) 2022/2555, in testiranje digitalne operativne odpornosti, kot je določeno v Uredbi (EU) 2022/2554 Evropskega parlamenta in Sveta[29]. Pri izbiri sektorjev bi bilo treba upoštevati tudi priporočilo Sveta o usklajenem vseevropskem pristopu za krepitev odpornosti kritične infrastrukture.
[29] 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.	[29] 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.

Predlog spremembe 15

Predlog uredbe
Uvodna izjava 30 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(30a) Pri usklajenem preskušanju pripravljenosti subjektov bi bilo treba dati prednost prometnemu sektorju, saj je ta sektor kritičnega pomena in z njim povezane kibernetske grožnje negativno vplivajo na mobilnost ter posledično na življenja potnikov in pešcev.

Predlog spremembe 16

Predlog uredbe
Uvodna izjava 35 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(35a) Glede na to, da je agenciji ENISA

s tem predlogom in predlogom akta o kibernetski odpornosti dodeljenih še več nalog in odgovornosti, je treba sprejeti spremembo proračuna agencije ENISA št. 1/2022 za pilotno izvajanje podpornega ukrepa za kibernetsko varnost. Glede na interese Unije, ki so na kocki, bi bilo treba agenciji ENISA dodeliti tudi dodatne finančne in človeške vire.

Predlog spremembe 17

Predlog uredbe
Uvodna izjava 38 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(38a) Na razvoj veščin in kompetenc bi se zato morali osredotočiti v vseh sektorjih, zlasti v tistih, ki so izpostavljeni kibernetskovarnostnim grožnjam, kot je osebje, ki dela na področju infrastrukture množičnega prevoza ali kritične infrastrukture, vključno s sistemi za nadzor vlakov in digitalnimi orodji za načrtovanje prometa za vse načine prevoza. Da bi lahko to uredbo uspešno izvajali in tako zagotovili ozaveščenost državljanov in strokovno znanje v vseh sektorjih kritične infrastrukture, je zato poglavitnega pomena, da se uvede oziroma nadalje razvije kultura kibernetske varnosti.

Predlog spremembe 18

Predlog uredbe
Člen 1 – odstavek 2 – točka a

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(a) okrepiti skupno odkrivanje kibernetskih groženj in incidentov v Uniji ter situacijsko zavedanje o njih, da se tako okrepi konkurenčni položaj industrijskega in storitvenega sektorja v Uniji v celotnem spletnem gospodarstvu ter prispeva k	(a) okrepiti skupno odkrivanje kibernetskih groženj in incidentov v Uniji ter situacijsko zavedanje o njih, da se tako okrepi konkurenčni položaj industrijskega ***sektorja, prometne infrastrukture*** in storitvenega sektorja v Uniji v celotnem

tehnološki suverenosti Unije na področju kibernetske varnosti;	spletnem gospodarstvu ter prispeva k tehnološki suverenosti Unije na področju kibernetske varnosti;

Predlog spremembe 19

Predlog uredbe
Člen 1 – odstavek 2 – točka b

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(b) okrepiti pripravljenost subjektov, ki delujejo v kritičnih in visoko kritičnih sektorjih po vsej Uniji, ter solidarnost z razvijanjem skupnih zmogljivosti za odzivanje na pomembne kibernetskovarnostne incidente ali take incidente velikih razsežnosti, med drugim z omogočanjem podpore Unije pri odzivanju na kibernetskovarnostne incidente tretjim državam, pridruženim programu Digitalna Evropa;	(b) okrepiti pripravljenost subjektov, ki delujejo v kritičnih in visoko kritičnih sektorjih po vsej Uniji, ter solidarnost z razvijanjem skupnih zmogljivosti za odzivanje na pomembne kibernetskovarnostne incidente ali take incidente velikih razsežnosti, ***pri čemer se posebna pozornost nameni kritični informacijski in fizični infrastrukturi,*** med drugim z omogočanjem podpore Unije pri odzivanju na kibernetskovarnostne incidente tretjim državam, pridruženim programu Digitalna Evropa;

Predlog spremembe 20

Predlog uredbe
Člen 1 – odstavek 2 – točka c a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(ca) okrepiti pripravljenost, sodelovanje in učinkovitost Unije pri tem, da se prometna infrastruktura in prometne storitev v državah članicah ščitijo pred kibernetskovarnostnimi incidenti, s tem zagotovijo neprekinjeno delovanje prometnega sektorja, celovitost dobavnih verig in mobilnost po vsej Uniji.

Predlog spremembe 21

Predlog uredbe
Člen 3 – odstavek 2 – pododstavek 1 – točka c

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(c) prispeva k boljši zaščiti ***proti kibernetskim grožnjam*** in k boljšemu odzivanju nanje***;***	(c) prispeva k boljši zaščiti ***pred kibernetskimi grožnjami*** in k boljšemu odzivanju nanje***, tudi za čezmejno prometno infrastrukturo, kot je omrežje TEN-T, ali z izmenjavo podatkov prek brezžičnih tehnologij, kot so inteligentni prometni sistemi.***

Predlog spremembe 22

Predlog uredbe
Člen 3 – odstavek 2 – pododstavek 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
Razvije se v sodelovanju z infrastrukturo za vseevropsko visokozmogljivostno računalništvo, vzpostavljeno v skladu z Uredbo (EU) 2021/1173.	Razvije se v sodelovanju z infrastrukturo za vseevropsko visokozmogljivostno računalništvo, vzpostavljeno v skladu z Uredbo (EU) 2021/1173. ***Prek namenskih protokolov in standardov omogoča sodelovanje s skupnostjo za kibernetsko obrambo, da se zagotovi razvoj večjih civilnih zmogljivosti za odkrivanje in spremljanje razmer za zaščito kritične infrastrukture. V zvezi s tem se poleg tega razvijejo sinergije z akcijskim načrtom za vojaško mobilnost 2.0, zagotovi pa se tudi učinkovita izmenjava informacij, da se lahko spremljajo razmere v vojaškem in civilnem prometnem sektorju.***

Predlog spremembe 23

Predlog uredbe
Člen 8 – odstavek 2 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	2a. Kadar bi sodelovanje ali prispevek fizične osebe ali podjetja iz tretje države verjetno vplival na kibernetsko varnost čezmejne kritične infrastrukture, kot je omrežje TEN-T, Komisija v svojem mnenju, ki ga državam članicam poda v okviru predloga uredbe o vseevropskem

	prometnem omrežju (COM(2021)0812), vključi evropski kibernetski ščit, zlasti čezmejne centre za varnostne operacije.

Predlog spremembe 24

Predlog uredbe
Člen 10 – odstavek 1 – točka a

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(a) ukrepe pripravljenosti, vključno z usklajenim preskušanjem pripravljenosti subjektov, ki delujejo v visoko kritičnih sektorjih po vsej Uniji;	(a) ukrepe pripravljenosti, vključno z usklajenim preskušanjem pripravljenosti subjektov, ki delujejo v visoko kritičnih sektorjih po vsej Uniji***, pri čemer se posebna pozornost nameni prometni infrastrukturi in njenim podsektorjem iz Priloge I k Direktivi (EU) 2022/2555***;

Predlog spremembe 25

Predlog uredbe
Člen 18 – odstavek 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. Agencija ENISA pri pripravi poročila o pregledu incidenta iz odstavka 1 sodeluje z vsemi ustreznimi deležniki, vključno s predstavniki držav članic, Komisijo, drugimi ustreznimi institucijami, organi, uradi in agencijami EU, ponudniki upravljanih varnostnih storitev in uporabniki kibernetskih storitev. Po potrebi sodeluje tudi s subjekti, ki so jih prizadeli pomembni kibernetskovarnostni incidenti ali taki incidenti velikih razsežnosti. Za podporo pregledu se lahko posvetuje tudi z drugimi vrstami deležnikov. Predstavniki, s katerimi se opravi posvetovanje, razkrijejo vsako morebitno navzkrižje interesov.	2. Agencija ENISA pri pripravi poročila o pregledu incidenta iz odstavka 1 sodeluje z vsemi ustreznimi deležniki, vključno s predstavniki držav članic, Komisijo, drugimi ustreznimi institucijami, organi, uradi in agencijami EU, ponudniki upravljanih varnostnih storitev in uporabniki kibernetskih storitev. Po potrebi sodeluje tudi s subjekti, ki so jih prizadeli pomembni kibernetskovarnostni incidenti ali taki incidenti velikih razsežnosti***, vključno s prevozniki***. Za podporo pregledu se lahko posvetuje tudi z drugimi vrstami deležnikov. Predstavniki, s katerimi se opravi posvetovanje, razkrijejo vsako morebitno navzkrižje interesov.

Predlog spremembe 26

Predlog uredbe

Člen 19 – odstavek 1 – točka 1 – točka b
Uredba (EU) 2021/694
Člen 6 – odstavek 2 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	2a. Glede na interese Unije, ki so na kocki, pa tudi glede na to, da je agencija ENISA dolžna pripraviti predloge za certifikacijske sheme v skladu z Uredbo (EU) 2019/881 ter pregledovati in ocenjevati kibernetske grožnje, ranljivosti in blažitev, pripravljati poročila o pregledu incidentov za mehanizem za pregledovanje kibernetskovarnostnih incidentov ter upravljavcem kritične infrastrukture zagotavljati usposabljanja v zvezi s kibernetskimi napadi in incidenti, pa tudi glede na dolžnosti, ki so ji po novem dodeljene s predlogom akta o kibernetski odpornosti, se tej agenciji zagotovijo potrebna sredstva iz proračuna Unije v skladu z veljavno zakonodajo.

Predlog spremembe 27

Predlog uredbe
Člen 19 – odstavek 1 – točka 1 a (novo)
Uredba (EU) 2021/694
Člen 7 – odstavek 1 – točka c a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(1a) člen 7 se spremeni:
	(a) odstavek 1 se spremeni:
	(1) vstavi se naslednja točka (ca):
	(ca) podpora visokokakovostnemu usposabljanju prevoznikov ter upravljavcev ključne prometne infrastrukture in osebja, med drugim zato, da bi ob kibernetskih napadih ali incidentih v zvezi s kritično infrastrukturo učinkovito izmenjevali in izvajali primere prakse za blažitev, na primer tiste iz zbirke orodij za kibernetsko varnost v prometu.

POSTOPEK V ODBORU, ZAPROŠENEM ZA MNENJE

Naslov	Določitev ukrepov za okrepitev solidarnosti in zmogljivosti v Uniji za odkrivanje kibernetskovarnostnih groženj in incidentov ter pripravo in odzivanje nanje
Referenčni dokumenti	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)
Pristojni odbor Datum razglasitve na zasedanju	ITRE 1.6.2023
Mnenje pripravil Datum razglasitve na zasedanju	TRAN 1.6.2023
Pripravljavec/-ka mnenja Datum imenovanja	Gheorghe Falcă 7.7.2023
Datum sprejetja	25.10.2023
Izid končnega glasovanja	+: 38 –: 0 0: 0
Poslanci, navzoči pri končnem glasovanju	Magdalena Adamowicz, Andris Ameriks, José Ramón Bauzá Díaz, Izaskun Bilbao Barandica, Karolin Braunsberger-Reinhold, Karima Delli, Anna Deparnay-Grunenberg, Gheorghe Falcă, Carlo Fidanza, Jens Gieseke, Elsi Katainen, Elena Kundura (Elena Kountoura), Bogusław Liberadzki, Peter Lundgren, Elżbieta Katarzyna Łukacijewska, Marian-Jean Marinescu, Tilly Metz, Cláudia Monteiro de Aguiar, Caroline Nagtegaal, Jan-Christoph Oetjen, Rovana Plumb, Thomas Rudner, Massimiliano Salini, Vera Tax, Barbara Thaler, István Ujhelyi, Achille Variati, Peter Vitanov (Petar Vitanov), Elisavet Vozemberg-Vrionidi (Elissavet Vozemberg-Vrionidi), Lucia Vuolo
Namestniki, navzoči pri končnem glasovanju	Sara Cerdas, Josianne Cutajar, Roman Haider, Pär Holmgren, Pierre Karleskind, Colm Markey, Ljudmila Novak, Dorien Rookmaker

POIMENSKO GLASOVANJE PRI KONČNEM GLASOVANJU V ODBORU, ZAPROŠENEM ZA MNENJE

38	+
ECR	Carlo Fidanza, Peter Lundgren, Dorien Rookmaker
ID	Roman Haider
PPE	Magdalena Adamowicz, Karolin Braunsberger-Reinhold, Gheorghe Falcă, Jens Gieseke, Elżbieta Katarzyna Łukacijewska, Marian-Jean Marinescu, Colm Markey, Cláudia Monteiro de Aguiar, Ljudmila Novak, Massimiliano Salini, Barbara Thaler, Elisavet Vozemberg-Vrionidi (Elissavet Vozemberg-Vrionidi), Lucia Vuolo
Renew	José Ramón Bauzá Díaz, Izaskun Bilbao Barandica, Pierre Karleskind, Elsi Katainen, Caroline Nagtegaal, Jan-Christoph Oetjen
S&D	Andris Ameriks, Sara Cerdas, Josianne Cutajar, Bogusław Liberadzki, Rovana Plumb, Thomas Rudner, Vera Tax, István Ujhelyi, Achille Variati, Peter Vitanov (Petar Vitanov)
The Left	Elena Kundura (Elena Kountoura)
Verts/ALE	Karima Delli, Anna Deparnay-Grunenberg, Pär Holmgren, Tilly Metz

0	-

0	0

Uporabljeni znaki:
+ : za
- : proti
0 : vzdržani

POSTOPEK V PRISTOJNEM ODBORU

Naslov	Določitev ukrepov za okrepitev solidarnosti in zmogljivosti v Uniji za odkrivanje kibernetskovarnostnih groženj in incidentov ter pripravo in odzivanje nanje			
Referenčni dokumenti	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)			
Datum predložitve EP	19.4.2023			
Pristojni odbor Datum razglasitve na zasedanju	ITRE 1.6.2023			
Odbori, zaprošeni za mnenje Datum razglasitve na zasedanju	AFET 1.6.2023	BUDG 1.6.2023	CONT 1.6.2023	IMCO 1.6.2023
	TRAN 1.6.2023	LIBE 1.6.2023		
Odbori, ki niso podali mnenja Datum sklepa	BUDG 26.4.2023	CONT 24.5.2023	IMCO 23.5.2023	LIBE 30.5.2023
Poročevalec/-ka Datum imenovanja	Lina Gálvez Muñoz 2.5.2023			
Obravnava v odboru	19.9.2023			
Datum sprejetja	7.12.2023			
Izid končnega glasovanja	+: –: 0:	43 10 1		
Poslanci, navzoči pri končnem glasovanju	Nicola Beer, Hildegard Bentele, Vasile Blaga, Michael Bloss, Marc Botenga, Martin Buschmann, Jerzy Buzek, Maria da Graça Carvalho, Josianne Cutajar, Nicola Danti, Marie Dauchy, Pilar del Castillo Vera, Martina Dlabajová, Christian Ehler, Valter Flego, Niels Fuglsang, Nicolás González Casares, Henrike Hahn, Ivo Hristov, Ivars Ijabs, Romana Jerković, Seán Kelly, Izabela-Helena Kloc, Andrius Kubilius, Miapetra Kumpula-Natri, Iskra Mihajlova (Iskra Mihaylova), Angelika Niebler, Niklas Nienaß, Johan Nissinen, Mikuláš Peksa, Cvetelina Penkova (Tsvetelina Penkova), Morten Petersen, Markus Pieper, Manuela Ripa, Robert Roos, Sara Skyttedal, Riho Terras, Pernille Weiss, Carlos Zorrinho			
Namestniki, navzoči pri končnem glasovanju	Andrus Ansip, Laura Ballarín Cereza, Cornelia Ernst, Aleksis Jeorgulis (Alexis Georgoulis), Ladislav Ilčić, Elena Kundura (Elena Kountoura), Alin Mituța, Günther Sidl, Jordi Solé, Susana Solís Pérez			
Namestniki (člen 209(7)), navzoči pri končnem glasovanju	Aleksander Aleksandrov Jordanov (Alexander Alexandrov Yordanov), Jonás Fernández, Virginie Joron, Radan Kanev, Karin Karlsbro			
Datum predložitve	8.12.2023			

POIMENSKO GLASOVANJE PRI KONČNEM GLASOVANJU V PRISTOJNEM ODBORU

43	+
ECR	Ladislav Ilčić, Izabela-Helena Kloc
ID	Marie Dauchy, Virginie Joron
NI	Aleksis Jeorgulis (Alexis Georgoulis)
PPE	Aleksander Aleksandrov Jordanov (Alexander Alexandrov Yordanov), Hildegard Bentele, Vasile Blaga, Jerzy Buzek, Maria da Graça Carvalho, Pilar del Castillo Vera, Christian Ehler, Radan Kanev, Seán Kelly, Andrius Kubilius, Angelika Niebler, Markus Pieper, Sara Skyttedal, Riho Terras, Pernille Weiss
Renew	Andrus Ansip, Nicola Beer, Nicola Danti, Martina Dlabajová, Valter Flego, Ivars Ijabs, Karin Karlsbro, Iskra Mihajlova (Iskra Mihaylova), Alin Mituța, Morten Petersen, Susana Solís Pérez
S&D	Laura Ballarín Cereza, Josianne Cutajar, Jonás Fernández, Niels Fuglsang, Nicolás González Casares, Ivo Hristov, Romana Jerković, Miapetra Kumpula-Natri, Cvetelina Penkova (Tsvetelina Penkova), Günther Sidl, Carlos Zorrinho
The Left	Elena Kundura (Elena Kountoura)

10	-
ECR	Johan Nissinen, Robert Roos
The Left	Marc Botenga, Cornelia Ernst
Verts/ALE	Michael Bloss, Henrike Hahn, Niklas Nienaß, Mikuláš Peksa, Manuela Ripa, Jordi Solé

1	0
NI	Martin Buschmann

Uporabljeni znaki:
+ : za
- : proti
0 : vzdržani