Evropski parlament
2019-2024

Odbor za zunanje zadeve

2023/0109(COD)

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

PA_Legam

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 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	(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. ***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

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.	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 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.	(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***, ter zmožnost proaktivnega ukrepanja in odločnega odzivanja na kibernetskovarnostne grožnje in incidente***.
[16] https://futureu.europa.eu/en/	[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	(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.	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 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).	(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, ***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	(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.

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 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	(14) V okviru evropskega kibernetskega 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

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.	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 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.	(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 ***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	(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.	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	(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 seznanitvi in morda občutljivo naravo izmenjanih informacij.

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 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	(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***

pravočasno opozarjanje organov in ustreznih subjektov, zlasti z uporabo najnovejših tehnologij umetne inteligence in podatkovne analitike.	***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	(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.	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.	[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, 20.12.2013, str. 924).	[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.	[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	(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.

(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 ***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	(29) V okviru ukrepov pripravljenosti bi bilo treba za spodbujanje doslednega pristopa ter krepitev varnosti po vsej Uniji

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

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 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

bi bilo treba upoštevati tudi priporočilo Sveta o usklajenem vseevropskem pristopu za krepitev odpornosti kritične infrastrukture.

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	(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.	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 ali visoko kritičnih sektorjih.	(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 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	(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.

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 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, 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	(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 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

zaupanja vredne ponudnike v tej uredbi.	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 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;	(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 ***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	(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***;***	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	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

operacije skleneta sporazum o gostiteljstvu in uporabi, ki ureja uporabo orodij in infrastruktur.	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 in uporabi, ki ureja uporabo orodij in infrastruktur.	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 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 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.	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, ***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 bi se olajšalo sodelovanje z vojaškimi akterji.	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 ***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,	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**.**	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	(f) ponudnik ***ima*** tehnično strojno in programsko opremo, potrebno za podporo

podporo zahtevani storitvi;	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, 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.	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***, 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	Komisija do ***[tri*** leta po datumu začetka

uporabe te ***uredbe]*** Evropskemu parlamentu in Svetu predloži poročilo o oceni in pregledu te uredbe.	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