**Európsky parlament**
2019-2024

*Výbor pre zahraničné veci*

**2023/0109(COD)**

27.10.2023

# STANOVISKO

Výboru pre zahraničné veci

pre Výbor pre priemysel, výskum a energetiku

k návrhu nariadenia Európskeho parlamentu a Rady, ktorým sa stanovujú opatrenia na posilnenie solidarity a kapacít v Únii na odhaľovanie kybernetických hrozieb a incidentov, prípravu a reakciu na ne (COM(2023/0209) – C9-0136/2023 – 2023/0109(COD))

Spravodajca výboru požiadaného o stanovisko: Dragoş Tudorache

PA_Legam

**Pozmeňujúci návrh 1**

**Návrh nariadenia**
**Odôvodnenie 1**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| (1) So zvyšovaním miery prepojenia a vzájomnej závislosti našich verejných správ, podnikov, ako aj ***občanov*** bez ohľadu na hranice a odvetvia hospodárstva stúpa význam používania informačných a komunikačných technológií a závislosti od nich vo všetkých odvetviach hospodárskej činnosti. | (1) So zvyšovaním miery prepojenia a vzájomnej závislosti našich verejných správ, podnikov ***a občanov***, ako aj ***vojenských a obranných aktérov*** bez ohľadu na hranice a odvetvia hospodárstva stúpa význam používania informačných a komunikačných technológií a závislosti od nich vo všetkých odvetviach hospodárskej ***a vojenskej*** činnosti. |

**Pozmeňujúci návrh 2**

**Návrh nariadenia**
**Odôvodnenie 2**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| (2) Rozsah, frekvencia a dosah kybernetických incidentov sa zvyšujú, pričom ide aj útoky na dodávateľský reťazec zamerané na kybernetickú špionáž, ransomware alebo narušenie. Tieto incidenty predstavujú závažnú hrozbu pre fungovanie sietí a informačných systémov. Hrozba možných rozsiahlych incidentov, ktoré by mohli významne narušiť alebo poškodiť kritické infraštruktúry, si vzhľadom na rýchly vývoj situácie v oblasti hrozieb vyžaduje vyššiu mieru pripravenosti na všetkých úrovniach rámca kybernetickej bezpečnosti v Únii. ***Táto hrozba nevyplýva*** len z ruskej vojenskej agresie voči Ukrajine a vzhľadom na veľký počet kriminálnych a haktivistických aktérov napojených na štát, ktorí sa podieľajú na aktuálnom geopolitickom napätí, ***môže*** pretrvávať. Takéto incidenty môžu zabraňovať poskytovaniu verejných služieb a realizácii hospodárskych činností, a to aj v kritických odvetviach alebo v odvetviach s vysokou úrovňou | (2) Rozsah, frekvencia a dosah kybernetických incidentov sa zvyšujú, pričom ide aj útoky na dodávateľský reťazec zamerané na kybernetickú špionáž, ransomware alebo narušenie. Tieto incidenty predstavujú závažnú hrozbu pre fungovanie sietí a informačných systémov. Hrozba možných rozsiahlych incidentov, ktoré by mohli významne narušiť alebo poškodiť kritické infraštruktúry, si vzhľadom na rýchly vývoj situácie v oblasti hrozieb vyžaduje vyššiu mieru pripravenosti na všetkých úrovniach rámca kybernetickej bezpečnosti v Únii. ***Závažnosť týchto hrozieb ešte vzrástla v dôsledku návratu vojny na náš kontinent. Tieto hrozby nevyplývajú*** len z ruskej vojenskej agresie voči Ukrajine a vzhľadom na veľký počet kriminálnych a haktivistických aktérov napojených na štát, ktorí sa podieľajú na aktuálnom geopolitickom napätí, ***môžu*** pretrvávať. Takéto incidenty môžu zabraňovať poskytovaniu verejných služieb a realizácii |

| | |
|---|---|
| kritickosti, spôsobovať značné finančné straty, narúšať dôveru používateľa, spôsobovať značné škody hospodárstvu Únie a dokonca by mohli mať zdravie alebo život ohrozujúce dôsledky. Kybernetické incidenty sú navyše nepredvídateľné, keďže často vznikajú a vyvíjajú sa vo veľmi krátkom časovom intervale, nie sú obmedzené na konkrétnu geografickú oblasť a vyskytujú sa súčasne v mnohých krajinách alebo sa v nich ihneď rozširujú. | hospodárskych činností, a to aj v kritických odvetviach alebo v odvetviach s vysokou úrovňou kritickosti, spôsobovať značné finančné straty, narúšať dôveru používateľa, spôsobovať značné škody hospodárstvu ***a bezpečnosti*** Únie a dokonca by mohli mať zdravie alebo život ohrozujúce dôsledky ***tým, že by mohli narušiť činnosť miestnych alebo národných zariadení súvisiacich s bezpečnosťou***. Kybernetické incidenty sú navyše nepredvídateľné, keďže často vznikajú a vyvíjajú sa vo veľmi krátkom časovom intervale, nie sú obmedzené na konkrétnu geografickú oblasť a vyskytujú sa súčasne v mnohých krajinách alebo sa v nich ihneď rozširujú. ***Kybernetická bezpečnosť je dôležitá na ochranu našich európskych hodnôt a zabezpečuje fungovanie našich demokracií tým, že chráni našu volebnú infraštruktúru a demokratické postupy pred akýmkoľvek zahraničným zasahovaním.*** |

**Pozmeňujúci návrh 3**

**Návrh nariadenia**
**Odôvodnenie 2 a (nové)**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| | ***(2a) Kybernetická bezpečnosť má zásadný význam pre zachovanie bezpečnosti našej Únie a zabránenie tomu, aby aktéri s nekalými úmyslami – štátni aj neštátni – oslabovali našu demokraciu, hospodárstvo a bezpečnosť. Nevyhnutné je zabrániť roztrieštenosti, pretože takáto situácia by nebola primeraným prístupom, najmä ak by sme čelili výzve budúceho rozsiahleho kybernetického útoku zameraného na viaceré členské štáty súčasne alebo na nadnárodnú kritickú infraštruktúru. Preto je potrebný orgán Únie, ktorý by pôsobil ako koordinačná platforma pre všetky existujúce a budúce nástroje, fondy*** |

***a mechanizmy kybernetickej bezpečnosti.***

**Pozmeňujúci návrh 4**

**Návrh nariadenia**
**Odôvodnenie 3**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| (3) Je nevyhnutné posilniť konkurenčnú pozíciu odvetví priemyslu a služieb v Únii v rámci celého digitalizovaného hospodárstva a podporiť ich digitálnu transformáciu, a to posilnením úrovne kybernetickej bezpečnosti na digitálnom jednotnom trhu. Podľa odporúčaní v troch rôznych návrhoch Konferencie o budúcnosti Európy[16] je nevyhnutné zvýšiť odolnosť občanov, podnikov a subjektov pôsobiacich v kritických infraštruktúrach voči čoraz väčším kybernetickým hrozbám, ktoré môžu mať zničujúce spoločenské a hospodárske dôsledky. ***Sú*** preto potrebné investície do infraštruktúr a služieb, ktorými sa podporí rýchlejšie odhaľovanie kybernetických hrozieb a incidentov a reakcia na ne, a členské štáty potrebujú pomoc, aby sa mohli lepšie pripraviť na významné a rozsiahle kybernetické incidenty a aby na ne mohli lepšie reagovať. Únia by takisto mala zvýšiť svoje kapacity v týchto oblastiach, predovšetkým v súvislosti so zberom a analýzou údajov o kybernetických hrozbách a incidentoch. | (3) Je nevyhnutné posilniť konkurenčnú pozíciu odvetví priemyslu a služieb v Únii v rámci celého digitalizovaného hospodárstva a podporiť ich digitálnu transformáciu, a to posilnením úrovne kybernetickej bezpečnosti na digitálnom jednotnom trhu. Podľa odporúčaní v troch rôznych návrhoch Konferencie o budúcnosti Európy[16] je nevyhnutné zvýšiť odolnosť občanov, podnikov a subjektov pôsobiacich v kritických infraštruktúrach voči čoraz väčším kybernetickým hrozbám, ktoré môžu mať zničujúce spoločenské a hospodárske dôsledky. Preto ***sú*** potrebné investície do infraštruktúr a služieb, ktorými sa podporí rýchlejšie odhaľovanie kybernetických hrozieb a incidentov a reakcia na ne, a členské štáty potrebujú pomoc, aby sa mohli lepšie pripraviť na významné a rozsiahle kybernetické incidenty a aby na ne mohli lepšie reagovať. Únia by takisto mala zvýšiť svoje kapacity v týchto oblastiach, predovšetkým v súvislosti so zberom a analýzou údajov o kybernetických hrozbách a incidentoch***, a zároveň zlepšiť svoju schopnosť aktívne konať a rozhodne reagovať na kybernetické hrozby a incidenty***. |
| [16] https://futureu.europa.eu/sk/. | [16] https://futureu.europa.eu/sk/. |

**Pozmeňujúci návrh 5**

**Návrh nariadenia**
**Odôvodnenie 4**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| (4) Únia už prijala niekoľko opatrení na zníženie zraniteľnosti a zvýšenie odolnosti kritických infraštruktúr a subjektov voči kybernetickobezpečnostným rizikám, najmä smernicu Európskeho parlamentu a Rady (EÚ) 2022/2555[17], odporúčanie Komisie (EÚ) 2017/1584[18], smernicu Európskeho parlamentu a Rady 2013/40/EÚ[19] a nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881[20]. V odporúčaní Rady o celoúnijnom koordinovanom prístupe k posilneniu odolnosti kritickej infraštruktúry sa členské štáty navyše vyzývajú, aby bezodkladne prijali účinné opatrenia a aby v duchu solidarity zabezpečili lojálnu, účinnú a koordinovanú spoluprácu medzi sebou, s Komisiou a inými príslušnými verejnými orgánmi, ako aj dotknutými subjektmi, a zvýšili tak odolnosť kritickej infraštruktúry, ktorá sa využíva pri poskytovaní základných služieb na vnútornom trhu. | (4) Únia už prijala niekoľko opatrení na zníženie zraniteľnosti a zvýšenie odolnosti kritických infraštruktúr a subjektov voči kybernetickobezpečnostným rizikám, najmä smernicu Európskeho parlamentu a Rady (EÚ) 2022/2555[17], odporúčanie Komisie (EÚ) 2017/1584[18], smernicu Európskeho parlamentu a Rady 2013/40/EÚ[19] a nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881[20]. V odporúčaní Rady o celoúnijnom koordinovanom prístupe k posilneniu odolnosti kritickej infraštruktúry sa členské štáty navyše vyzývajú, aby bezodkladne prijali účinné opatrenia a aby v duchu solidarity zabezpečili lojálnu, účinnú***, proaktívnu*** a koordinovanú spoluprácu medzi sebou, s Komisiou a inými príslušnými verejnými orgánmi, ako aj dotknutými subjektmi, a zvýšili tak odolnosť kritickej infraštruktúry, ktorá sa využíva pri poskytovaní základných služieb na vnútornom trhu. ***Únia okrem toho v marci 2022 schválila a spustila Strategický kompas pre bezpečnosť a obranu, ktorý sa okrem iného zameriava na posilnenie kybernetickej bezpečnosti a prehĺbenie medzinárodnej spolupráce s podobne zmýšľajúcimi spojencami a demokratickými partnermi, a to najmä v tejto oblasti. Kybernetická bezpečnosť je navyše ústredným bodom nedávneho tretieho spoločného vyhlásenia o spolupráci medzi EÚ a NATO z januára 2023. V záverečnej hodnotiacej správe osobitnej skupiny EÚ – NATO sa konkrétne odporúča v plnej miere využívať synergie medzi EÚ a NATO[1] vrátane výmeny najlepších postupov medzi civilnými a vojenskými aktérmi pri vykonávaní príslušných politík a právnych predpisov v oblasti kybernetickej bezpečnosti.*** |
| | ***[1]*** |

| | |
|---|---|
| | ***https://commission.europa.eu/document/34209534-3c59-4b01-b4f0-b2c6ee2df736_en*** |
| [17] Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (Ú. v. EÚ L 333, 27.12.2022, s. 80). | [17] Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (Ú. v. EÚ L 333, 27.12.2022, s. 80). |
| [18] Odporúčanie Komisie (EÚ) 2017/1584 z 13. septembra 2017 o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu (Ú. v. EÚ L 239, 19.9.2017, s. 36). | [18] Odporúčanie Komisie (EÚ) 2017/1584 z 13. septembra 2017 o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu (Ú. v. EÚ L 239, 19.9.2017, s. 36). |
| [19] Smernica Európskeho parlamentu a Rady 2013/40/EÚ z 12. augusta 2013 o útokoch na informačné systémy, ktorou sa nahrádza rámcové rozhodnutie Rady 2005/222/SVV (Ú. v. EÚ L 218, 14.8.2013, s. 8). | [19] Smernica Európskeho parlamentu a Rady 2013/40/EÚ z 12. augusta 2013 o útokoch na informačné systémy, ktorou sa nahrádza rámcové rozhodnutie Rady 2005/222/SVV (Ú. v. EÚ L 218, 14.8.2013, s. 8). |
| [20] Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti) (Ú. v. EÚ L 151, 7.6.2019, s. 15). | [20] Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti) (Ú. v. EÚ L 151, 7.6.2019, s. 15). |

**Pozmeňujúci návrh 6**

**Návrh nariadenia**
**Odôvodnenie 6**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| (6) V spoločnom oznámení o politike EÚ v oblasti kybernetickej obrany[22] prijatom 10. novembra 2022 bola | (6) V spoločnom oznámení o politike EÚ v oblasti kybernetickej obrany[22] prijatom 10. novembra 2022 bola |

| | |
|---|---|
| oznámená iniciatíva na podporu kybernetickej solidarity EÚ, ktorá má tieto ciele: posilniť spoločné spôsobilosti EÚ týkajúce sa odhaľovania, situačnej informovanosti a reakcie presadzovaním zavádzania infraštruktúry centier bezpečnostných operácií v EÚ, podporovať postupné vybudovanie kybernetických rezerv na úrovni EÚ so službami od dôveryhodných súkromných poskytovateľov a podporovať testovanie možných zraniteľností kritických subjektov na základe posúdení rizika na úrovni EÚ. | oznámená iniciatíva na podporu kybernetickej solidarity EÚ, ktorá má tieto ciele: posilniť spoločné spôsobilosti EÚ týkajúce sa odhaľovania, situačnej informovanosti a reakcie presadzovaním zavádzania infraštruktúry centier bezpečnostných operácií v EÚ, podporovať postupné vybudovanie kybernetických rezerv na úrovni EÚ so službami od dôveryhodných súkromných poskytovateľov a podporovať testovanie možných zraniteľností kritických subjektov na základe posúdení rizika na úrovni EÚ. ***Okrem toho rýchlo sa vyvíjajúce prostredie kybernetických hrozieb a rýchle tempo technologického vývoja poukazujú aj na potrebu posilnenia civilno-vojenskej koordinácie a spolupráce, ako zdôraznila Rada vo svojich záveroch o politike EÚ v oblasti kybernetickej obrany[1].***<br><br>***[1] Závery Rady o politike EÚ v oblasti kybernetickej obrany, ktoré Rada schválila na svojom zasadnutí 22. mája 2023 (9618/23).*** |
| [22] Spoločné oznámenie Európskemu parlamentu a Rade Politika EÚ v oblasti kybernetickej obrany [JOIN(2022) 49 final]. | [22] Spoločné oznámenie Európskemu parlamentu a Rade Politika EÚ v oblasti kybernetickej obrany [JOIN(2022) 49 final]. |

**Pozmeňujúci návrh 7**

**Návrh nariadenia**
**Odôvodnenie 6 a (nové)**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| | ***(6a) Vzhľadom na stieranie hraníc medzi sférami civilných a vojenských záležitostí a dvojaké využitie kybernetických nástrojov a technológií je potrebné, aby sa k digitálnej oblasti zaujal komplexný a holistický prístup. V prípade kybernetických incidentov a krízových situácií veľkého rozsahu týkajúcich sa viac ako jedného členského štátu by sa*** |

| | |
|---|---|
| | ***mali zriadiť primerané štruktúry pre krízové riadenie a správu. Takéto štruktúry by mali organizovať výmenu informácií, koordináciu a spoluprácu so štruktúrami Únie pre riadenie vonkajšej bezpečnosti a vojenských kríz a s orgánmi členských štátov zodpovednými za bezpečnosť a obranu (komunita kybernetickej obrany). To by malo platiť aj pre operácie a misie spoločnej bezpečnostnej a obrannej politiky, ktoré Únia uskutočňuje s cieľom zabezpečiť mier a stabilitu vo svojom susedstve aj mimo neho.*** |

**Pozmeňujúci návrh 8**

**Návrh nariadenia**
**Odôvodnenie 7**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| (7) Je nevyhnutné posilniť odhaľovanie kybernetických hrozieb a incidentov a situačnú informovanosť o nich v celej Únii a posilniť solidaritu zvýšením pripravenosti členských štátov a Únie na významné a rozsiahle kybernetické incidenty a ich spôsobilostí reagovať na tieto incidenty. Mala by sa preto zaviesť celoeurópska infraštruktúra centier bezpečnostných operácií (európsky kybernetický štít) s cieľom vybudovať a posilniť spoločné spôsobilosti týkajúce sa odhaľovania a situačnej informovanosti; mal by sa zriadiť mechanizmus na riešenie kybernetickobezpečnostných núdzových situácií s cieľom podporiť členské štáty pri príprave na významné a rozsiahle kybernetické incidenty, pri reakcii na ne a pri okamžitom zotavení sa z nich; mal by sa vytvoriť mechanizmus preskúmania kybernetických incidentov, ktorý bude slúžiť na skúmanie a posudzovanie konkrétnych významných alebo rozsiahlych incidentov. Týmito opatreniami nie sú dotknuté články 107 a 108 Zmluvy o fungovaní Európskej únie | (7) Je nevyhnutné posilniť odhaľovanie kybernetických hrozieb a incidentov a situačnú informovanosť o nich v celej Únii a posilniť solidaritu zvýšením pripravenosti členských štátov a Únie na významné a rozsiahle kybernetické incidenty a ich spôsobilostí reagovať na tieto incidenty. Mala by sa preto zaviesť celoeurópska infraštruktúra centier bezpečnostných operácií (európsky kybernetický štít) s cieľom vybudovať a posilniť spoločné spôsobilosti týkajúce sa odhaľovania a situačnej informovanosti; mal by sa zriadiť mechanizmus na riešenie kybernetickobezpečnostných núdzových situácií s cieľom podporiť členské štáty pri príprave na významné a rozsiahle kybernetické incidenty, pri reakcii na ne a pri okamžitom zotavení sa z nich ***vrátane incidentov zahŕňajúcich viac ako jeden členský štát. V prípadoch, keď je to uskutočniteľné a potrebné, by mal mechanizmus na riešenie kybernetickobezpečnostných núdzových situácií organizovať výmenu informácií a spoluprácu s obrannými orgánmi*** |

(ďalej len „ZFEÚ“).

***členských štátov za podpory inštitúcií, orgánov a agentúr EÚ (komunita EÚ v oblasti kybernetickej obrany)***; mal by sa vytvoriť mechanizmus preskúmania kybernetických incidentov, ktorý bude slúžiť na skúmanie a posudzovanie konkrétnych významných alebo rozsiahlych incidentov***. Tieto nové štruktúry by mali podporovať aj operácie a misie SBOP EÚ***. Týmito opatreniami nie sú dotknuté články 107 a 108 Zmluvy o fungovaní Európskej únie (ďalej len „ZFEÚ“).

**Pozmeňujúci návrh 9**

**Návrh nariadenia**
**Odôvodnenie 11**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| (11) Na účely správneho finančného riadenia by sa mali stanoviť osobitné pravidlá pre prenos nepoužitých viazaných a platobných rozpočtových prostriedkov. Pri dodržiavaní zásady, že rozpočet Únie sa stanovuje ročne, by sa týmto nariadením s ohľadom na nepredvídateľný, neobyčajný a špecifický charakter prostredia kybernetickej bezpečnosti mala nad rámec možností stanovených v nariadení o rozpočtových pravidlách stanoviť možnosť preniesť nepoužité finančné prostriedky, a tak maximalizovať kapacitu mechanizmu na riešenie kybernetickobezpečnostných núdzových situácií podporovať členské štáty v účinnom boji proti kybernetickým hrozbám. | (11) Na účely správneho finančného riadenia by sa mali stanoviť osobitné pravidlá pre prenos nepoužitých viazaných a platobných rozpočtových prostriedkov. Pri dodržiavaní zásady, že rozpočet Únie sa stanovuje ročne, by sa týmto nariadením s ohľadom na nepredvídateľný, neobyčajný a špecifický charakter prostredia kybernetickej bezpečnosti mala nad rámec možností stanovených v nariadení o rozpočtových pravidlách stanoviť možnosť preniesť nepoužité finančné prostriedky, a tak maximalizovať kapacitu mechanizmu na riešenie kybernetickobezpečnostných núdzových situácií podporovať členské štáty v účinnom boji proti kybernetickým hrozbám. ***Tieto osobitné pravidlá by takisto umožnili dlhodobejšiu finančnú podporu spoločného obstarávania ultrabezpečných nástrojov a infraštruktúry novej generácie s cieľom zlepšiť kapacity kolektívneho odhaľovania využitím najnovších technológií umelej inteligencie a analýzy údajov.*** |

**Pozmeňujúci návrh 10**

**Návrh nariadenia**
**Odôvodnenie 13**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| (13) Každý členský štát by mal na vnútroštátnej úrovni určiť verejný subjekt poverený v danom členskom štáte koordináciou činností v oblasti odhaľovania kybernetických hrozieb. Tieto vnútroštátne centrá bezpečnostných operácií by mali fungovať ako referenčné miesto a brána na vnútroštátnej úrovni, pokiaľ ide o účasť na európskom kybernetickom štíte, a mali by zabezpečiť na vnútroštátnej úrovni účinnú a efektívnu výmenu a zber informácií o kybernetických hrozbách od verejných a súkromných subjektov. | (13) Každý členský štát by mal na vnútroštátnej úrovni určiť verejný subjekt poverený v danom členskom štáte koordináciou činností v oblasti odhaľovania kybernetických hrozieb. Tieto vnútroštátne centrá bezpečnostných operácií by mali fungovať ako referenčné miesto a brána na vnútroštátnej úrovni, pokiaľ ide o účasť na európskom kybernetickom štíte, a mali by zabezpečiť na vnútroštátnej úrovni účinnú a efektívnu výmenu a zber informácií o kybernetických hrozbách od verejných a súkromných subjektov. ***V prípadoch, keď je to uskutočniteľné a potrebné, by centrá bezpečnostných operácií mali tiež umožniť účasť obranných subjektov vytvorením tzv. obranného piliera z hľadiska riadenia a druhu vymieňaných informácií, ako sa uvádza v spoločnom oznámení o politike EÚ v oblasti kybernetickej obrany[1], a to s podporou vysokého predstaviteľa.*** |
| | ***[1] Spoločné oznámenie Európskemu parlamentu a Rade, Politika EÚ v oblasti kybernetickej obrany [JOIN(2022) 49 final].*** |

**Pozmeňujúci návrh 11**

**Návrh nariadenia**
**Odôvodnenie 14**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| (14) V rámci európskeho kybernetického štítu by sa malo zriadiť viacero cezhraničných centier bezpečnostných operácií. V nich by sa mali | (14) V rámci európskeho kybernetického štítu by sa malo zriadiť viacero cezhraničných centier bezpečnostných operácií. V nich by sa mali |

| | |
|---|---|
| združovať vnútroštátne centrá bezpečnostných operácií aspoň z troch členských štátov, aby bolo možné v plnej miere dosiahnuť prínos z cezhraničného odhaľovania hrozieb a výmeny a riadenia informácií. Všeobecným cieľom cezhraničných centier bezpečnostných operácií by malo byť posilnenie kapacít týkajúcich sa analýzy kybernetickobezpečnostných hrozieb, predchádzania týmto hrozbám a ich odhaľovania a podpora získavania kvalitných spravodajských informácií o kybernetickobezpečnostných hrozbách, predovšetkým prostredníctvom spoločného využívania údajov z rozličných zdrojov, verejných či súkromných, ako aj prostredníctvom výmeny a spoločného využívania najmodernejších nástrojov a spoločného rozvoja spôsobilostí týkajúcich sa odhaľovania, analýzy a prevencie v dôveryhodnom prostredí. Centrá by mali vytvárať nové dodatočné kapacity, ktoré by vychádzali z existujúcich centier bezpečnostných operácií a jednotiek pre riešenie počítačových bezpečnostných incidentov (ďalej len „jednotky CSIRT“) a iných príslušných aktérov a dopĺňali ich. | združovať vnútroštátne centrá bezpečnostných operácií aspoň z troch členských štátov ***vrátane tzv. obranného piliera***, aby bolo možné v plnej miere dosiahnuť prínos z cezhraničného odhaľovania hrozieb a výmeny a riadenia informácií. Všeobecným cieľom cezhraničných centier bezpečnostných operácií by malo byť posilnenie kapacít týkajúcich sa analýzy kybernetickobezpečnostných hrozieb, predchádzania týmto hrozbám a ich odhaľovania a podpora získavania kvalitných spravodajských informácií o kybernetickobezpečnostných hrozbách, predovšetkým prostredníctvom spoločného využívania údajov z rozličných zdrojov, verejných či súkromných, ***a v prípadoch, keď je to potrebné a uskutočniteľné, z vojenských zdrojov s dostatočnými usmerneniami na výmenu informácií,*** ako aj prostredníctvom výmeny a spoločného využívania najmodernejších nástrojov a spoločného rozvoja spôsobilostí týkajúcich sa odhaľovania, analýzy a prevencie v dôveryhodnom prostredí. Centrá by mali vytvárať nové dodatočné kapacity, ktoré by vychádzali z existujúcich centier bezpečnostných operácií a jednotiek pre riešenie počítačových bezpečnostných incidentov (ďalej len „jednotky CSIRT“) a iných príslušných aktérov a dopĺňali ich. |

**Pozmeňujúci návrh 12**

**Návrh nariadenia**
**Odôvodnenie 15**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| (15) Na vnútroštátnej úrovni zabezpečujú monitorovanie, odhaľovanie a analýzu kybernetických hrozieb zvyčajne centrá bezpečnostných operácií verejných a súkromných subjektov v kombinácii s jednotkami CSIRT. Jednotky CSIRT si okrem toho v súlade so smernicou (EÚ) | (15) Na vnútroštátnej úrovni zabezpečujú monitorovanie, odhaľovanie a analýzu kybernetických hrozieb zvyčajne centrá bezpečnostných operácií verejných a súkromných subjektov v kombinácii s jednotkami CSIRT. Jednotky CSIRT si okrem toho v súlade so smernicou (EÚ) |

2022/2555 vymieňajú informácie v rámci siete jednotiek CSIRT. Cezhraničné centrá bezpečnostných operácií by mali predstavovať novú kapacitu, ktorá bude dopĺňať sieť jednotiek CSIRT tým, že budú zhromažďovať údaje o kybernetickobezpečnostných hrozbách od verejných a súkromných subjektov a zabezpečovať spoločné využívanie týchto údajov, zvyšovať ich hodnotu prostredníctvom odborných analýz, spoločne nadobudnutých infraštruktúr a najmodernejších nástrojov a prispievať k rozvoju spôsobilostí a ***technologickej suverenity*** Únie.

2022/2555 vymieňajú informácie v rámci siete jednotiek CSIRT. Cezhraničné centrá bezpečnostných operácií by mali predstavovať novú kapacitu, ktorá bude dopĺňať sieť jednotiek CSIRT tým, že budú zhromažďovať údaje o kybernetickobezpečnostných hrozbách od verejných a súkromných subjektov a zabezpečovať spoločné využívanie týchto údajov, zvyšovať ich hodnotu prostredníctvom odborných analýz, spoločne nadobudnutých infraštruktúr a najmodernejších nástrojov a prispievať k rozvoju spôsobilostí a ***odolnosti*** Únie.

**Pozmeňujúci návrh 13**

**Návrh nariadenia**
**Odôvodnenie 16**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| (16) Cezhraničné centrá bezpečnostných operácií by mali fungovať ako ústredné kontaktné miesto umožňujúce rozsiahle zhromažďovanie relevantných údajov a spravodajských informácií o kybernetických hrozbách, ktoré umožňuje rozširovanie informácií o hrozbách rozsiahlemu a rozmanitému súboru aktérov [napr. tímom reakcie na núdzové počítačové situácie (ďalej len „CERT“), jednotkám CSIRT, strediskám pre výmenu a analýzu informácií, prevádzkovateľom kritických ***infraštruktúr]***. Medzi informácie, ktoré sú predmetom výmeny medzi účastníkmi cezhraničného centra bezpečnostných operácií, by mohli patriť údaje zo sietí a senzorov, z informačných kanálov pre spravodajské informácie o hrozbách, z indikátorov ohrozenia a z kontextualizované informácie o incidentoch, hrozbách a zraniteľnostiach. Navyše by cezhraničné centrá bezpečnostných operácií mali takisto uzatvárať dohody o spolupráci s inými | (16) Cezhraničné centrá bezpečnostných operácií by mali fungovať ako ústredné kontaktné miesto umožňujúce rozsiahle zhromažďovanie relevantných údajov a spravodajských informácií o kybernetických hrozbách, ktoré umožňuje rozširovanie informácií o hrozbách rozsiahlemu a rozmanitému súboru aktérov [napr. tímom reakcie na núdzové počítačové situácie (ďalej len „CERT“), jednotkám CSIRT, strediskám pre výmenu a analýzu informácií, prevádzkovateľom kritických ***infraštruktúr, ako aj komunite kybernetickej obrany]***. Medzi informácie, ktoré sú predmetom výmeny medzi účastníkmi cezhraničného centra bezpečnostných operácií, by mohli patriť údaje zo sietí a senzorov, z informačných kanálov pre spravodajské informácie o hrozbách, z indikátorov ohrozenia a z kontextualizované informácie o incidentoch, hrozbách a zraniteľnostiach. Navyše by cezhraničné centrá bezpečnostných operácií mali takisto |

| | |
|---|---|
| cezhraničnými centrami bezpečnostných operácií. | uzatvárať dohody o spolupráci s inými cezhraničnými centrami bezpečnostných operácií ***a operačnou sieťou pre tímy milCERT (MICNET), keď bude zriadená***. |

**Pozmeňujúci návrh 14**

**Návrh nariadenia**
**Odôvodnenie 17**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| (17) Spoločná situačná informovanosť relevantných orgánov je nevyhnutnou podmienkou pripravenosti a koordinácie celej Únie, pokiaľ ide o významné a rozsiahle kybernetické incidenty. Smernicou (EÚ) 2022/2555 sa zriaďuje sieť EU-CyCLONe s cieľom podporiť koordinované riadenie rozsiahlych kybernetických incidentov a kríz na operačnej úrovni a zabezpečiť pravidelnú výmenu relevantných informácií medzi členskými štátmi a inštitúciami, orgánmi a agentúrami Únie. Odporúčanie (EÚ) 2017/1584 o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu sa zaoberá úlohou všetkých príslušných aktérov. V smernici (EÚ) 2022/2555 sa takisto pripomína zodpovednosť Komisie v rámci mechanizmu Únie v oblasti civilnej ochrany zriadeného rozhodnutím Európskeho parlamentu a Rady č. 1313/2013/EÚ, ako aj jej zodpovednosť za poskytovanie analytických správ týkajúcich sa dojednaní mechanizmu integrovanej politickej reakcie na krízu podľa vykonávacieho rozhodnutia (EÚ) 2018/1993. Cezhraničné centrá bezpečnostných operácií by preto v situáciách, keď získajú informácie týkajúce sa potenciálneho alebo prebiehajúceho rozsiahleho kybernetického incidentu, mali poskytnúť relevantné informácie sieti EU-CyCLONe, sieti jednotiek CSIRT a Komisii. V závislosti od situácie by medzi informácie určené na | (17) Spoločná situačná informovanosť relevantných orgánov je nevyhnutnou podmienkou pripravenosti a koordinácie celej Únie, pokiaľ ide o významné a rozsiahle kybernetické incidenty. Smernicou (EÚ) 2022/2555 sa zriaďuje sieť EU-CyCLONe s cieľom podporiť koordinované riadenie rozsiahlych kybernetických incidentov a kríz na operačnej úrovni a zabezpečiť pravidelnú výmenu relevantných informácií medzi členskými štátmi a inštitúciami, orgánmi a agentúrami Únie. Odporúčanie (EÚ) 2017/1584 o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu sa zaoberá úlohou všetkých príslušných aktérov. V smernici (EÚ) 2022/2555 sa takisto pripomína zodpovednosť Komisie v rámci mechanizmu Únie v oblasti civilnej ochrany zriadeného rozhodnutím Európskeho parlamentu a Rady č. 1313/2013/EÚ, ako aj jej zodpovednosť za poskytovanie analytických správ týkajúcich sa dojednaní mechanizmu integrovanej politickej reakcie na krízu podľa vykonávacieho rozhodnutia (EÚ) 2018/1993. Cezhraničné centrá bezpečnostných operácií by preto v situáciách, keď získajú informácie týkajúce sa potenciálneho alebo prebiehajúceho rozsiahleho kybernetického incidentu, mali poskytnúť relevantné informácie sieti EU-CyCLONe, sieti jednotiek CSIRT***, komunite kybernetickej obrany*** a Komisii. V závislosti od situácie |

| | |
|---|---|
| spoločné využívanie mohli patriť najmä technické informácie, informácie o povahe a motívoch útočníka alebo potenciálneho útočníka a netechnické informácie vyššej úrovne o potenciálnom alebo prebiehajúcom rozsiahlom kybernetickom incidente. V tejto súvislosti by sa mala náležitá pozornosť venovať zásade potreby poznať a potenciálne citlivej povahe vymieňaných informácií. | by medzi informácie určené na spoločné využívanie mohli patriť najmä technické informácie, informácie o povahe a motívoch útočníka alebo potenciálneho útočníka a netechnické informácie vyššej úrovne o potenciálnom alebo prebiehajúcom rozsiahlom kybernetickom incidente. V tejto súvislosti by sa mala náležitá pozornosť venovať zásade potreby poznať a potenciálne citlivej povahe vymieňaných informácií. |

**Pozmeňujúci návrh 15**

**Návrh nariadenia**
**Odôvodnenie 19**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| (19) S cieľom umožniť výmenu údajov o kybernetickobezpečnostných hrozbách z rôznych zdrojov, v širokom meradle a v dôveryhodnom prostredí by subjekty zúčastnené na európskom kybernetickom štíte mali byť vybavené najmodernejšími a mimoriadne bezpečnými nástrojmi, vybavením a infraštruktúrami. To by malo umožniť zlepšenie kapacít kolektívneho odhaľovania a včasného varovania pre orgány a príslušné subjekty, predovšetkým prostredníctvom používania najnovších technológií umelej inteligencie a analýzy údajov. | (19) S cieľom umožniť výmenu údajov o kybernetickobezpečnostných hrozbách z rôznych zdrojov, v širokom meradle a v dôveryhodnom prostredí by subjekty zúčastnené na európskom kybernetickom štíte mali byť vybavené najmodernejšími a mimoriadne bezpečnými nástrojmi, vybavením a infraštruktúrami***, pričom sa vylúčia vysokorizikoví dodávatelia kritických produktov s digitálnymi prvkami***. To by malo umožniť zlepšenie kapacít kolektívneho odhaľovania a včasného varovania pre orgány a príslušné subjekty, predovšetkým prostredníctvom používania najnovších technológií umelej inteligencie a analýzy údajov. ***Pri používaní umelej inteligencie by sa mal zabezpečiť ľudský dohľad a mala by sa zaistiť dostatočná úroveň gramotnosti v oblasti umelej inteligencie, potrebná podpora a právomoc na vykonávanie tejto funkcie.*** |

**Pozmeňujúci návrh 16**

**Návrh nariadenia**
**Odôvodnenie 19 a (nové)**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| | ***(19a) V súlade s nariadením [XX/XXXX (akt o kybernetickej odolnosti)] by sa aj na subjekty zúčastnené na európskom kybernetickom štíte mali vzťahovať požiadavky stanovené v tomto nariadení, pokiaľ ide o všetky produkty s digitálnymi prvkami. Vzhľadom na rastúce riziká vyplývajúce z hospodárskej závislosti je potrebné minimalizovať vystavenie vysokorizikovým dodávateľom kritických produktov prostredníctvom spoločného strategického rámca pre hospodársku bezpečnosť EÚ. Závislosť od vysokorizikových dodávateľov kritických produktov s digitálnymi prvkami predstavuje strategické riziko, ktoré by sa malo riešiť na úrovni Únie, najmä ak sa krajina zapája do priemyselnej špionáže alebo vyvíja hospodársky nátlak a jej právne predpisy nariaďujú svojvoľný prístup k akémukoľvek druhu operácií alebo údajov spoločností, a to najmä ak sú kritické produkty určené na použitie kľúčovými subjektmi uvedenými v smernici (EÚ) 2022/2555.*** |

**Pozmeňujúci návrh 17**

**Návrh nariadenia**
**Odôvodnenie 20**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| (20) Vďaka zberu, spoločnému využívaniu a výmene údajov by európsky kybernetický štít mal posilniť technologickú suverenitu Únie. Zhromažďovanie vybratých údajov vysokej kvality by malo takisto prispieť k rozvoju vyspelých technológií umelej inteligencie a analýzy údajov. To by sa malo uľahčiť prepojením európskeho kybernetického štítu s celoeurópskou infraštruktúrou vysokovýkonnej výpočtovej techniky zriadenou nariadením | (20) Vďaka zberu, spoločnému využívaniu a výmene údajov by európsky kybernetický štít mal posilniť technologickú suverenitu***, strategickú autonómiu, konkurencieschopnosť a odolnosť*** Únie. Zhromažďovanie vybratých údajov vysokej kvality by malo takisto prispieť k rozvoju vyspelých technológií umelej inteligencie a analýzy údajov. To by sa malo uľahčiť prepojením európskeho kybernetického štítu s celoeurópskou infraštruktúrou |

Rady (EÚ) 2021/1173[25].

vysokovýkonnej výpočtovej techniky zriadenou nariadením Rady (EÚ) 2021/1173[25].

[25] Nariadenie Rady (EÚ) 2021/1173 z 13. júla 2021 o zriadení spoločného podniku pre európsku vysokovýkonnú výpočtovú techniku a o zrušení nariadenia (EÚ) 2018/1488 (Ú. v. EÚ L 256, 19.7.2021, s. 3).

[25] Nariadenie Rady (EÚ) 2021/1173 z 13. júla 2021 o zriadení spoločného podniku pre európsku vysokovýkonnú výpočtovú techniku a o zrušení nariadenia (EÚ) 2018/1488 (Ú. v. EÚ L 256, 19.7.2021, s. 3).

**Pozmeňujúci návrh 18**

**Návrh nariadenia**
**Odôvodnenie 25**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| (25) Mechanizmus na riešenie kybernetických núdzových situácií by mal poskytovať podporu členským štátom, ktorá bude dopĺňať ich vlastné opatrenia a zdroje a ďalšie existujúce možnosti podpory v prípade reakcie na významné a rozsiahle kybernetické incidenty a okamžitého zotavenia sa z nich, ako sú služby poskytované Agentúrou Európskej únie pre kybernetickú bezpečnosť (ďalej len „ENISA“) v súlade s jej mandátom, koordinovaná reakcia a pomoc siete jednotiek CSIRT, podpora na zmierňovanie od siete EU-CyCLONe, ako aj vzájomná pomoc medzi členskými štátmi aj v súvislosti s článkom 42 ods. 7 ZEÚ, tímy rýchlej kybernetickej reakcie stálej štruktúrovanej spolupráce (PESCO)***26*** a tímy rýchlej reakcie na hybridné hrozby. Týmto mechanizmom by sa mala riešiť potreba zabezpečiť, aby na účely podpory pripravenosti na kybernetické incidenty a reakcie na ne v celej Únii a v tretích krajinách ***boli k dispozícii špecializované prostriedky***. | (25) Mechanizmus na riešenie kybernetických núdzových situácií by mal poskytovať podporu členským štátom, ktorá bude dopĺňať ich vlastné opatrenia a zdroje a ďalšie existujúce možnosti podpory v prípade reakcie na významné a rozsiahle kybernetické incidenty a okamžitého zotavenia sa z nich, ako sú služby poskytované Agentúrou Európskej únie pre kybernetickú bezpečnosť (ďalej len „ENISA“) v súlade s jej mandátom, koordinovaná reakcia a pomoc siete jednotiek CSIRT, podpora na zmierňovanie od siete EU-CyCLONe, ako aj vzájomná pomoc medzi členskými štátmi aj v súvislosti s článkom 42 ods. 7 ZEÚ, tímy rýchlej kybernetickej reakcie stálej štruktúrovanej spolupráce (PESCO)***[1], nový projekt PESCO Koordinačné centrum pre kybernetickú a informačnú oblasť (CIDCC) a jeho navrhovaný nástupca Koordinačné centrum kybernetickej obrany EÚ (EUCDCC),*** a tímy rýchlej reakcie na hybridné hrozby. Týmto mechanizmom by sa mala riešiť potreba zabezpečiť, aby na účely podpory pripravenosti na kybernetické incidenty a reakcie na ne ***boli k dispozícii špecializované prostriedky*** v celej Únii a v |

tretích krajinách***, a to najmä v tých kandidátskych krajinách EÚ, ktoré dosiahli súlad so spoločnou zahraničnou a bezpečnostnou politikou a spoločnou bezpečnostnou a obrannou politikou EÚ, s cieľom podporiť ich pri budovaní kybernetických spôsobilostí a posilňovaní cezhraničnej a regionálnej spolupráce medzi týmito kandidátskymi krajinami v oblasti kybernetickej bezpečnosti***.

***[1] ROZHODNUTIE RADY (SZBP) 2017/2315 z 11. decembra 2017 o nadviazaní stálej štruktúrovanej spolupráce (PESCO) a stanovení zoznamu zúčastnených členských štátov.***

---

[26] ROZHODNUTIE RADY (SZBP) 2017/2315 z 11. decembra 2017 o nadviazaní stálej štruktúrovanej spolupráce (PESCO) a stanovení zoznamu zúčastnených členských štátov.

---

[26] ROZHODNUTIE RADY (SZBP) 2017/2315 z 11. decembra 2017 o nadviazaní stálej štruktúrovanej spolupráce (PESCO) a stanovení zoznamu zúčastnených členských štátov.

**Pozmeňujúci návrh 19**

**Návrh nariadenia**
**Odôvodnenie 26**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| (26) Týmto nástrojom nie sú dotknuté postupy a rámce na koordináciu reakcie na krízu na úrovni Únie, najmä mechanizmus Únie v oblasti civilnej ochrany[27], mechanizmus integrovanej politickej reakcie na krízu[28], a smernica (EÚ) 2022/2555. Nástroj môže prispievať k opatreniam vykonávaným v kontexte článku 42 ods. 7 ZEÚ alebo v situáciách vymedzených v článku 222 ZFEÚ alebo ich môže dopĺňať. Využívanie tohto nástroja by sa ***malo v prípade potreby*** koordinovať s vykonávaním opatrení súboru nástrojov kybernetickej diplomacie. | (26) Týmto nástrojom nie sú dotknuté postupy a rámce na koordináciu reakcie na krízu na úrovni Únie, najmä mechanizmus Únie v oblasti civilnej ochrany[27], mechanizmus integrovanej politickej reakcie na krízu[28], a smernica (EÚ) 2022/2555. Nástroj môže prispievať k opatreniam vykonávaným v kontexte článku 42 ods. 7 ZEÚ alebo v situáciách vymedzených v článku 222 ZFEÚ alebo ich môže dopĺňať. Využívanie tohto nástroja by sa ***tiež malo*** koordinovať s vykonávaním opatrení súboru nástrojov kybernetickej diplomacie***, čím sa posilní spolupráca na strategickej, operačnej a technickej úrovni medzi komunitou kybernetickej obrany a inými*** |

| | |
|---|---|
| | ***kybernetickými komunitami, najmä s cieľom posilniť spôsobilosti v boji proti kybernetickým hrozbám z krajín mimo Únie vrátane reštriktívnych opatrení, ktoré možno použiť na predchádzanie škodlivým kybernetickým činnostiam a reakciu na ne***. |
| [27] Rozhodnutie Európskeho parlamentu a Rady č. 1313/2013/EÚ zo 17. decembra 2013 o mechanizme Únie v oblasti civilnej ochrany (Ú. v. EÚ L 347, 20.12.2013, s. 924). | [27] Rozhodnutie Európskeho parlamentu a Rady č. 1313/2013/EÚ zo 17. decembra 2013 o mechanizme Únie v oblasti civilnej ochrany (Ú. v. EÚ L 347, 20.12.2013, s. 924). |
| [28] Mechanizmus integrovanej politickej reakcie na krízu a v súlade s odporúčaním Komisie (EÚ) 2017/1584 z 13. septembra 2017 o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu. | [28] Mechanizmus integrovanej politickej reakcie na krízu a v súlade s odporúčaním Komisie (EÚ) 2017/1584 z 13. septembra 2017 o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu. |

**Pozmeňujúci návrh 20**

**Návrh nariadenia**
**Odôvodnenie 28**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| (28) Podľa smernice (EÚ) 2022/2555 musia členské štáty určiť alebo zriadiť aspoň jeden orgán pre riadenie kybernetických kríz a musia zabezpečiť, aby tieto orgány mali primerané zdroje na účinné a efektívne vykonávanie svojich úloh. Členské štáty podľa nej musia ďalej určiť spôsobilosti, aktíva a postupy, ktoré možno použiť v prípade krízy, a musia prijať národný plán reakcie na rozsiahle kybernetické incidenty a krízy, v ktorom sa stanovia ciele a spôsoby riadenia rozsiahlych kybernetických incidentov a kríz. Členské štáty takisto musia zriadiť jednu alebo viacero jednotiek CSIRT poverených zodpovednosťou za riešenie incidentov podľa presne stanoveného postupu, ktoré sa budú zaoberať prinajmenšom odvetviami, pododvetviami | (28) Podľa smernice (EÚ) 2022/2555 musia členské štáty určiť alebo zriadiť aspoň jeden orgán pre riadenie kybernetických kríz a musia zabezpečiť, aby tieto orgány mali primerané zdroje na účinné a efektívne vykonávanie svojich úloh. Členské štáty podľa nej musia ďalej určiť spôsobilosti, aktíva a postupy, ktoré možno použiť v prípade krízy, a musia prijať národný plán reakcie na rozsiahle kybernetické incidenty a krízy, v ktorom sa stanovia ciele a spôsoby riadenia rozsiahlych kybernetických incidentov a kríz. Členské štáty takisto musia zriadiť jednu alebo viacero jednotiek CSIRT poverených zodpovednosťou za riešenie incidentov podľa presne stanoveného postupu, ktoré sa budú zaoberať prinajmenšom odvetviami, pododvetviami |

| | |
|---|---|
| a druhmi subjektov, ktoré patria do rozsahu pôsobnosti uvedenej smernice, a musia zabezpečiť, aby tieto jednotky mali primerané zdroje na účinné plnenie svojich úloh. Týmto nariadením nie je dotknutá úloha Komisie pri zabezpečovaní dodržiavania povinností vyplývajúcich zo smernice (EÚ) 2022/2555 členskými štátmi. Mechanizmus na riešenie kybernetických núdzových situácií by mal poskytovať pomoc pri opatreniach zameraných na posilňovanie pripravenosti, ako aj pri opatreniach reakcie na incidenty s cieľom zmierniť vplyv významných a rozsiahlych kybernetických incidentov, podporovať okamžité zotavenie sa a/alebo obnoviť fungovanie základných služieb. | a druhmi subjektov, ktoré patria do rozsahu pôsobnosti uvedenej smernice, a musia zabezpečiť, aby tieto jednotky mali primerané zdroje na účinné plnenie svojich úloh. Týmto nariadením nie je dotknutá úloha Komisie pri zabezpečovaní dodržiavania povinností vyplývajúcich zo smernice (EÚ) 2022/2555 členskými štátmi. Mechanizmus na riešenie kybernetických núdzových situácií by mal poskytovať pomoc pri opatreniach zameraných na posilňovanie pripravenosti, ako aj pri opatreniach reakcie na incidenty s cieľom zmierniť vplyv významných a rozsiahlych kybernetických incidentov, podporovať okamžité zotavenie sa a/alebo obnoviť fungovanie základných služieb***, pričom sa primerane využije celý rad obranných možností, ktoré majú civilné a vojenské komunity k dispozícii***. |

**Pozmeňujúci návrh 21**

**Návrh nariadenia**
**Odôvodnenie 29**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| (29) V rámci opatrení v oblasti pripravenosti a v záujme presadzovania jednotného prístupu a zvýšenia bezpečnosti v celej Únii a na jej vnútornom trhu by sa mala poskytovať koordinovaná podpora na testovanie a posudzovanie kybernetickej bezpečnosti subjektov pôsobiacich v odvetviach s vysokou úrovňou kritickosti určených v súlade so smernicou (EÚ) 2022/2555. Na tento účel by Komisia s podporou agentúry ENISA a v spolupráci so skupinou pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti zriadenou na základe smernice (EÚ) 2022/2555 mala pravidelne určovať relevantné odvetvia alebo pododvetvia, ktoré by mali byť oprávnené prijímať finančnú podporu na koordinované testovanie na úrovni Únie. ***Odvetvia*** alebo ***pododvetvia*** by sa mali vyberať z prílohy I | (29) V rámci opatrení v oblasti pripravenosti a v záujme presadzovania jednotného prístupu a zvýšenia bezpečnosti v celej Únii a na jej vnútornom trhu by sa mala poskytovať koordinovaná podpora na testovanie a posudzovanie kybernetickej bezpečnosti subjektov pôsobiacich v odvetviach s vysokou úrovňou kritickosti určených v súlade so smernicou (EÚ) 2022/2555. Na tento účel by Komisia s podporou agentúry ENISA a v spolupráci so skupinou pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti zriadenou na základe smernice (EÚ) 2022/2555 mala pravidelne určovať relevantné odvetvia alebo pododvetvia, ktoré by mali byť oprávnené prijímať finančnú podporu na koordinované testovanie na úrovni Únie. ***V prípade potreby by sa Európska služba pre*** |

k smernici (EÚ) 2022/2555 (ďalej len „odvetvia s vysokou úrovňou kritickosti“). Výkon koordinovaného testovania by mal vychádzať zo spoločných scenárov rizika a metodík. Aj vzhľadom na potrebu zabrániť duplicite by sa pri výbere odvetví a vypracúvaní scenárov rizika mali zohľadniť relevantné posúdenia rizík a scenáre rizika pre celú Úniu, ako sú napríklad hodnotenia rizík a scenáre rizika požadované v záveroch Rady o vývoji prístupu Európskej únie ku kybernetickej bezpečnosti, ktoré má vykonávať Komisia, vysoký predstaviteľ a skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti v spolupráci s príslušnými civilnými a vojenskými orgánmi a agentúrami a vytvorenými sieťami vrátane siete EU-CyCLONe, ako aj posúdenie rizika komunikačných sietí a infraštruktúr požadované v spoločnej ministerskej výzve z Nevers, ktoré vykonáva skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti s podporou Komisie a agentúry ENISA a v spolupráci s Orgánom európskych regulátorov pre elektronické komunikácie, koordinované posúdenia rizík, ktoré sa majú vykonávať podľa článku 22 smernice (EÚ) 2022/2555, a testovanie digitálnej prevádzkovej odolnosti stanovené v nariadení Európskeho parlamentu a Rady (EÚ) 2022/2554***29***. Pri výbere odvetví by sa malo zohľadniť aj odporúčanie Rady o celoúnijnom koordinovanom prístupe k posilneniu odolnosti kritickej infraštruktúry.

***vonkajšiu činnosť (ESVČ), najmä prostredníctvom Spravodajského centra EÚ (INTCEN) a jeho strediska pre hybridné hrozby, s podporou riaditeľstva spravodajskej služby Vojenského štábu Európskej únie (EUMS) v rámci jednotnej kapacity na analýzu spravodajských informácií (SIAC), mala zapojiť aj do poskytovania aktuálnych posúdení, a tak prispievať k identifikácii odvetví*** alebo ***pododvetví, ktoré*** by sa mali vyberať z prílohy I k smernici (EÚ) 2022/2555 (ďalej len „odvetvia s vysokou úrovňou kritickosti“). Výkon koordinovaného testovania by mal vychádzať zo spoločných scenárov rizika a metodík***. Tieto testovania by mali zohrávať dôležitú úlohu aj pri zlepšovaní spolupráce medzi civilnými a vojenskými subjektmi. Pri organizovaní testovania by preto Komisia, ESVČ a agentúra ENISA mali systematicky zvažovať zapojenie účastníkov z iných kybernetických komunít, ako je napr. Európska obranná agentúra (EDA) a iné príslušné subjekty.*** Aj vzhľadom na potrebu zabrániť duplicite by sa pri výbere odvetví a vypracúvaní scenárov rizika mali zohľadniť relevantné posúdenia rizík a scenáre rizika pre celú Úniu, ako sú napríklad hodnotenia rizík a scenáre rizika požadované v záveroch Rady o vývoji prístupu Európskej únie ku kybernetickej bezpečnosti, ktoré má vykonávať Komisia, vysoký predstaviteľ a skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti v spolupráci s príslušnými civilnými a vojenskými orgánmi a agentúrami a vytvorenými sieťami vrátane siete EU-CyCLONe, ako aj posúdenie rizika komunikačných sietí a infraštruktúr požadované v spoločnej ministerskej výzve z Nevers, ktoré vykonáva skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti s podporou Komisie a agentúry ENISA a v spolupráci s Orgánom európskych regulátorov pre elektronické komunikácie, koordinované posúdenia rizík, ktoré sa majú vykonávať podľa článku 22 smernice

(EÚ) 2022/2555, a testovanie digitálnej prevádzkovej odolnosti stanovené v nariadení Európskeho parlamentu a Rady (EÚ) 2022/2554***[1]***. Pri výbere odvetví by sa malo zohľadniť aj odporúčanie Rady o celoúnijnom koordinovanom prístupe k posilneniu odolnosti kritickej infraštruktúry.

***[1] Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011.***

---

[29] Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011.

[29] Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011.

**Pozmeňujúci návrh 22**

**Návrh nariadenia**
**Odôvodnenie 32**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| (32) Mechanizmus na riešenie kybernetických núdzových situácií by mal podporovať pomoc, ktorú poskytujú členské štáty členskému štátu, ktorý čelí významnému alebo rozsiahlemu kybernetickému incidentu, vrátane pomoci poskytovanej sieťou jednotiek CSIRT stanovenou v článku 15 smernice (EÚ) 2022/2555. Členským štátom poskytujúcim pomoc by sa malo umožniť predkladať žiadosti na pokrytie nákladov súvisiacich s vysielaním tímov odborníkov v rámci vzájomnej pomoci. Oprávnené náklady by mohli zahŕňať príspevky na cestovné výdavky, na ubytovanie a diéty odborníkov | (32) Mechanizmus na riešenie kybernetických núdzových situácií by mal podporovať pomoc, ktorú poskytujú členské štáty členskému štátu, ktorý čelí významnému alebo rozsiahlemu kybernetickému incidentu, vrátane pomoci poskytovanej sieťou jednotiek CSIRT stanovenou v článku 15 smernice (EÚ) 2022/2555. Členským štátom poskytujúcim pomoc by sa malo umožniť predkladať žiadosti na pokrytie nákladov súvisiacich s vysielaním tímov odborníkov v rámci vzájomnej pomoci***, čím sa zabezpečí účinná koordinácia medzi príslušnými programami a nástrojmi EÚ vrátane*** |

| | |
|---|---|
| na kybernetickú bezpečnosť. | ***Európskeho mierového nástroja (EPF), SZBP a NDICI pri poskytovaní pomoci tretím krajinám, najmä Ukrajine a Moldavsku***. Oprávnené náklady by mohli zahŕňať príspevky na cestovné výdavky, na ubytovanie a diéty odborníkov na kybernetickú bezpečnosť. |

**Pozmeňujúci návrh 23**

**Návrh nariadenia**
**Odôvodnenie 33**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| (33) Postupne by sa mala vytvoriť rezerva na úrovni Únie na účely kybernetickej bezpečnosti, ktorú by mali tvoriť služby súkromných poskytovateľov riadených bezpečnostných služieb na podporu opatrení reakcie a okamžitého zotavenia sa v prípadoch významných alebo rozsiahlych kybernetických incidentov. Rezerva EÚ na účely kybernetickej bezpečnosti by mala zabezpečovať dostupnosť a pripravenosť služieb. Služby rezervy EÚ na účely kybernetickej bezpečnosti by mali slúžiť na podporu vnútroštátnych orgánov pri poskytovaní pomoci zasiahnutým subjektom pôsobiacim v kritických odvetviach alebo v odvetviach s vysokou úrovňou kritickosti ako doplnok k ich vlastným opatreniam na vnútroštátnej úrovni. Keď členské štáty žiadajú o podporu z rezervy EÚ na účely kybernetickej bezpečnosti, mali by výslovne uviesť podporu poskytovanú zasiahnutému subjektu na vnútroštátnej úrovni, ktorá by sa mala zohľadniť pri posudzovaní žiadosti členského štátu. Služby rezervy EÚ na účely kybernetickej bezpečnosti sa za podobných podmienok môžu používať aj na podporu inštitúcií, orgánov a agentúr Únie. | (33) Postupne by sa mala vytvoriť rezerva na úrovni Únie na účely kybernetickej bezpečnosti, ktorú by mali tvoriť služby súkromných poskytovateľov riadených bezpečnostných služieb na podporu opatrení reakcie a okamžitého zotavenia sa v prípadoch významných alebo rozsiahlych kybernetických incidentov. Rezerva EÚ na účely kybernetickej bezpečnosti by mala zabezpečovať dostupnosť a pripravenosť služieb. Služby rezervy EÚ na účely kybernetickej bezpečnosti by mali slúžiť na podporu vnútroštátnych orgánov pri poskytovaní pomoci zasiahnutým subjektom pôsobiacim v kritických odvetviach alebo v odvetviach s vysokou úrovňou kritickosti ako doplnok k ich vlastným opatreniam na vnútroštátnej úrovni. Keď členské štáty žiadajú o podporu z rezervy EÚ na účely kybernetickej bezpečnosti, mali by výslovne uviesť podporu poskytovanú zasiahnutému subjektu na vnútroštátnej úrovni, ktorá by sa mala zohľadniť pri posudzovaní žiadosti členského štátu. Služby rezervy EÚ na účely kybernetickej bezpečnosti sa za podobných podmienok môžu používať aj na podporu inštitúcií, orgánov a agentúr Únie ***vrátane misií SBOP***. |

**Pozmeňujúci návrh 24**

**Návrh nariadenia**
**Odôvodnenie 34**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| (34) Na účely výberu súkromných poskytovateľov služieb na poskytovanie služieb v kontexte rezervy EÚ na účely kybernetickej bezpečnosti je nevyhnutné stanoviť súbor minimálnych kritérií, ktoré by sa mali uviesť vo výzve na predkladanie ponúk, na základe ktorej sa vyberú títo poskytovatelia, aby sa zabezpečilo, že budú splnené potreby orgánov členských štátov a subjektov pôsobiacich v kritických odvetviach alebo v odvetviach s vysokou úrovňou kritickosti. | (34) Na účely výberu súkromných poskytovateľov služieb na poskytovanie služieb v kontexte rezervy EÚ na účely kybernetickej bezpečnosti je nevyhnutné stanoviť súbor minimálnych kritérií, ktoré by sa mali uviesť vo výzve na predkladanie ponúk, na základe ktorej sa vyberú títo poskytovatelia, aby sa zabezpečilo, že budú splnené potreby orgánov členských štátov a subjektov pôsobiacich v kritických odvetviach alebo v odvetviach s vysokou úrovňou kritickosti***, pričom sa zohľadnia aj riziká spojené s účasťou poskytovateľov zo strategických konkurenčných krajín, ktoré môžu ohroziť hospodársku bezpečnosť, ako aj dôsledky pre strategickú bezpečnosť Únie***. |

**Pozmeňujúci návrh 25**

**Návrh nariadenia**
**Odôvodnenie 36**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| (36) V záujme podpory cieľov tohto nariadenia týkajúcich sa presadzovania spoločnej situačnej informovanosti, zvyšovania odolnosti Únie a umožnenia účinnej reakcie na významné a rozsiahle kybernetické incidenty by sieť EU-CyCLONe, sieť jednotiek CSIRT alebo Komisia mali mať možnosť požiadať agentúru ENISA o preskúmanie a posúdenie hrozieb, zraniteľností a zmierňujúcich opatrení s ohľadom na konkrétny významný alebo rozsiahly kybernetický incident. Po dokončení preskúmania a posúdenia incidentu by agentúra ENISA mala vypracovať správu o preskúmaní incidentu, a to v spolupráci | (36) V záujme podpory cieľov tohto nariadenia týkajúcich sa presadzovania spoločnej situačnej informovanosti, zvyšovania odolnosti Únie a umožnenia účinnej reakcie na významné a rozsiahle kybernetické incidenty by sieť EU-CyCLONe, sieť jednotiek CSIRT alebo Komisia mali mať možnosť požiadať agentúru ENISA o preskúmanie a posúdenie hrozieb, zraniteľností a zmierňujúcich opatrení s ohľadom na konkrétny významný alebo rozsiahly kybernetický incident. ***So zreteľom na vývoj systému bezpečnej konektivity, ktorý vychádza z európskej kvantovej komunikačnej infraštruktúry (EuroQCI)*** |

s príslušnými zainteresovanými stranami vrátane zástupcov súkromného sektora, členských štátov, Komisie a iných relevantných inštitúcií, orgánov a agentúr EÚ. Pokiaľ ide o súkromný sektor, agentúra ENISA vyvíja spôsoby výmeny informácií so špecializovanými poskytovateľmi vrátane poskytovateľov riadených bezpečnostných riešení a predajcov s cieľom prispieť k poslaniu agentúry ENISA dosiahnuť vysokú spoločnú úroveň kybernetickej bezpečnosti v celej Únii. Vychádzajúc zo spolupráce so zainteresovanými stranami vrátane súkromného sektora by sa správa o preskúmaní konkrétnych incidentov mala zamerať na posúdenie príčin, vplyvov incidentu a krokov na jeho zmiernenie po jeho výskyte. Osobitnú pozornosť by bolo treba venovať vstupným informáciám a poznatkom, ktoré poskytujú poskytovatelia riadených bezpečnostných služieb, ktorí spĺňajú podmienky najvyššej úrovne odbornej integrity, nestrannosti a nevyhnutných technických odborných znalostí vyžadovaných týmto nariadením. Správa by sa mala doručiť sieti EU-CyCLONe, sieti jednotiek CSIRT a Komisii a mala by sa premietnuť do ich činností. Ak incident súvisí s treťou krajinou, Komisia správu poskytne aj vysokému predstaviteľovi.

***a vládnej satelitnej komunikácie Európskej únie (GOVSATCOM), najmä zavedenie GNSS GALILEO pre používateľov v oblasti obrany, by mal akýkoľvek možný budúci vývoj zohľadňovať nástup „hypervojny“, v ktorej sa spája rýchlosť a sofistikovanosť kvantovej výpočtovej techniky s vysoko autonómnymi vojenskými systémami.*** Po dokončení preskúmania a posúdenia incidentu by agentúra ENISA mala vypracovať správu o preskúmaní incidentu, a to v spolupráci s príslušnými zainteresovanými stranami vrátane zástupcov súkromného sektora, členských štátov, Komisie a iných relevantných inštitúcií, orgánov a agentúr EÚ**.** Pokiaľ ide o súkromný sektor, agentúra ENISA vyvíja spôsoby výmeny informácií so špecializovanými poskytovateľmi vrátane poskytovateľov riadených bezpečnostných riešení a predajcov s cieľom prispieť k poslaniu agentúry ENISA dosiahnuť vysokú spoločnú úroveň kybernetickej bezpečnosti v celej Únii. Vychádzajúc zo spolupráce so zainteresovanými stranami vrátane súkromného sektora by sa správa o preskúmaní konkrétnych incidentov mala zamerať na posúdenie príčin, vplyvov incidentu a krokov na jeho zmiernenie po jeho výskyte. Osobitnú pozornosť by bolo treba venovať vstupným informáciám a poznatkom, ktoré poskytujú poskytovatelia riadených bezpečnostných služieb, ktorí spĺňajú podmienky najvyššej úrovne odbornej integrity, nestrannosti a nevyhnutných technických odborných znalostí vyžadovaných týmto nariadením. Správa by sa mala doručiť sieti EU-CyCLONe, sieti jednotiek CSIRT a Komisii a mala by sa premietnuť do ich činností. Ak incident súvisí s treťou krajinou, Komisia správu poskytne aj vysokému predstaviteľovi***, ESVČ a každej misii SBOP v krajine, ktorá čelí incidentu, prostredníctvom ich ústredia***.

**Pozmeňujúci návrh 26**

**Návrh nariadenia**
**Odôvodnenie 37**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| (37) S ohľadom na nepredvídateľnosť útokov na kybernetickú bezpečnosť a na skutočnosť, že tieto útoky často nie sú obmedzené na konkrétnu geografickú oblasť a predstavujú vysoké riziko presahu, prispieva k ochrane celej Únie zvýšenie odolnosti susedných krajín a posilnenie ich kapacity účinne reagovať na významné a rozsiahle kybernetické incidenty. Tretie krajiny pridružené k programu Digitálna Európa sa preto ***môžu*** podporovať z rezervy EÚ na účely kybernetickej bezpečnosti, ***ak*** je ***to možné podľa príslušnej dohody o pridružení k programu Digitálna Európa***. Financovanie určené pre pridružené tretie krajiny by mala podporiť Únia v rámci príslušných partnerstiev a nástrojov financovania týchto krajín. Podpora by sa mala vzťahovať na služby v oblasti reakcie na významné a rozsiahle kybernetické incidenty a v oblasti okamžitého zotavenia sa z nich. Pri poskytovaní podpory tretím krajinám pridruženým k programu Digitálna Európa by sa mali uplatňovať podmienky stanovené v tomto nariadení pre rezervu EÚ na účely kybernetickej bezpečnosti a dôveryhodných poskytovateľov. | (37) S ohľadom na nepredvídateľnosť útokov na kybernetickú bezpečnosť a na skutočnosť, že tieto útoky často nie sú obmedzené na konkrétnu geografickú oblasť a predstavujú vysoké riziko presahu, prispieva k ochrane celej Únie zvýšenie odolnosti susedných krajín***, najmä Ukrajiny a Moldavska,*** a posilnenie ich kapacity účinne reagovať na významné a rozsiahle kybernetické incidenty. Tretie krajiny pridružené k programu Digitálna Európa ***by*** sa preto ***mali*** podporovať z rezervy EÚ na účely kybernetickej bezpečnosti***. Podpora by sa mala vzťahovať aj na tie tretie krajiny***, ***v ktorých*** je ***nasadená misia SBOP s osobitným mandátom na posilnenie odolnosti voči hybridným hrozbám vrátane kybernetických hrozieb alebo v ktorých bolo prijaté opatrenie pomoci EPF na posilnenie kybernetickej odolnosti krajiny***. Financovanie určené pre pridružené tretie krajiny by mala podporiť Únia v rámci príslušných partnerstiev a nástrojov financovania týchto krajín. Podpora by sa mala vzťahovať na služby v oblasti reakcie na významné a rozsiahle kybernetické incidenty a v oblasti okamžitého zotavenia sa z nich. Pri poskytovaní podpory tretím krajinám pridruženým k programu Digitálna Európa by sa mali uplatňovať podmienky stanovené v tomto nariadení pre rezervu EÚ na účely kybernetickej bezpečnosti a dôveryhodných poskytovateľov. |

**Pozmeňujúci návrh 27**

**Návrh nariadenia**
**Článok 1 – odsek 1 – písmeno c**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| c) vytvorenie európskeho mechanizmu preskúmania kybernetických incidentov, ktorý bude slúžiť na skúmanie a posudzovanie významných alebo rozsiahlych incidentov. | c) vytvorenie európskeho mechanizmu preskúmania kybernetických incidentov, ktorý bude slúžiť na skúmanie a posudzovanie významných alebo rozsiahlych incidentov ***alebo hrozieb***. |

**Pozmeňujúci návrh 28**

**Návrh nariadenia**
**Článok 1 – odsek 2 – písmeno a**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| a) posilniť spoločné odhaľovanie kybernetických hrozieb a incidentov a situačnú informovanosť o nich v Únii, v dôsledku čoho bude možné posilniť konkurenčnú pozíciu odvetví priemyslu a služieb v Únii v rámci celého digitálneho hospodárstva a prispievať k technologickej ***suverenite*** Únie v oblasti kybernetickej bezpečnosti; | a) posilniť spoločné odhaľovanie kybernetických hrozieb a incidentov a situačnú informovanosť o nich v Únii, v dôsledku čoho bude možné posilniť konkurenčnú pozíciu odvetví priemyslu a služieb v Únii v rámci celého digitálneho hospodárstva a prispievať k technologickej ***odolnosti*** Únie v oblasti kybernetickej bezpečnosti; |

**Pozmeňujúci návrh 29**

**Návrh nariadenia**
**Článok 1 – odsek 2 – písmeno b**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| b) posilniť pripravenosť subjektov pôsobiacich v kritických odvetviach a v odvetviach s vysokou úrovňou kritickosti z celej Únie a posilniť solidaritu rozvíjaním kapacít spoločnej reakcie na významné alebo rozsiahle kybernetické incidenty, a to aj sprístupnením podpory Únie týkajúcej sa reakcie na kybernetické incidenty tretím krajinám pridruženým k programu Digitálna Európa; | b) posilniť pripravenosť subjektov pôsobiacich v kritických odvetviach a v odvetviach s vysokou úrovňou kritickosti z celej Únie a posilniť solidaritu rozvíjaním kapacít spoločnej reakcie na významné alebo rozsiahle kybernetické incidenty, a to aj sprístupnením podpory Únie týkajúcej sa reakcie na kybernetické incidenty tretím krajinám pridruženým k programu Digitálna Európa ***alebo tým tretím krajinám, ktoré sú kandidátmi na pristúpenie k Únii a nekonajú v rozpore s bezpečnostnými a obrannými záujmami Únie a jej členských štátov, ako je*** |

***stanovené v rámci SZBP podľa hlavy V ZEÚ; Členské štáty by mali považovať program aktívnej kybernetickej obrany za súčasť svojej vnútroštátnej stratégie kybernetickej bezpečnosti, ktorá zahŕňa pravidelné spoločné cvičenia odbornej prípravy medzi členskými štátmi a naprieč medzinárodnými organizáciami. Takýto program by mal poskytnúť synchronizovanú kapacitu na zisťovanie, odhaľovanie, analýzu a zmierňovanie hrozieb v reálnom čase.***

**Pozmeňujúci návrh 30**

**Návrh nariadenia**
**Článok 1 – odsek 2 a (nový)**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| | ***2a. znížiť systémové kybernetickobezpečnostné riziká vyplývajúce zo závislosti od kritického vybavenia z krajín, ktoré konajú v rozpore s bezpečnostnými a obrannými záujmami Únie a jej členských štátov, ako je stanovené v rámci SZBP podľa hlavy V ZEÚ;*** |

**Pozmeňujúci návrh 31**

**Návrh nariadenia**
**Článok 2 – odsek 2 a (nový)**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| | ***„komunita kybernetickej obrany“ je komunita, ktorú tvoria orgány obrany členských štátov a ktorú podporujú inštitúcie, orgány a agentúry EÚ, ako sa stanovuje v spoločnom oznámení o politike EÚ v oblasti kybernetickej obrany[1]*** |
| | ***[1] Spoločné oznámenie Európskemu parlamentu a Rade, Politika EÚ v oblasti kybernetickej obrany [JOIN(2022) 49*** |

***final].***

**Pozmeňujúci návrh 32**

**Návrh nariadenia**
**Článok 3 – odsek 2 – pododsek 1 – písmeno b a (nové)**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| | ***ba) pomáha modernizovať celé systémy kybernetickej obrany, pričom zvyšuje kvalitu spôsobilostí v oblasti kybernetickej obrany zavádzaním systémov umelej inteligencie a urýchľuje výmenu informácií medzi národnými centrami bezpečnostných operácií a cezhraničnými centrami bezpečnostných operácií;*** |

**Pozmeňujúci návrh 33**

**Návrh nariadenia**
**Článok 3 – odsek 2 – pododsek 1 – písmeno d a (nové)**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| | ***da) preskúmava a vyhodnocuje kritické kybernetickobezpečnostné technológie a vybavenie, ktoré používajú centrá bezpečnostných operácií v reakcii na kybernetické incidenty, pokiaľ ide o systémové riziká vyplývajúce z toho, že krajiny, ktoré by mohli konať rozpore s bezpečnostnými a obrannými záujmami Únie a jej členských štátov, ako sa stanovuje v rámci SZBP podľa hlavy V ZEÚ, majú kontrolu nad vysokorizikovými dodávateľmi;*** |

**Pozmeňujúci návrh 34**

**Návrh nariadenia**
**Článok 4 – odsek 1 – pododsek 2**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| Má spôsobilosť konať ako referenčný bod a brána pre ďalšie verejné a súkromné organizácie na vnútroštátnej úrovni na účely zhromažďovania a analyzovania informácií o kybernetických hrozbách a incidentoch a prispievania k cezhraničnému centru bezpečnostných operácií. Je vybavené najmodernejšími technológiami, ktoré sú schopné odhaľovať, agregovať a analyzovať údaje relevantné z hľadiska kybernetických hrozieb a incidentov. | Má spôsobilosť konať ako referenčný bod a brána pre ďalšie verejné a súkromné ***a v prípade potreby vojenské*** organizácie na vnútroštátnej úrovni na účely zhromažďovania a analyzovania informácií o kybernetických hrozbách a incidentoch a prispievania k cezhraničnému centru bezpečnostných operácií. Je vybavené najmodernejšími technológiami, ktoré sú schopné odhaľovať, agregovať a analyzovať údaje relevantné z hľadiska kybernetických hrozieb a incidentov. |

**Pozmeňujúci návrh 35**

**Návrh nariadenia**
**Článok 4 – odsek 2**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| 2. V nadväznosti na výzvu na vyjadrenie záujmu vyberá Európske centrum priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti (ďalej len „kompetenčné centrum“) vnútroštátne centrá bezpečnostných operácií na účely účasti na spoločnom obstarávaní nástrojov a infraštruktúr s kompetenčným centrom. Vybratým vnútroštátnym centrám bezpečnostných operácií môže kompetenčné centrum udeľovať granty na financovanie prevádzky týchto nástrojov a infraštruktúr. Až 50 % obstarávacích nákladov na nástroje a infraštruktúry a až 50 % prevádzkových nákladov pokrýva finančný príspevok Únie, pričom zvyšné náklady pokrývajú členské štáty. Pred spustením postupu nadobudnutia nástrojov a infraštruktúr kompetenčné centrum a vnútroštátne centrá bezpečnostných operácií uzavrú dohodu o poskytovaní hostiteľských služieb a o používaní, ktorou sa upravuje používanie nástrojov | 2. V nadväznosti na výzvu na vyjadrenie záujmu vyberá Európske centrum priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti (ďalej len „kompetenčné centrum“) vnútroštátne centrá bezpečnostných operácií na účely účasti na spoločnom obstarávaní nástrojov a infraštruktúr s kompetenčným centrom. Vybratým vnútroštátnym centrám bezpečnostných operácií môže kompetenčné centrum udeľovať granty na financovanie prevádzky týchto nástrojov a infraštruktúr ***pod prísnou podmienkou, že takéto nástroje a infraštruktúru poskytujú dôveryhodní poskytovatelia v súlade s článkom 16***. Až 50 % obstarávacích nákladov na nástroje a infraštruktúry a až 50 % prevádzkových nákladov pokrýva finančný príspevok Únie, pričom zvyšné náklady pokrývajú členské štáty. Pred spustením postupu nadobudnutia nástrojov a infraštruktúr kompetenčné centrum a vnútroštátne centrá bezpečnostných operácií uzavrú dohodu |

| | |
|---|---|
| a infraštruktúr. | o poskytovaní hostiteľských služieb a o používaní, ktorou sa upravuje používanie nástrojov a infraštruktúr. |

**Pozmeňujúci návrh 36**

**Návrh nariadenia**
**Článok 5 – odsek 2**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| 2. V nadväznosti na výzvu na vyjadrenie záujmu kompetenčné centrum vyberie hostiteľské konzorcium na účely účasti na spoločnom obstarávaní nástrojov a infraštruktúr s kompetenčným centrom. Na financovanie prevádzky týchto nástrojov a infraštruktúr môže kompetenčné centrum udeliť hostiteľskému konzorciu grant**.** Až 75 % obstarávacích nákladov na nástroje a infraštruktúry a až 50 % prevádzkových nákladov pokrýva finančný príspevok Únie, pričom zvyšné náklady pokryje hostiteľské konzorcium. Pred spustením postupu nadobudnutia nástrojov a infraštruktúr kompetenčné centrum a hostiteľské konzorcium uzavrú dohodu o poskytovaní hostiteľských služieb a o používaní, ktorou sa upravuje používanie nástrojov a infraštruktúr. | 2. V nadväznosti na výzvu na vyjadrenie záujmu kompetenčné centrum vyberie hostiteľské konzorcium na účely účasti na spoločnom obstarávaní nástrojov a infraštruktúr s kompetenčným centrom. Na financovanie prevádzky týchto nástrojov a infraštruktúr môže kompetenčné centrum udeliť hostiteľskému konzorciu grant ***pod prísnou podmienkou, že takéto nástroje a infraštruktúru poskytujú dôveryhodní poskytovatelia v súlade s článkom 16.*** Až 75 % obstarávacích nákladov na nástroje a infraštruktúry a až 50 % prevádzkových nákladov pokrýva finančný príspevok Únie, pričom zvyšné náklady pokryje hostiteľské konzorcium. Pred spustením postupu nadobudnutia nástrojov a infraštruktúr kompetenčné centrum a hostiteľské konzorcium uzavrú dohodu o poskytovaní hostiteľských služieb a o používaní, ktorou sa upravuje používanie nástrojov a infraštruktúr. |

**Pozmeňujúci návrh 37**

**Návrh nariadenia**
**Článok 5 – odsek 2 a (nový)**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| | ***2a. Akákoľvek infraštruktúra alebo poskytovateľ pochádzajúci z vysokorizikovej tretej krajiny sa automaticky vylúči.*** |

**Pozmeňujúci návrh 38**

**Návrh nariadenia**
**Článok 6 – odsek 1 – písmeno b a (nové)**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| | ***ba) priamo podporuje posilnenie vojenských a obranných spôsobilostí zúčastnených členov alebo predchádza priamemu a bezprostrednému ohrozeniu ich bezpečnosti. Keďže zneužitie zraniteľných miest v sektore obrany môže spôsobiť značné narušenie a škody, kybernetická bezpečnosť obranného priemyslu si vyžaduje osobitné opatrenia na zaistenie bezpečnosti dodávateľských reťazcov, najmä subjektov z nižších úrovní dodávateľských reťazcov, ktoré síce nevyžadujú prístup k utajovaným skutočnostiam, ale mohli by predstavovať vážne riziká pre celé odvetvie. Osobitná pozornosť by sa mala venovať vplyvu, ktorý by akékoľvek porušenie mohlo mať, a hrozbe akejkoľvek potenciálnej manipulácie so sieťovými údajmi, ktorá by mohla viesť k tomu, že kritické obranné prostriedky by boli zbytočné alebo by dokonca prevažovali nad príslušnými operačnými systémami, čím by sa stali zraniteľnými voči „únosu“.*** |

**Pozmeňujúci návrh 39**

**Návrh nariadenia**
**Článok 6 – odsek 1 – písmeno b b (nové)**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| | ***bb) podporuje posilnenie obranných spôsobilostí zúčastnených členov alebo predchádza priamemu a bezprostrednému ohrozeniu ich bezpečnosti, pričom zaisťuje bezpečnosť dodávateľských reťazcov, najmä pokiaľ ide o subjekty z nižších úrovní dodávateľských reťazcov,*** |

| | |
|---|---|
| | ***ktoré síce nevyžadujú prístup k utajovaným skutočnostiam, ale mohli by predstavovať vážne riziká pre celé odvetvie.*** |

**Pozmeňujúci návrh 40**

**Návrh nariadenia**
**Článok 7 – odsek 1**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| 1. Ak cezhraničné centrá bezpečnostných operácií získajú informácie týkajúce sa potenciálneho alebo prebiehajúceho rozsiahleho kybernetického incidentu, poskytnú bez zbytočného odkladu relevantné informácie sieti EU-CyCLONe, sieti jednotiek CSIRT a Komisii s ohľadom na ich príslušné úlohy v oblasti krízového riadenia v súlade so smernicou (EÚ) 2022/2555. | 1. Ak cezhraničné centrá bezpečnostných operácií získajú informácie týkajúce sa potenciálneho alebo prebiehajúceho rozsiahleho kybernetického incidentu, poskytnú bez zbytočného odkladu relevantné informácie sieti EU-CyCLONe, sieti jednotiek CSIRT a Komisii ***vrátane vysokého predstaviteľa a ESVČ, ak sa týkajú tretej krajiny,*** s ohľadom na ich príslušné úlohy v oblasti krízového riadenia v súlade so smernicou (EÚ) 2022/2555. |

**Pozmeňujúci návrh 41**

**Návrh nariadenia**
**Článok 8 – odsek 1**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| 1. Členské štáty, ktoré sa zúčastňujú na európskom kybernetickom štíte, zaistia vysokú úroveň bezpečnosti údajov a fyzickej bezpečnosti infraštruktúry európskeho kybernetického štítu a zaistia primerané spravovanie a kontrolu infraštruktúry takým spôsobom, aby bola chránená pred hrozbami a aby bola zaistená jej bezpečnosť a bezpečnosť systémov vrátane bezpečnosti údajov, ktoré sa vymieňajú prostredníctvom infraštruktúry. | 1. Členské štáty, ktoré sa zúčastňujú na európskom kybernetickom štíte, zaistia vysokú úroveň bezpečnosti údajov a fyzickej bezpečnosti infraštruktúry európskeho kybernetického štítu a zaistia primerané spravovanie a kontrolu infraštruktúry takým spôsobom, aby bola chránená pred hrozbami a aby bola zaistená jej bezpečnosť a bezpečnosť systémov***, znižovanie rizík a podpora technologickej výhody EÚ v kritických sektoroch*** vrátane ***opatrení na obmedzenie alebo vylúčenie vysokorizikových dodávateľov, ako aj ochranu*** bezpečnosti údajov, ktoré sa vymieňajú |

prostredníctvom infraštruktúry.

**Pozmeňujúci návrh 42**

**Návrh nariadenia**
**Článok 8 – odsek 2**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| 2. Členské štáty, ktoré sa zúčastňujú na európskom kybernetickom štíte, zaistia, aby výmena informácií v rámci európskeho kybernetického štítu so subjektmi, ktoré nie sú verejnými subjektmi členských štátov, negatívne neovplyvnila bezpečnostné záujmy Únie. | 2. Členské štáty, ktoré sa zúčastňujú na európskom kybernetickom štíte, zaistia, aby výmena informácií v rámci európskeho kybernetického štítu so subjektmi, ktoré nie sú verejnými subjektmi členských štátov, negatívne neovplyvnila bezpečnostné záujmy Únie ***a aby akákoľvek výmena informácií s vysokorizikovými dodávateľmi mala obmedzený rozsah a neohrozovala bezpečnosť a strategické záujmy Únie***. |

**Pozmeňujúci návrh 43**

**Návrh nariadenia**
**Článok 8 – odsek 3**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| 3. Komisia môže prijať vykonávacie akty, v ktorých sa stanovia technické požiadavky pre členské štáty, aby si splnili povinnosť podľa odseku 1 a 2. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 21 ods. 2 tohto nariadenia. S cieľom uľahčiť spoluprácu s vojenskými aktérmi pritom Komisia s podporou vysokého predstaviteľa zohľadňuje relevantné bezpečnostné normy na úrovni obrany. | 3. Komisia môže prijať vykonávacie akty, v ktorých sa stanovia technické požiadavky pre členské štáty, aby si splnili povinnosť podľa odseku 1 a 2. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 21 ods. 2 tohto nariadenia. S cieľom uľahčiť spoluprácu s vojenskými aktérmi pritom Komisia s podporou vysokého predstaviteľa zohľadňuje relevantné bezpečnostné normy na úrovni obrany***, pričom primerane využíva celú škálu obranných možností, ktoré majú civilné a vojenské komunity k dispozícii na širšiu bezpečnosť a obranu EÚ, a informuje Európsky parlament***. |

**Pozmeňujúci návrh 44**

**Návrh nariadenia**
**Článok 9 – odsek 2**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| 2. Opatrenia, ktorými sa mechanizmus na riešenie kybernetických núdzových situácií vykonáva, sa podporia financovaním z programu Digitálna Európa a vykonávajú sa v súlade s nariadením (EÚ) 2021/694, a najmä s jeho špecifickým cieľom 3**.** | 2. Opatrenia, ktorými sa mechanizmus na riešenie kybernetických núdzových situácií vykonáva, sa podporia financovaním z programu Digitálna Európa a vykonávajú sa v súlade s nariadením (EÚ) 2021/694, a najmä s jeho špecifickým cieľom 3***, a prostredníctvom Európskeho mierového nástroja (EPF) pri poskytovaní opatrení pomoci tretím krajinám, najmä Ukrajine a Moldavsku;*** |

**Pozmeňujúci návrh 45**

**Návrh nariadenia**
**Článok 10 – odsek 1 – písmeno a**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| a) opatrenia v oblasti pripravenosti vrátane koordinovaného testovania pripravenosti subjektov pôsobiacich v odvetviach s vysokou úrovňou kritickosti ***v*** celej Únii; | a) opatrenia v oblasti pripravenosti vrátane koordinovaného testovania pripravenosti subjektov pôsobiacich v odvetviach s vysokou úrovňou kritickosti***, ako sú verejná infraštruktúra, volebná infraštruktúra, doprava, zdravotná starostlivosť, finančný sektor, telekomunikácie, potravinové dodávky a bezpečnosť v*** celej Únii; |

**Pozmeňujúci návrh 46**

**Návrh nariadenia**
**Článok 10 – odsek 1 – písmeno c**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| c) opatrenia vzájomnej pomoci, ktoré zahŕňajú poskytovanie pomoci vnútroštátnymi orgánmi jedného členského štátu druhému členskému štátu, najmä podľa článku 11 ods. 3 písm. f) smernice | c) opatrenia vzájomnej pomoci, ktoré zahŕňajú poskytovanie pomoci vnútroštátnymi orgánmi jedného členského štátu druhému členskému štátu, najmä podľa článku 11 ods. 3 písm. f) smernice |

| | |
|---|---|
| (EÚ) 2022/2555. | (EÚ) 2022/2555 ***a v kontexte článku 42 ods. 7 ZEÚ a článku 222 ZFEÚ;*** |

**Pozmeňujúci návrh 47**

**Návrh nariadenia**
**Článok 10 – odsek 1 – písmeno c a (nové)**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| | ***ca) nahradenie a postupné vyradenie kritického vybavenia od vysokorizikových dodávateľov, ktorí konajú v rozpore s bezpečnostnými a obrannými záujmami Únie a jej členských štátov, ako je stanovené v rámci SZBP podľa hlavy V ZEÚ;*** |

**Pozmeňujúci návrh 48**

**Návrh nariadenia**
**Článok 11 – odsek 2**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| 2. Skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti v spolupráci s Komisiou, agentúrou ENISA ***a*** vysokým predstaviteľom vypracováva spoločné scenáre rizika a metodiky na vykonávanie koordinovaného testovania. | 2. Skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti v spolupráci s Komisiou, agentúrou ENISA***,*** vysokým predstaviteľom***, ESVČ a v príslušných prípadoch agentúrou EDA*** vypracováva spoločné scenáre rizika a metodiky na vykonávanie koordinovaného testovania. |

**Pozmeňujúci návrh 49**

**Návrh nariadenia**
**Článok 12 – odsek 2**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| 2. Rezerva EÚ na účely kybernetickej bezpečnosti sa pozostáva zo služieb reakcie na incidenty poskytovaných dôveryhodnými poskytovateľmi vybratými v súlade s kritériami stanovenými | 2. Rezerva EÚ na účely kybernetickej bezpečnosti sa pozostáva zo služieb reakcie na incidenty poskytovaných dôveryhodnými poskytovateľmi vybratými v súlade s kritériami stanovenými |

| | |
|---|---|
| v článku 16. Súčasťou rezervy sú vopred vyčlenené služby. Tieto služby ***sú nasaditeľné*** vo všetkých členských štátoch. | v článku 16. Súčasťou rezervy sú vopred vyčlenené služby. Tieto služby ***možno nasadiť*** vo všetkých členských štátoch ***a tretích krajinách, ktoré spĺňajú uplatniteľné požiadavky tohto nariadenia***. |

**Pozmeňujúci návrh 50**

**Návrh nariadenia**
**Článok 12 – odsek 3 – písmeno b**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| b) inštitúcie, orgány a agentúry Únie. | b) inštitúcie, orgány a agentúry Únie ***vrátane misií SBOP***. |

**Pozmeňujúci návrh 51**

**Návrh nariadenia**
**Článok 12 – odsek 4**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| 4. Používatelia uvedení v odseku 3 písm. a) využívajú služby z rezervy EÚ na účely kybernetickej bezpečnosti s cieľom reagovať alebo podporovať reakciu na významné alebo rozsiahle kybernetické incidenty, ktoré zasahujú subjekty pôsobiace v kritických odvetviach alebo v odvetviach s vysokou úrovňou kritickosti, a okamžité zotavenie sa z nich. | 4. Používatelia uvedení v odseku 3 písm. a) využívajú služby z rezervy EÚ na účely kybernetickej bezpečnosti s cieľom reagovať alebo podporovať reakciu na významné alebo rozsiahle kybernetické incidenty, ktoré zasahujú subjekty pôsobiace v kritických odvetviach alebo v odvetviach s vysokou úrovňou kritickosti, ***ako sú verejná infraštruktúra, volebná infraštruktúra, doprava, zdravotná starostlivosť, finančný sektor, telekomunikácie, potravinové dodávky*** a ***bezpečnosť, a*** okamžité zotavenie sa z nich. |

**Pozmeňujúci návrh 52**

**Návrh nariadenia**
**Článok 12 – odsek 5**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| 5. Celkovú zodpovednosť za | 5. Celkovú zodpovednosť za |

| | |
|---|---|
| vykonávanie rezervy EÚ na účely kybernetickej bezpečnosti nesie Komisia. Komisia určuje priority a vývoj rezervy EÚ na účely kybernetickej bezpečnosti v súlade požiadavkami používateľov uvedených v odseku 3 a dohliada na jej vykonávanie a zaisťuje komplementárnosť, súdržnosť, synergie a prepojenia s ďalšími podpornými opatreniami na základe tohto nariadenia, ako aj s ďalšími opatreniami ***a*** programami Únie. | vykonávanie rezervy EÚ na účely kybernetickej bezpečnosti nesie Komisia. Komisia určuje priority a vývoj rezervy EÚ na účely kybernetickej bezpečnosti v súlade požiadavkami používateľov uvedených v odseku 3 a dohliada na jej vykonávanie a zaisťuje komplementárnosť, súdržnosť, synergie a prepojenia s ďalšími podpornými opatreniami na základe tohto nariadenia, ako aj s ďalšími opatreniami***,*** programami a ***cieľmi*** Únie***, najmä so strategickým cieľom znížiť závislosť od vysokorizikových dodávateľov, ktorí konajú v rozpore s bezpečnostnými a obrannými záujmami Únie a jej členských štátov, ako je stanovené v rámci SZBP podľa hlavy V ZEÚ***. |

**Pozmeňujúci návrh 53**

**Návrh nariadenia**
**Článok 12 – odsek 7**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| 7. S cieľom podporiť Komisiu pri vytváraní rezervy EÚ na účely kybernetickej bezpečnosti agentúra ENISA vypracuje po konzultáciách s členskými štátmi a Komisiou mapovanie potrebných služieb. Po konzultácii s Komisiou vypracuje agentúra ENISA podobné mapovanie s cieľom identifikovať potreby tretích krajín, ktoré majú podľa článku 17 nárok na podporu z rezervy EÚ na účely kybernetickej bezpečnosti. Komisia v prípade potreby uskutoční konzultácie s vysokým predstaviteľom. | 7. S cieľom podporiť Komisiu pri vytváraní rezervy EÚ na účely kybernetickej bezpečnosti agentúra ENISA vypracuje po konzultáciách s členskými štátmi a Komisiou mapovanie potrebných služieb. Po konzultácii s Komisiou vypracuje agentúra ENISA ***s podporou ESVČ*** podobné mapovanie s cieľom identifikovať potreby tretích krajín, ktoré majú podľa článku 17 nárok na podporu z rezervy EÚ na účely kybernetickej bezpečnosti. Komisia v prípade potreby uskutoční konzultácie s vysokým predstaviteľom. |

**Pozmeňujúci návrh 54**

**Návrh nariadenia**
**Článok 14 – odsek 2 – písmeno a a (nové)**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| | ***aa) vplyv incidentu na bezpečnosť a obranu Únie;*** |

**Pozmeňujúci návrh 55**

**Návrh nariadenia**
**Článok 15 – odsek 3**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| 3. Podporou v rámci mechanizmu na riešenie kybernetických núdzových situácií sa na základe konzultácie s vysokým predstaviteľom môže dopĺňať pomoc poskytnutá v kontexte spoločnej zahraničnej a bezpečnostnej politiky a spoločnej bezpečnostnej a obrannej politiky, a to aj prostredníctvom tímov rýchlej kybernetickej reakcie. Môže sa ňou dopĺňať aj pomoc poskytnutá jedným členským štátom inému členskému štátu v kontexte článku 42 ods. 7 Zmluvy o Európskej únii alebo môže k takejto pomoci prispievať. | 3. Podporou v rámci mechanizmu na riešenie kybernetických núdzových situácií sa na základe konzultácie s vysokým predstaviteľom môže dopĺňať pomoc poskytnutá v kontexte spoločnej zahraničnej a bezpečnostnej politiky a spoločnej bezpečnostnej a obrannej politiky, a to aj prostredníctvom tímov rýchlej kybernetickej reakcie ***(CRRT) s cieľom väčšmi podporiť členské štáty EÚ, misie a operácie SBOP a tie tretie krajiny, ktoré dosiahli súlad so spoločnou zahraničnou a bezpečnostnou politikou a spoločnou bezpečnostnou a obrannou politikou EÚ, najmä Ukrajinu a Moldavsko, pri ich úsilí o budovanie kapacít v oblasti kybernetickej obrany***. Môže sa ňou dopĺňať aj pomoc poskytnutá jedným členským štátom inému členskému štátu v kontexte článku 42 ods. 7 Zmluvy o Európskej únii alebo môže k takejto pomoci prispievať. |

**Pozmeňujúci návrh 56**

**Návrh nariadenia**
**Článok 16 – odsek 2 – písmeno b a (nové)**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| | ***aa) poskytovateľ preukáže, že jeho rozhodovacie a riadiace štruktúry nepodliehajú neprípustnému ovplyvňovaniu zo strany vlád štátov, ktoré*** |

| | |
|---|---|
| | ***je v rozpore s bezpečnostnými a obrannými záujmami Únie a jej členských štátov, ako je stanovené v rámci SZBP podľa hlavy V ZEÚ;*** |

**Pozmeňujúci návrh 57**

**Návrh nariadenia**
**Článok 16 – odsek 2 – písmeno f**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| f) poskytovateľ disponuje hardvérovým a softvérovým technickým vybavením potrebným na podporu požadovanej služby; | f) poskytovateľ disponuje hardvérovým a softvérovým technickým vybavením potrebným na podporu požadovanej služby ***a spĺňa požiadavky stanovené v článku X nariadenia XX/XXXX (akt o kybernetickej odolnosti)***; |

**Pozmeňujúci návrh 58**

**Návrh nariadenia**
**Článok 16 – odsek 2 – písmeno j a (nové)**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| | ***ja) prípustný nie je žiadny poskytovateľ pochádzajúci z vysokorizikovej tretej krajiny;*** |

**Pozmeňujúci návrh 59**

**Návrh nariadenia**
**Článok 16 – odsek 2 – písmeno j b (nové)**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| | ***jb) poskytovateľ musí podľa možnosti úzko spolupracovať s príslušnými MSP;*** |

**Pozmeňujúci návrh 60**

**Návrh nariadenia**
**Článok 17 – odsek 1**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| 1. Tretie krajiny môžu požiadať o podporu z rezervy EÚ na účely kybernetickej bezpečnosti, ***ak*** sa to ***umožňuje*** v dohodách o pridružení uzatvorených v súvislosti s účasťou týchto krajín na programe Digitálna Európa. | 1. Tretie krajiny môžu požiadať o podporu z rezervy EÚ na účely kybernetickej bezpečnosti, ***pokiaľ:*** |
| | ***a)*** sa to ***stanovuje*** v dohodách o pridružení uzatvorených v súvislosti s účasťou týchto krajín na programe Digitálna Európa***;*** |
| | ***b) v týchto tretích krajinách je nasadená misia SBOP s osobitným mandátom na posilnenie odolnosti voči hybridným hrozbám vrátane kybernetických hrozieb alebo v nich bolo prijaté opatrenie pomoci EPF na posilnenie kybernetickej odolnosti krajiny.*** |

**Pozmeňujúci návrh 61**

**Návrh nariadenia**
**Článok 17 – odsek 2**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| 2. Podpora z rezervy EÚ na účely kybernetickej bezpečnosti musí byť v súlade s týmto nariadením a so všetkými osobitnými podmienkami stanovenými v dohodách o pridružení uvedených v odseku 1. | 2. Podpora z rezervy EÚ na účely kybernetickej bezpečnosti musí byť v súlade s týmto nariadením a so všetkými osobitnými podmienkami stanovenými v dohodách o pridružení uvedených v odseku ***s výnimkou tých tretích krajín, na ktoré sa vzťahujú ustanovenia uvedené*** v odseku 1***písm. b)***. |

**Pozmeňujúci návrh 62**

**Návrh nariadenia**
**Článok 18 – odsek 1**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| 1. Na žiadosť Komisie, siete EU-CyCLONe alebo siete jednotiek CSIRT agentúra ENISA preskúma a posúdi | 1. Na žiadosť Komisie, siete EU-CyCLONe alebo siete jednotiek CSIRT agentúra ENISA preskúma a posúdi |

| | |
|---|---|
| hrozby, zraniteľnosti a zmierňujúce opatrenia, pokiaľ ide o konkrétny významný alebo rozsiahly kybernetický incident. Po dokončení preskúmania a posúdenia incidentu predloží agentúra ENISA správu o preskúmaní incidentu sieti jednotiek CSIRT, sieti EU-CyCLONe a Komisii s cieľom podporiť ich pri plnení ich úloh, najmä so zreteľom na úlohy stanovené v článkoch 15 a 16 smernice (EÚ) 2022/2555. V prípade potreby Komisia správu poskytne vysokému predstaviteľovi. | hrozby, zraniteľnosti a zmierňujúce opatrenia, pokiaľ ide o konkrétny významný alebo rozsiahly kybernetický incident. Po dokončení preskúmania a posúdenia incidentu predloží agentúra ENISA správu o preskúmaní incidentu sieti jednotiek CSIRT, sieti EU-CyCLONe a Komisii s cieľom podporiť ich pri plnení ich úloh, najmä so zreteľom na úlohy stanovené v článkoch 15 a 16 smernice (EÚ) 2022/2555. V prípade potreby***, najmä ak sa incident týka tretej krajiny,*** Komisia správu poskytne vysokému predstaviteľovi ***a ESVČ***. |

**Pozmeňujúci návrh 63**

**Návrh nariadenia**
**Článok 18 – odsek 3 a (nový)**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| | ***3a. Správa sa poskytuje Európskemu parlamentu v súlade s právom Únie alebo vnútroštátnym právom o ochrane citlivých utajovaných skutočností.*** |

**Pozmeňujúci návrh 64**

**Návrh nariadenia**
**Článok 19 – odsek 1 – bod 1 – písmeno a – bod 1**
Nariadenie (EÚ) 2021/694
Článok 6 – odsek 1

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| aa) podpora rozvoja kybernetického štítu EÚ vrátane rozvoja, nasadenia a prevádzky platforiem vnútroštátnych a cezhraničných centier bezpečnostných operácií, ktoré prispievajú k situačnej informovanosti v Únii a k zlepšovaniu spôsobilostí Únie v oblasti spravodajských informácií o kybernetických hrozbách; | aa) podpora rozvoja kybernetického štítu EÚ vrátane rozvoja, nasadenia a prevádzky platforiem vnútroštátnych a cezhraničných centier bezpečnostných operácií, ktoré prispievajú k situačnej informovanosti v Únii a k zlepšovaniu spôsobilostí Únie v oblasti spravodajských informácií o kybernetických hrozbách ***a k znižovaniu závislosti Únie od vysokorizikových dodávateľov kritického kybernetickobezpečnostného vybavenia a*** |

| | |
|---|---|
| | ***komponentov, ktorí konajú v rozpore s bezpečnostnými a obrannými záujmami Únie a jej členských štátov, ako je stanovené v rámci SZBP podľa hlavy V ZEÚ***; |

**Pozmeňujúci návrh 65**

**Návrh nariadenia**
**Článok 20 – odsek 1**

| *Text predložený Komisiou* | *Pozmeňujúci návrh* |
|---|---|
| Komisia do ***[štyri*** roky od dátumu začatia uplatňovania tohto ***nariadenia]*** predloží Európskemu parlamentu a Rade správu o hodnotení a preskúmaní tohto nariadenia. | Komisia do ***[tri*** roky od dátumu začatia uplatňovania tohto ***nariadenia a potom každé dva roky]*** predloží Európskemu parlamentu a Rade správu o hodnotení a preskúmaní tohto nariadenia. |

## POSTUP VÝBORU POŽIADANÉHO O STANOVISKO

| | |
|---|---|
| **Názov** | Stanovenie opatrení na posilnenie solidarity a kapacít v Únii na odhaľovanie kybernetických hrozieb a incidentov, prípravu a reakciu na ne |
| **Referenčné čísla** | COM(2023)0209 – C9-0136/2023 – 2023/0109(COD) |
| **Gestorský výbor**<br>dátum oznámenia na schôdzi | ITRE<br>1.6.2023 |
| **Výbor požiadaný o stanovisko**<br>dátum oznámenia na schôdzi | AFET<br>1.6.2023 |
| **Spravodajca výboru požiadaného o stanovisko:**<br>dátum vymenovania | Dragoş Tudorache<br>16.6.2023 |
| **Prerokovanie vo výbore** | 18.9.2023 |
| **Dátum prijatia** | 24.10.2023 |
| **Výsledok záverečného hlasovania** | +: 39<br>–: 4<br>0: 0 |
| **Poslanci prítomní na záverečnom hlasovaní** | Alexander Alexandrov Yordanov, Petras Auštrevičius, Traian Băsescu, Anna Bonfrisco, Włodzimierz Cimoszewicz, Katalin Cseh, Michael Gahler, 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, Demetris Papadakis, Kostas Papadakis, Tonino Picula, Thijs Reuten, Nacho Sánchez Amor, Andreas Schieder, Jordi Solé, Sergei Stanishev, Tineke Strik, Dominik Tarczyński, Dragoş Tudorache, Thomas Waitz, Bernhard Zimniok, Željana Zovko |
| **Náhradníci prítomní na záverečnom hlasovaní** | Attila Ara-Kovács, Lars Patrick Berg, Andrey Kovatchev, Georgios Kyrtsos, Sergey Lagodinsky, Giuliano Pisapia, Mick Wallace |

## ZÁVEREČNÉ HLASOVANIE PODĽA MIEN VO VÝBORE POŽIADANOM O STANOVISKO

| 39 | + |
|---|---|
| ECR | Lars Patrick Berg, Dominik Tarczyński |
| ID | Anna Bonfrisco, Jaak Madison |
| PPE | Alexander Alexandrov Yordanov, Traian Băsescu, Michael Gahler, Sunčana Glavak, Sandra Kalniete, 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 Kyrtsos, Dragoş Tudorache |
| S&D | Attila Ara-Kovács, Włodzimierz Cimoszewicz, Dietmar Köster, Pedro Marques, Sven Mikser, Matjaž Nemec, Demetris Papadakis, Tonino Picula, Giuliano Pisapia, Thijs Reuten, Nacho Sánchez Amor, Andreas Schieder, Sergei Stanishev |
| Verts/ALE | Sergey Lagodinsky, Jordi Solé, Tineke Strik, Thomas Waitz |

| 4 | - |
|---|---|
| ID | Bernhard Zimniok |
| NI | Kostas Papadakis |
| The Left | Giorgos Georgiou, Mick Wallace |

| 0 | 0 |
|---|---|
| | |

Vysvetlenie použitých znakov:
+ : za
- : proti
0 : zdržali sa hlasovania