Evropský parlament
2019-2024

Výbor pro zahraniční věci

2023/0109(COD)

27.10.2023

STANOVISKO

Výboru pro zahraniční věci

pro Výbor pro průmysl, výzkum a energetiku

k návrhu nařízení Evropského parlamentu a Rady, kterým se stanoví opatření k posílení solidarity a kapacit v Unii pro odhalování kybernetických bezpečnostních hrozeb a incidentů a pro připravenost a reakci na ně (COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

Zpravodaj: Dragoş Tudorache

PA_Legam

Pozměňovací návrh 1

Návrh nařízení
Bod odůvodnění 1

Znění navržené Komisí	*Pozměňovací návrh*
(1) Používání informačních a komunikačních technologií a závislost na nich je dnes základním aspektem ve všech odvětvích hospodářské činnosti, neboť naše orgány státní správy, společnosti a občané jsou více než kdykoli předtím vzájemně propojení a závislí, a to napříč odvětvími i hranicemi.	(1) Používání informačních a komunikačních technologií a závislost na nich je dnes základním aspektem ve všech odvětvích hospodářské ***a vojenské*** činnosti, neboť naše orgány státní správy, společnosti a občané ***a také subjekty ve vojenské a obranné oblasti*** jsou více než kdykoli předtím vzájemně propojení a závislí, a to napříč odvětvími i hranicemi.

Pozměňovací návrh 2

Návrh nařízení
Bod odůvodnění 2

Znění navržené Komisí	*Pozměňovací návrh*
(2) Rozsah, četnost a dopad kybernetických bezpečnostních incidentů se zvyšuje, včetně útoků na dodavatelský řetězec, a jejich cílem je kybernetická špionáž, ransomware nebo narušení provozu. Představují zásadní hrozbu pro fungování síťových a informačních systémů. Vzhledem k rychle se vyvíjejícímu prostředí hrozeb vyžaduje hrozba možných rozsáhlých incidentů, které mohou způsobit významné narušení a poškození kritických infrastruktur, zvýšenou připravenost na všech úrovních rámce kybernetické bezpečnosti Unie. ***Tato hrozba přesahuje*** rámec ruské vojenské agrese vůči Ukrajině a pravděpodobně ***bude*** trvat i nadále vzhledem k množství se státem spojených, kriminálních a aktivistických hackerských subjektů, které se podílejí na stávajícím geopolitickém napětí. Takové incidenty mohou narušit poskytování veřejných služeb a výkon hospodářských činností, a to i v kritických nebo vysoce kritických odvětvích, způsobit	(2) Rozsah, četnost a dopad kybernetických bezpečnostních incidentů se zvyšuje, včetně útoků na dodavatelský řetězec, a jejich cílem je kybernetická špionáž, ransomware nebo narušení provozu. Představují zásadní hrozbu pro fungování síťových a informačních systémů. Vzhledem k rychle se vyvíjejícímu prostředí hrozeb vyžaduje hrozba možných rozsáhlých incidentů, které mohou způsobit významné narušení a poškození kritických infrastruktur, zvýšenou připravenost na všech úrovních rámce kybernetické bezpečnosti Unie. ***Závažnost těchto hrozeb se stala ještě aktuálnější v souvislosti s návratem války na náš kontinent. Tyto hrozby přesahují*** rámec ruské vojenské agrese vůči Ukrajině a pravděpodobně ***budou*** trvat i nadále vzhledem k množství se státem spojených, kriminálních a aktivistických hackerských subjektů, které se podílejí na stávajícím geopolitickém napětí. Takové incidenty mohou narušit poskytování veřejných

značné finanční ztráty, podkopat důvěru uživatelů, způsobit velké škody hospodářství Unie a mohou mít i zdraví nebo životy ohrožující následky. Kybernetické bezpečnostní incidenty jsou navíc nepředvídatelné, protože se často objevují a vyvíjejí ve velmi krátkém časovém období, nejsou omezeny na konkrétní zeměpisnou oblast a vyskytují se současně nebo se okamžitě šíří v mnoha zemích.	služeb a výkon hospodářských činností, a to i v kritických nebo vysoce kritických odvětvích, způsobit značné finanční ztráty, podkopat důvěru uživatelů, způsobit velké škody hospodářství ***a bezpečnosti*** Unie a mohou mít i zdraví nebo životy ohrožující následky***, neboť by mohly narušit činnost místních či celostátních zařízení spojených s bezpečností***. Kybernetické bezpečnostní incidenty jsou navíc nepředvídatelné, protože se často objevují a vyvíjejí ve velmi krátkém časovém období, nejsou omezeny na konkrétní zeměpisnou oblast a vyskytují se současně nebo se okamžitě šíří v mnoha zemích. ***Kybernetická bezpečnost je důležitá pro ochranu našich evropských hodnot a zajišťuje fungování našich demokracií tím, že chrání naši volební infrastrukturu a demokratické postupy před veškerým zahraničním vměšováním.***

Pozměňovací návrh 3

Návrh nařízení
Bod odůvodnění 2 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	(2a) Kybernetická bezpečnost má zásadní význam pro zachování bezpečnosti naší Unie a pro zamezení tomu, aby státní i nestátní subjekty s nekalými úmysly podkopávaly naši demokracii, hospodářství a bezpečnost. Je nezbytné zabránit nejednotnosti, neboť taková situace by nebyla vhodným přístupem, zejména pokud bychom čelili hrozbě budoucího rozsáhlého kybernetického útoku zaměřeného na několik členských států současně nebo na nadnárodní kritickou infrastrukturu. Proto je zapotřebí orgán Unie, který by fungoval jako koordinační platforma pro všechny stávající i budoucí nástroje, fondy a mechanismy v oblasti kybernetické bezpečnosti.

Pozměňovací návrh 4

Návrh nařízení
Bod odůvodnění 3

Znění navržené Komisí	*Pozměňovací návrh*
(3) Je nezbytné posílit konkurenceschopnost odvětví průmyslu a služeb v Unii v rámci celé digitalizované ekonomiky a podpořit jejich digitální transformaci zvýšením úrovně kybernetické bezpečnosti na jednotném digitálním trhu. Jak je doporučeno ve třech různých návrzích konference o budoucnosti Evropy[16], je nutné zvýšit odolnost občanů, podniků a subjektů provozujících kritické infrastruktury vůči rostoucím kybernetickým bezpečnostním hrozbám, které mohou mít ničivé společenské a hospodářské dopady. Proto je třeba investovat do infrastruktur a služeb, které podpoří rychlejší odhalování kybernetických bezpečnostních hrozeb a incidentů a reakci na ně, přičemž členské státy potřebují pomoc při lepší přípravě na významné a rozsáhlé incidenty v oblasti kybernetické bezpečnosti a při reakci na ně. Unie by rovněž měla zvýšit své kapacity v těchto oblastech, zejména pokud jde o shromažďování a analýzu údajů o kybernetických bezpečnostních hrozbách a incidentech.	(3) Je nezbytné posílit konkurenceschopnost odvětví průmyslu a služeb v Unii v rámci celé digitalizované ekonomiky a podpořit jejich digitální transformaci zvýšením úrovně kybernetické bezpečnosti na jednotném digitálním trhu. Jak je doporučeno ve třech různých návrzích konference o budoucnosti Evropy[16], je nutné zvýšit odolnost občanů, podniků a subjektů provozujících kritické infrastruktury vůči rostoucím kybernetickým bezpečnostním hrozbám, které mohou mít ničivé společenské a hospodářské dopady. Proto je třeba investovat do infrastruktur a služeb, které podpoří rychlejší odhalování kybernetických bezpečnostních hrozeb a incidentů a reakci na ně, přičemž členské státy potřebují pomoc při lepší přípravě na významné a rozsáhlé incidenty v oblasti kybernetické bezpečnosti a při reakci na ně. Unie by rovněž měla zvýšit své kapacity v těchto oblastech, zejména pokud jde o shromažďování a analýzu údajů o kybernetických bezpečnostních hrozbách a incidentech***, a zlepšit svou schopnost proaktivního jednání a rozhodné reakce na kybernetické bezpečnostní hrozby a incidenty***.
[16] https://futureu.europa.eu/cs/	[16] https://futureu.europa.eu/cs/

Pozměňovací návrh 5

Návrh nařízení
Bod odůvodnění 4

Znění navržené Komisí	*Pozměňovací návrh*
(4) Unie již přijala řadu opatření ke snížení zranitelnosti a zvýšení odolnosti kritických infrastruktur a subjektů vůči rizikům v oblasti kybernetické bezpečnosti, zejména směrnici Evropského parlamentu a Rady (EU) 2022/2555[17], doporučení Komise (EU) 2017/1584[18], směrnici Evropského parlamentu a Rady 2013/40/EU[19] a nařízení Evropského parlamentu a Rady (EU) 2019/881[20]. Doporučení Rady o celounijním koordinovaném přístupu za účelem posílení odolnosti kritické infrastruktury navíc vyzývá členské státy, aby přijaly naléhavá a účinná opatření a aby loajálně, efektivně, solidárně a koordinovaně spolupracovaly mezi sebou navzájem, s Komisí a dalšími příslušnými orgány veřejné moci, jakož i s dotčenými subjekty s cílem zvýšit odolnost kritické infrastruktury používané k poskytování základních služeb na vnitřním trhu.	(4) Unie již přijala řadu opatření ke snížení zranitelnosti a zvýšení odolnosti kritických infrastruktur a subjektů vůči rizikům v oblasti kybernetické bezpečnosti, zejména směrnici Evropského parlamentu a Rady (EU) 2022/2555[17], doporučení Komise (EU) 2017/1584[18], směrnici Evropského parlamentu a Rady 2013/40/EU[19] a nařízení Evropského parlamentu a Rady (EU) 2019/881[20]. Doporučení Rady o celounijním koordinovaném přístupu za účelem posílení odolnosti kritické infrastruktury navíc vyzývá členské státy, aby přijaly naléhavá a účinná opatření a aby loajálně, efektivně, ***proaktivně,*** solidárně a koordinovaně spolupracovaly mezi sebou navzájem, s Komisí a dalšími příslušnými orgány veřejné moci, jakož i s dotčenými subjekty s cílem zvýšit odolnost kritické infrastruktury používané k poskytování základních služeb na vnitřním trhu. ***Kromě toho Unie v březnu 2022 schválila a spustila Strategický kompas pro bezpečnost a obranu, který se mimo jiné zaměřuje na posílení kybernetické bezpečnosti a prohloubení mezinárodní spolupráce s podobně smýšlejícími spojenci a demokratickými partnery, zejména v této oblasti. Kybernetická bezpečnost kromě toho tvoří ústřední bod nedávného třetího společného prohlášení o spolupráci mezi EU a NATO z ledna 2023. Zejména v závěrečné hodnotící zprávě vypracované pracovní skupinou EU-NATO se doporučuje plně využívat součinnosti mezi EU a NATO[1], včetně výměny osvědčených postupů mezi civilními a vojenskými subjekty při provádění příslušných politik a právních předpisů souvisejících s kybernetickou bezpečností.*** ***[1] https://commission.europa.eu/document/34209534-3c59-4b01-b4f0-***

[17] Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (Úř. věst. L 333, 27.12.2022).

[18] Doporučení Komise (EU) 2017/1584 ze dne 13. září 2017 o koordinované reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize (Úř. věst. L 239, 19.9.2017, s. 36).

[19] Směrnice Evropského parlamentu a Rady 2013/40/EU ze dne 12. srpna 2013 o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV (Úř. věst. L 218, 14.8.2013, s. 8).

[20] Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“) (Úř. věst. L 151, 7.6.2019, s. 15).

[17] Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (Úř. věst. L 333, 27.12.2022).

[18] Doporučení Komise (EU) 2017/1584 ze dne 13. září 2017 o koordinované reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize (Úř. věst. L 239, 19.9.2017, s. 36).

[19] Směrnice Evropského parlamentu a Rady 2013/40/EU ze dne 12. srpna 2013 o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV (Úř. věst. L 218, 14.8.2013, s. 8).

[20] Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“) (Úř. věst. L 151, 7.6.2019, s. 15).

Pozměňovací návrh 6

Návrh nařízení
Bod odůvodnění 6

Znění navržené Komisí	*Pozměňovací návrh*
(6) Společné sdělení o politice kybernetické obrany EU[22] přijaté 10. listopadu 2022 oznámilo iniciativu EU pro kybernetickou solidaritu s těmito cíli: posílit společné schopnosti EU v oblasti odhalování, situačního povědomí a reakce podporou zavádění infrastruktury EU v	(6) Společné sdělení o politice kybernetické obrany EU[22] přijaté 10. listopadu 2022 oznámilo iniciativu EU pro kybernetickou solidaritu s těmito cíli: posílit společné schopnosti EU v oblasti odhalování, situačního povědomí a reakce podporou zavádění infrastruktury EU v

podobě bezpečnostních operačních středisek, podporovat postupné vytváření rezervy pro kybernetickou bezpečnost na úrovni EU se službami důvěryhodných soukromých poskytovatelů a testování kritických subjektů na potenciální zranitelnost na základě posouzení rizik v EU.

podobě bezpečnostních operačních středisek, podporovat postupné vytváření rezervy pro kybernetickou bezpečnost na úrovni EU se službami důvěryhodných soukromých poskytovatelů a testování kritických subjektů na potenciální zranitelnost na základě posouzení rizik v EU. ***Rychle se vyvíjející oblast kybernetických hrozeb a překotný technologický vývoj navíc ukazují, že je zapotřebí posílené civilně-vojenské koordinace a spolupráce, jak zdůraznila Rada ve svých závěrech o politice EU pro kybernetickou obranu[1].***

[1] Závěry Rady o politice EU pro kybernetickou obranu schválené Radou na zasedání dne 22. května 2023 (9618/23).

---

[22] Společné sdělení Evropskému parlamentu a Radě, Politika kybernetické obrany EU, JOIN/2022/49 final.

[22] Společné sdělení Evropskému parlamentu a Radě, Politika kybernetické obrany EU, JOIN/2022/49 final.

Pozměňovací návrh 7

Návrh nařízení
Bod odůvodnění 6 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	(6a) Vzhledem k nejasným hranicím mezi oblastí civilních a vojenských záležitosti a dvojímu využití kybernetických nástrojů a technologií je třeba, aby byl v digitální oblasti uplatňován komplexní a celostní přístup. V případě rozsáhlého kybernetického bezpečnostního incidentu a krize zahrnující více než jeden členský stát by mělo být zavedeno odpovídající řešení a řízení krize. Tyto struktury by měly organizovat výměnu informací, koordinaci a spolupráci se strukturami Unie v oblasti vnější bezpečnosti a řízení vojenských krizí a se subjekty členských států odpovědnými za bezpečnost a

obranu (komunitou kybernetické obrany). To by se mělo vztahovat i na operace a mise v rámci společné bezpečnostní a obranné politiky, které provádí Unie s cílem zajistit mír a stabilitu ve svém sousedství i mimo něj.

Pozměňovací návrh 8

Návrh nařízení
Bod odůvodnění 7

Znění navržené Komisí	*Pozměňovací návrh*
(7) Je nezbytné posílit odhalování kybernetických hrozeb a incidentů a situační povědomí v celé Unii a posílit solidaritu tím, že se zvýší připravenost a schopnost členských států a Unie reagovat na významné a rozsáhlé kybernetické bezpečnostní incidenty. Proto by měla být zavedena celoevropská infrastruktura bezpečnostních operačních středisek (evropský kybernetický štít) s cílem vybudovat a posílit společné schopnosti odhalování a situačního povědomí; měl by být zřízen mechanismus pro mimořádné události v oblasti kybernetické bezpečnosti, který by podporoval členské státy při přípravě na významné a rozsáhlé incidenty v oblasti kybernetické bezpečnosti, při reakci na ně a při okamžité obnově po nich; měl by být zřízen mechanismus přezkumu kybernetických bezpečnostních incidentů, který by přezkoumával a posuzoval konkrétní významné nebo rozsáhlé incidenty. Těmito opatřeními nejsou dotčeny články 107 a 108 Smlouvy o fungování Evropské unie (dále jen „SFEU“).	(7) Je nezbytné posílit odhalování kybernetických hrozeb a incidentů a situační povědomí v celé Unii a posílit solidaritu tím, že se zvýší připravenost a schopnost členských států a Unie reagovat na významné a rozsáhlé kybernetické bezpečnostní incidenty. Proto by měla být zavedena celoevropská infrastruktura bezpečnostních operačních středisek (evropský kybernetický štít) s cílem vybudovat a posílit společné schopnosti odhalování a situačního povědomí; měl by být zřízen mechanismus pro mimořádné události v oblasti kybernetické bezpečnosti, který by podporoval členské státy při přípravě na významné a rozsáhlé incidenty v oblasti kybernetické bezpečnosti, při reakci na ně a při okamžité obnově po nich***, včetně incidentů zahrnujících více než jeden členský stát. Je-li to proveditelné a nezbytné, měl by mechanismus pro mimořádné situace v oblasti kybernetické bezpečnosti organizovat výměnu informací a spolupráci s obrannými orgány členských států a měl by být podporován orgány, institucemi a jinými subjekty EU (společenství EU v oblasti kybernetické obrany)***; měl by být zřízen mechanismus přezkumu kybernetických bezpečnostních incidentů, který by přezkoumával a posuzoval konkrétní významné nebo rozsáhlé incidenty***. Tyto nové struktury by rovněž měly podporovat operace a mise SBOP EU***. Těmito

opatřeními nejsou dotčeny články 107 a 108 Smlouvy o fungování Evropské unie (dále jen „SFEU“).

Pozměňovací návrh 9

Návrh nařízení
Bod odůvodnění 11

Znění navržené Komisí	*Pozměňovací návrh*
(11) Pro účely řádného finančního řízení by měla být stanovena zvláštní pravidla pro přenos nevyužitých prostředků na závazky a platby. Při respektování zásady, že rozpočet Unie je stanovován na ročním základě, by toto nařízení mělo vzhledem k nepředvídatelné, výjimečné a specifické povaze prostředí kybernetické bezpečnosti stanovit možnosti přenosu nevyužitých finančních prostředků nad rámec prostředků stanovených ve finančním nařízení, čímž by se maximalizovala schopnost mechanismu pro mimořádné události v oblasti kybernetické bezpečnosti účinně podporovat členské státy v boji proti kybernetickým hrozbám.	(11) Pro účely řádného finančního řízení by měla být stanovena zvláštní pravidla pro přenos nevyužitých prostředků na závazky a platby. Při respektování zásady, že rozpočet Unie je stanovován na ročním základě, by toto nařízení mělo vzhledem k nepředvídatelné, výjimečné a specifické povaze prostředí kybernetické bezpečnosti stanovit možnosti přenosu nevyužitých finančních prostředků nad rámec prostředků stanovených ve finančním nařízení, čímž by se maximalizovala schopnost mechanismu pro mimořádné události v oblasti kybernetické bezpečnosti účinně podporovat členské státy v boji proti kybernetickým hrozbám. ***Tato zvláštní pravidla by rovněž umožnila dlouhodobější finanční podporu pro společné zadávání zakázek na vysoce bezpečné nástroje a infrastrukturu nové generace, aby se zlepšily schopnosti kolektivního odhalování s využitím nejnovějších technologií umělé inteligence a analýzy dat.***

Pozměňovací návrh 10

Návrh nařízení
Bod odůvodnění 13

Znění navržené Komisí	*Pozměňovací návrh*
(13) Každý členský stát by měl určit veřejnoprávní subjekt na vnitrostátní úrovni, který bude pověřen koordinací činností v oblasti odhalování	(13) Každý členský stát by měl určit veřejnoprávní subjekt na vnitrostátní úrovni, který bude pověřen koordinací činností v oblasti odhalování

kybernetických hrozeb v daném členském státě. Tato národní bezpečnostní operační střediska by měla na vnitrostátní úrovni fungovat jako referenční bod a brána pro účast v evropském kybernetickém štítu a měla by zajistit, aby informace o kybernetických hrozbách od veřejných a soukromých subjektů byly na vnitrostátní úrovni sdíleny a shromažďovány účinně a efektivně.

kybernetických hrozeb v daném členském státě. Tato národní bezpečnostní operační střediska by měla na vnitrostátní úrovni fungovat jako referenční bod a brána pro účast v evropském kybernetickém štítu a měla by zajistit, aby informace o kybernetických hrozbách od veřejných a soukromých subjektů byly na vnitrostátní úrovni sdíleny a shromažďovány účinně a efektivně. ***Je-li to proveditelné a nezbytné, měla by bezpečnostní operační střediska rovněž umožnit účast obranných subjektů vytvořením „obranného pilíře“, pokud jde o správu a druh sdílených informací, jak je uvedeno ve společném sdělení o politice kybernetické obrany EU[1] a jak jej podpořil vysoký představitel.***

[1] Společné sdělení Evropskému parlamentu a Radě, Politika kybernetické obrany EU, JOIN/2022/49 final

Pozměňovací návrh 11

Návrh nařízení
Bod odůvodnění 14

Znění navržené Komisí	*Pozměňovací návrh*
(14) V rámci evropského kybernetického štítu by měla být zřízena řada přeshraničních operačních středisek v oblasti kybernetické bezpečnosti (dále jen „přeshraniční bezpečnostní operační střediska“). Ta by měla sdružovat národní bezpečnostní operační střediska alespoň ze tří členských států, aby bylo možné plně využít výhod přeshraničního odhalování hrozeb a sdílení a správy informací. Obecným cílem přeshraničních bezpečnostních operačních středisek by mělo být posílení kapacit pro analýzu, prevenci a odhalování kybernetických bezpečnostních hrozeb a podpora vytváření vysoce kvalitních zpravodajských informací o kybernetických bezpečnostních hrozbách, zejména prostřednictvím sdílení údajů z různých zdrojů, ať už veřejných	(14) V rámci evropského kybernetického štítu by měla být zřízena řada přeshraničních operačních středisek v oblasti kybernetické bezpečnosti (dále jen „přeshraniční bezpečnostní operační střediska“). Ta by měla sdružovat národní bezpečnostní operační střediska alespoň ze tří členských států, ***včetně „obranného pilíře“,*** aby bylo možné plně využít výhod přeshraničního odhalování hrozeb a sdílení a správy informací. Obecným cílem přeshraničních bezpečnostních operačních středisek by mělo být posílení kapacit pro analýzu, prevenci a odhalování kybernetických bezpečnostních hrozeb a podpora vytváření vysoce kvalitních zpravodajských informací o kybernetických bezpečnostních hrozbách, zejména prostřednictvím sdílení údajů z

nebo soukromých, jakož i prostřednictvím sdílení a společného využívání nejmodernějších nástrojů a společným rozvojem schopností odhalování, analýzy a prevence v důvěryhodném prostředí. Měla by poskytnout nové dodatečné kapacity, které budou vycházet ze stávajících bezpečnostních operačních středisek a týmů pro reakce na počítačové bezpečnostní incidenty (dále jen „týmy CSIRT“) a dalších příslušných subjektů a budou je doplňovat.

různých zdrojů, ať už veřejných nebo soukromých, ***a je-li to proveditelné a nezbytné, z vojenských zdrojů s dostatečnými pokyny ohledně sdílení informací,*** jakož i prostřednictvím sdílení a společného využívání nejmodernějších nástrojů a společným rozvojem schopností odhalování, analýzy a prevence v důvěryhodném prostředí. Měla by poskytnout nové dodatečné kapacity, které budou vycházet ze stávajících bezpečnostních operačních středisek a týmů pro reakce na počítačové bezpečnostní incidenty (dále jen „týmy CSIRT“) a dalších příslušných subjektů a budou je doplňovat.

Pozměňovací návrh 12

Návrh nařízení
Bod odůvodnění 15

Znění navržené Komisí	*Pozměňovací návrh*
(15) Na vnitrostátní úrovni zajišťují monitorování, odhalování a analýzu kybernetických hrozeb obvykle bezpečnostní operační střediska veřejných a soukromých subjektů v kombinaci s týmy CSIRT. Kromě toho si týmy CSIRT vyměňují informace v rámci sítě CSIRT v souladu se směrnicí (EU) 2022/2555. Přeshraniční bezpečnostní operační střediska by měla představovat novou kapacitu, která doplní síť týmů pro reakce na kybernetické bezpečnostní incidenty, neboť bude sdružovat a sdílet údaje o kybernetických bezpečnostních hrozbách od veřejných a soukromých subjektů, zvyšovat hodnotu těchto údajů prostřednictvím odborné analýzy a společně pořízené infrastruktury a nejmodernějších nástrojů a přispívat k rozvoji schopností a ***technologické suverenity*** Unie.	(15) Na vnitrostátní úrovni zajišťují monitorování, odhalování a analýzu kybernetických hrozeb obvykle bezpečnostní operační střediska veřejných a soukromých subjektů v kombinaci s týmy CSIRT. Kromě toho si týmy CSIRT vyměňují informace v rámci sítě CSIRT v souladu se směrnicí (EU) 2022/2555. Přeshraniční bezpečnostní operační střediska by měla představovat novou kapacitu, která doplní síť týmů pro reakce na kybernetické bezpečnostní incidenty, neboť bude sdružovat a sdílet údaje o kybernetických bezpečnostních hrozbách od veřejných a soukromých subjektů, zvyšovat hodnotu těchto údajů prostřednictvím odborné analýzy a společně pořízené infrastruktury a nejmodernějších nástrojů a přispívat k rozvoji schopností a ***odolnosti*** Unie.

Pozměňovací návrh 13

Návrh nařízení
Bod odůvodnění 16

Znění navržené Komisí	*Pozměňovací návrh*
(16) Přeshraniční bezpečnostní operační střediska by měla fungovat jako ústřední bod umožňující široké sdružování příslušných údajů a zpravodajských informací o kybernetických hrozbách, umožňovat šíření informací o hrozbách mezi velkým a různorodým souborem subjektů (např. týmy pro reakci na počítačové hrozby (dále jen „týmy CERT“), týmy CSIRT, střediska pro sdílení a analýzu informací (dále jen „střediska ISAC“), provozovatelé kritických infrastruktur). Informace vyměňované mezi účastníky přeshraničního bezpečnostního operačního střediska mohou zahrnovat údaje ze sítí a čidel, zpravodajské informace o hrozbách, indikátory narušení a kontextualizované informace o incidentech, hrozbách a zranitelnostech. Přeshraniční bezpečnostní operační střediska by také měla uzavírat dohody o spolupráci s jinými přeshraničními bezpečnostními operačními středisky.	(16) Přeshraniční bezpečnostní operační střediska by měla fungovat jako ústřední bod umožňující široké sdružování příslušných údajů a zpravodajských informací o kybernetických hrozbách, umožňovat šíření informací o hrozbách mezi velkým a různorodým souborem subjektů (např. týmy pro reakci na počítačové hrozby (dále jen „týmy CERT“), týmy CSIRT, střediska pro sdílení a analýzu informací (dále jen „střediska ISAC“), provozovatelé kritických infrastruktur***, jakož i komunita kybernetické obrany***). Informace vyměňované mezi účastníky přeshraničního bezpečnostního operačního střediska mohou zahrnovat údaje ze sítí a čidel, zpravodajské informace o hrozbách, indikátory narušení a kontextualizované informace o incidentech, hrozbách a zranitelnostech. Přeshraniční bezpečnostní operační střediska by také měla uzavírat dohody o spolupráci s jinými přeshraničními bezpečnostními operačními středisky ***a s operační sítí pro vojenské týmy pro reakci na počítačové hrozby (vojenské týmy CERT) – sítí MICNET, až bude vytvořena***.

Pozměňovací návrh 14

Návrh nařízení
Bod odůvodnění 17

Znění navržené Komisí	*Pozměňovací návrh*
(17) Sdílené situační povědomí mezi příslušnými orgány je nezbytným předpokladem připravenosti a koordinace v celé Unii, pokud jde o významné a rozsáhlé kybernetické bezpečnostní	(17) Sdílené situační povědomí mezi příslušnými orgány je nezbytným předpokladem připravenosti a koordinace v celé Unii, pokud jde o významné a rozsáhlé kybernetické bezpečnostní

incidenty. Směrnice (EU) 2022/2555 zřizuje síť EU–CyCLONe za účelem podpory koordinovaného řešení rozsáhlých kybernetických bezpečnostních incidentů a krizí na operativní úrovni a pro zajištění pravidelné výměny relevantních informací mezi členskými státy a orgány, institucemi nebo jinými subjekty Unie. Doporučení (EU) 2017/1584 o koordinované reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize se zabývá úlohou všech příslušných aktérů. Směrnice (EU) 2022/2555 rovněž připomíná povinnosti Komise v rámci mechanismu civilní ochrany Unie zřízeného rozhodnutím Evropského parlamentu a Rady 1313/2013/EU, jakož i povinnost poskytování analytických zpráv pro opatření integrovaného mechanismu pro politickou reakci na krize podle prováděcího rozhodnutí (EU) 2018/1993. V situacích, kdy přeshraniční bezpečnostní operační střediska získají informace týkající se potenciálního nebo probíhajícího rozsáhlého kybernetického bezpečnostního incidentu, by proto měla poskytnout příslušné informace síti EU-CyCLONe, síti CSIRT a Komisi. V závislosti na situaci mohou informace, které mají být sdíleny, zahrnovat zejména technické údaje, informace o povaze a motivech útočníka nebo potenciálního útočníka a jiné než technické údaje vyšší úrovně o potenciálním nebo probíhajícím rozsáhlém kybernetickém bezpečnostním incidentu. V této souvislosti je třeba věnovat náležitou pozornost zásadě „vědět jen to nejnutnější“ a potenciálně citlivé povaze sdílených informací.

incidenty. Směrnice (EU) 2022/2555 zřizuje síť EU–CyCLONe za účelem podpory koordinovaného řešení rozsáhlých kybernetických bezpečnostních incidentů a krizí na operativní úrovni a pro zajištění pravidelné výměny relevantních informací mezi členskými státy a orgány, institucemi nebo jinými subjekty Unie. Doporučení (EU) 2017/1584 o koordinované reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize se zabývá úlohou všech příslušných aktérů. Směrnice (EU) 2022/2555 rovněž připomíná povinnosti Komise v rámci mechanismu civilní ochrany Unie zřízeného rozhodnutím Evropského parlamentu a Rady 1313/2013/EU, jakož i povinnost poskytování analytických zpráv pro opatření integrovaného mechanismu pro politickou reakci na krize podle prováděcího rozhodnutí (EU) 2018/1993. V situacích, kdy přeshraniční bezpečnostní operační střediska získají informace týkající se potenciálního nebo probíhajícího rozsáhlého kybernetického bezpečnostního incidentu, by proto měla poskytnout příslušné informace síti EU-CyCLONe, síti CSIRT***, komunitě kybernetické obrany*** a Komisi. V závislosti na situaci mohou informace, které mají být sdíleny, zahrnovat zejména technické údaje, informace o povaze a motivech útočníka nebo potenciálního útočníka a jiné než technické údaje vyšší úrovně o potenciálním nebo probíhajícím rozsáhlém kybernetickém bezpečnostním incidentu. V této souvislosti je třeba věnovat náležitou pozornost zásadě „vědět jen to nejnutnější“ a potenciálně citlivé povaze sdílených informací.

Pozměňovací návrh 15

Návrh nařízení
Bod odůvodnění 19

Znění navržené Komisí	*Pozměňovací návrh*
(19) Aby byla umožněna rozsáhlá výměna údajů o kybernetických bezpečnostních hrozbách z různých zdrojů v důvěryhodném prostředí, měly by být subjekty zapojené do evropského kybernetického štítu vybaveny nejmodernějšími a vysoce bezpečnými nástroji, zařízeními a infrastrukturami. Díky tomu by mělo být možné zlepšit schopnost kolektivního odhalování a včasného varování orgánů a příslušných subjektů, zejména s využitím nejnovějších technologií umělé inteligence a analýzy dat.	(19) Aby byla umožněna rozsáhlá výměna údajů o kybernetických bezpečnostních hrozbách z různých zdrojů v důvěryhodném prostředí, měly by být subjekty zapojené do evropského kybernetického štítu***, s výjimkou vysoce rizikových dodavatelů kritických produktů s digitálními prvky,*** vybaveny nejmodernějšími a vysoce bezpečnými nástroji, zařízeními a infrastrukturami. Díky tomu by mělo být možné zlepšit schopnost kolektivního odhalování a včasného varování orgánů a příslušných subjektů, zejména s využitím nejnovějších technologií umělé inteligence a analýzy dat. ***Při používání umělé inteligence by měl být zajištěn lidský dohled a dostatečná úroveň gramotnosti v oblasti umělé inteligence, nezbytná podpora a pravomoc k výkonu této funkce.***

Pozměňovací návrh 16

Návrh nařízení
Bod odůvodnění 19 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	(19 a) V souladu s nařízením [XX/XXXX (akt o kybernetické odolnosti)] by subjekty zapojené do evropského kybernetického štítu měly požadavky stanovené v tomto nařízení splnit také u všech produktů s digitálními prvky. Vzhledem k rostoucím rizikům plynoucím z ekonomických závislostí je nutné minimalizovat vystavení vysoce rizikovým dodavatelům kritických produktů prostřednictvím společného strategického rámce pro hospodářskou bezpečnost EU. Závislost na vysoce rizikových dodavatelích kritických produktů s digitálními prvky představuje strategické riziko, které je třeba řešit na úrovni Unie, zejména pokud se určitá země dopouští hospodářské špionáže nebo

	vyvíjí ekonomický nátlak a její právní předpisy zavazují ke svévolnému přístupu k jakémukoli druhu operací nebo údajů společností, zejména pokud jsou kritické produkty určeny k použití základními subjekty ve smyslu směrnice (EU) 2022/2555.

Pozměňovací návrh 17

Návrh nařízení
Bod odůvodnění 20

Znění navržené Komisí	*Pozměňovací návrh*
(20) Prostřednictvím shromažďování, sdílení a výměny údajů by měl evropský kybernetický štít posílit technologickou suverenitu Unie. Sdružování vysoce kvalitních kontrolovaných údajů by mělo rovněž přispět k rozvoji pokročilých technologií umělé inteligence a analýzy dat. Mělo by být usnadněno propojením evropského kybernetického štítu s celoevropskou infrastrukturou pro vysoce výkonnou výpočetní techniku zřízenou nařízením Rady (EU) 2021/1173[25].	(20) Prostřednictvím shromažďování, sdílení a výměny údajů by měl evropský kybernetický štít posílit technologickou suverenitu Unie***, její strategickou autonomii, konkurenceschopnost a odolnost***. Sdružování vysoce kvalitních kontrolovaných údajů by mělo rovněž přispět k rozvoji pokročilých technologií umělé inteligence a analýzy dat. Mělo by být usnadněno propojením evropského kybernetického štítu s celoevropskou infrastrukturou pro vysoce výkonnou výpočetní techniku zřízenou nařízením Rady (EU) 2021/1173[25].
[25] Nařízení Rady (EU) 2021/1173 ze dne 13. července 2021, kterým se zřizuje společný podnik pro evropskou vysoce výkonnou výpočetní techniku a zrušuje nařízení (EU) 2018/1488 (Úř. věst. L 256, 19.7.2021, s. 3).	[25]Nařízení Rady (EU) 2021/1173 ze dne 13. července 2021, kterým se zřizuje společný podnik pro evropskou vysoce výkonnou výpočetní techniku a zrušuje nařízení (EU) 2018/1488 (Úř. věst. L 256, 19.7.2021, s. 3).

Pozměňovací návrh 18

Návrh nařízení
Bod odůvodnění 25

Znění navržené Komisí	*Pozměňovací návrh*
(25) Mechanismus pro mimořádné události v kybernetické oblasti by měl	(25) Mechanismus pro mimořádné události v kybernetické oblasti by měl

členským státům poskytovat podporu doplňující jejich vlastní opatření a zdroje a další stávající možnosti podpory v případě reakce na významné a rozsáhlé kybernetické bezpečnostní incidenty a okamžité obnovy po nich, jako jsou služby poskytované Agenturou Evropské unie pro bezpečnost sítí a informací (dále jen „ENISA“) v souladu s jejím mandátem, koordinovaná reakce a pomoc ze strany sítě CSIRT, podpora při zmírňování následků ze strany sítě EU-CyCLONe, jakož i vzájemná pomoc mezi členskými státy, a to i v kontextu čl. 42 odst. 7 SEU, týmy rychlé reakce v kybernetickém prostoru v rámci stálé strukturované ***spolupráce26*** a hybridní týmy rychlé reakce. Měl by zajistit, aby byly k dispozici specializované prostředky na podporu připravenosti a reakce na kybernetické bezpečnostní incidenty v celé Unii a ve třetích zemích.

[26] ROZHODNUTÍ RADY (SZBP) 2017/2315 ze dne 11. prosince 2017, kterým se zřizuje stálá strukturovaná spolupráce a stanoví seznam zúčastněných členských států.

členským státům poskytovat podporu doplňující jejich vlastní opatření a zdroje a další stávající možnosti podpory v případě reakce na významné a rozsáhlé kybernetické bezpečnostní incidenty a okamžité obnovy po nich, jako jsou služby poskytované Agenturou Evropské unie pro bezpečnost sítí a informací (dále jen „ENISA“) v souladu s jejím mandátem, koordinovaná reakce a pomoc ze strany sítě CSIRT, podpora při zmírňování následků ze strany sítě EU-CyCLONe, jakož i vzájemná pomoc mezi členskými státy, a to i v kontextu čl. 42 odst. 7 SEU, týmy rychlé reakce v kybernetickém prostoru v rámci stálé strukturované ***spolupráce[1], nový projekt PESCO Koordinační středisko pro kybernetický a informační prostor (CIDCC) a navrhované koordinační středisko EU pro kybernetickou obranu (EUCDCC), které jej má nahradit,*** a hybridní týmy rychlé reakce. Měl by zajistit, aby byly k dispozici specializované prostředky na podporu připravenosti a reakce na kybernetické bezpečnostní incidenty v celé Unii a ve třetích zemích***, zejména v těchkandidátských zemích EU, které dosáhly souladu se společnou zahraniční a bezpečnostní politikou a společnou bezpečnostní a obrannou politikou EU, a bylo možné je podpořit v úsilí o budování vlastních kapacit kybernetické obrany a posílit přeshraniční a regionální spolupráci mezi těmito kandidátskými zeměmi v kybernetické oblasti***.

[1] ROZHODNUTÍ RADY (SZBP) 2017/2315 ze dne 11. prosince 2017, kterým se zřizuje stálá strukturovaná spolupráce a stanoví seznam zúčastněných členských států.

[26] ROZHODNUTÍ RADY (SZBP) 2017/2315 ze dne 11. prosince 2017, kterým se zřizuje stálá strukturovaná spolupráce a stanoví seznam zúčastněných členských států.

Pozměňovací návrh 19

Návrh nařízení
Bod odůvodnění 26

Znění navržené Komisí	*Pozměňovací návrh*
(26) Tímto nástrojem nejsou dotčeny postupy a rámce pro koordinaci reakce na krize na úrovni Unie, zejména mechanismus civilní ochrany Unie[27], integrovaná opatření EU pro politickou reakci na krize[28], a směrnice (EU) 2022/2555. Může přispívat k opatřením prováděným v souvislosti s čl. 42 odst. 7 SEU nebo v situacích vymezených v článku 222 SFEU nebo tato opatření doplňovat. ***Používání*** tohoto nástroje by mělo být ***v případě potřeby*** koordinováno s prováděním opatření souboru nástrojů ***kybernetické diplomacie***.	(26) Tímto nástrojem nejsou dotčeny postupy a rámce pro koordinaci reakce na krize na úrovni Unie, zejména mechanismus civilní ochrany Unie[27], integrovaná opatření EU pro politickou reakci na krize[28], a směrnice (EU) 2022/2555. Může přispívat k opatřením prováděným v souvislosti s čl. 42 odst. 7 SEU nebo v situacích vymezených v článku 222 SFEU nebo tato opatření doplňovat. ***Používání*** tohoto nástroje by mělo být ***rovněž*** koordinováno s prováděním opatření souboru nástrojů ***kybernetické diplomacie, čímž se posílí spolupráce na strategické, operační a technické úrovni mezi komunitou kybernetické obrany a dalšími komunitami v kybernetické oblasti, zejména za účelem posílení schopnosti bojovat proti kybernetickým hrozbám ze zemí mimo Unii, včetně restriktivních opatření, která lze využít k předcházení nepřátelské činnosti v kyberprostoru a k reakci na ni***.
[27] Rozhodnutí Evropského parlamentu a Rady č. 1313/2013/EU ze dne 17. prosince 2013 o mechanismu civilní ochrany Unie (Úř. věst. L 347, 20.12.2013, s. 924).	[27] Rozhodnutí Evropského parlamentu a Rady č. 1313/2013/EU ze dne 17. prosince 2013 o mechanismu civilní ochrany Unie (Úř. věst. L 347, 20.12.2013, s. 924).
[28] Integrovaná opatření EU pro politickou reakci na krize (IPCR) a v souladu s doporučením Komise (EU) 2017/1584 ze dne 13. září 2017 o koordinované reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize.	[28] Integrovaná opatření EU pro politickou reakci na krize (IPCR) a v souladu s doporučením Komise (EU) 2017/1584 ze dne 13. září 2017 o koordinované reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize.

Pozměňovací návrh 20

Návrh nařízení
Bod odůvodnění 28

Znění navržené Komisí	*Pozměňovací návrh*
(28) Směrnice (EU) 2022/2555 vyžaduje, aby členské státy určily nebo zřídily jeden nebo více orgánů pro řešení kybernetických krizí a zajistily, aby tyto orgány měly k dispozici odpovídající zdroje pro účinné a účelné plnění svěřených úkolů. Požaduje také, aby členské státy určily kapacity, prostředky a postupy, které mohou být nasazeny v případě krize, a aby přijaly národní plán reakce na rozsáhlé kybernetické bezpečnostní incidenty a krize, v němž budou stanoveny cíle a způsoby řešení rozsáhlých kybernetických bezpečnostních incidentů a krizí. Členské státy jsou rovněž povinny zřídit jeden nebo více týmů CSIRT, které budou pověřeny odpovědností za řešení incidentů podle řádně vymezeného postupu a budou pokrývat alespoň odvětví, pododvětví a druhy subjektů spadající do oblasti působnosti uvedené směrnice, a zajistit, aby tyto týmy měly pro účinné plnění svých úkolů odpovídající zdroje. Tímto nařízením není dotčena úloha Komise při zajišťování toho, aby členské státy plnily povinnosti vyplývající ze směrnice (EU) 2022/2555. Mechanismus pro mimořádné události v kybernetické oblasti by měl poskytovat pomoc při opatřeních zaměřených na posílení připravenosti, jakož i při opatřeních v reakci na incidenty s cílem zmírnit dopady významných a rozsáhlých kybernetických bezpečnostních incidentů, podpořit okamžitou obnovu a/nebo obnovit fungování základních služeb.	(28) Směrnice (EU) 2022/2555 vyžaduje, aby členské státy určily nebo zřídily jeden nebo více orgánů pro řešení kybernetických krizí a zajistily, aby tyto orgány měly k dispozici odpovídající zdroje pro účinné a účelné plnění svěřených úkolů. Požaduje také, aby členské státy určily kapacity, prostředky a postupy, které mohou být nasazeny v případě krize, a aby přijaly národní plán reakce na rozsáhlé kybernetické bezpečnostní incidenty a krize, v němž budou stanoveny cíle a způsoby řešení rozsáhlých kybernetických bezpečnostních incidentů a krizí. Členské státy jsou rovněž povinny zřídit jeden nebo více týmů CSIRT, které budou pověřeny odpovědností za řešení incidentů podle řádně vymezeného postupu a budou pokrývat alespoň odvětví, pododvětví a druhy subjektů spadající do oblasti působnosti uvedené směrnice, a zajistit, aby tyto týmy měly pro účinné plnění svých úkolů odpovídající zdroje. Tímto nařízením není dotčena úloha Komise při zajišťování toho, aby členské státy plnily povinnosti vyplývající ze směrnice (EU) 2022/2555. Mechanismus pro mimořádné události v kybernetické oblasti by měl poskytovat pomoc při opatřeních zaměřených na posílení připravenosti, jakož i při opatřeních v reakci na incidenty s cílem zmírnit dopady významných a rozsáhlých kybernetických bezpečnostních incidentů, podpořit okamžitou obnovu a/nebo obnovit fungování základních služeb***, přičemž by měl vhodným způsobem využívat celé řady možností obrany dostupných civilním a vojenským komunitám***.

Pozměňovací návrh 21

Návrh nařízení
Bod odůvodnění 29

Znění navržené Komisí	*Pozměňovací návrh*
(29) V rámci opatření v oblasti připravenosti by měla být v zájmu prosazování jednotného přístupu a posílení bezpečnosti v celé Unii a na jejím vnitřním trhu poskytována podpora pro koordinované testování a posuzování kybernetické bezpečnosti subjektů působících ve vysoce kritických odvětvích určených podle směrnice (EU) 2022/2555. Za tímto účelem by měla Komise s podporou agentury ENISA a ve spolupráci se skupinou pro spolupráci v oblasti bezpečnosti sítí a informací zřízenou směrnicí (EU) 2022/2555 pravidelně určovat příslušná odvětví nebo pododvětví, která by měla být způsobilá pro získání finanční podpory na koordinované testování na úrovni Unie. Odvětví nebo pododvětví by měla být vybrána z přílohy I směrnice (EU) 2022/2555 (dále jen „vysoce kritická odvětví“). Koordinované testování by mělo být založeno na společných scénářích a metodikách týkajících se rizik. Výběr odvětví a vypracování rizikových scénářů by měly zohlednit příslušná hodnocení rizik a scénáře rizik pro celou Unii, včetně potřeby vyhnout se zdvojování, jako jsou hodnocení rizik a rizikové scénáře, které požaduje Rada v závěrech o rozvoji kybernetické pozice Evropské unie, které mají provádět Komise, vysoký představitel a skupina pro spolupráci v oblasti bezpečnosti sítí a informací v koordinaci s příslušnými civilními i vojenskými orgány a agenturami a se zavedenými sítěmi včetně sítě EU CyCLONe, jakož i posouzení rizik komunikačních sítí a infrastruktur, které požaduje společná výzva ministrů z Nevers a které provádí skupina pro spolupráci v oblasti bezpečnosti sítí a informací za podpory	(29) V rámci opatření v oblasti připravenosti by měla být v zájmu prosazování jednotného přístupu a posílení bezpečnosti v celé Unii a na jejím vnitřním trhu poskytována podpora pro koordinované testování a posuzování kybernetické bezpečnosti subjektů působících ve vysoce kritických odvětvích určených podle směrnice (EU) 2022/2555. Za tímto účelem by měla Komise s podporou agentury ENISA a ve spolupráci se skupinou pro spolupráci v oblasti bezpečnosti sítí a informací zřízenou směrnicí (EU) 2022/2555 pravidelně určovat příslušná odvětví nebo pododvětví, která by měla být způsobilá pro získání finanční podpory na koordinované testování na úrovni Unie. ***Evropská služba pro vnější činnost (ESVČ), zejména prostřednictvím Zpravodajského a informačního centra EU (EU INTCEN) a jeho střediska pro hybridní hrozby, by se v případě potřeby měla s podporou zpravodajského ředitelství Vojenského štábu EU (EUMS) v rámci společné zpravodajsko-analytické složky (SIAC) rovněž zapojit do zajištění aktuálních posouzení, a přispět tak k určení*** odvětví nebo pododvětví***, která*** by měla být vybrána z přílohy I směrnice (EU) 2022/2555 (dále jen „vysoce kritická odvětví“). Koordinované testování by mělo být založeno na společných scénářích a metodikách týkajících se rizik***. Tato testování by také měla hrát důležitou roli ve zlepšování spolupráce mezi civilními a vojenskými subjekty. Při organizování testování by proto Komise, ESVČ a agentura ENISA měly systematicky zvažovat zapojení účastníků z jiných kybernetických komunit, jako je Evropská obranná agentura (EDA) a další příslušné***

Komise a agentury ENISA a ve spolupráci se Sdružením evropských regulačních orgánů v oblasti elektronických komunikací (dále jen „BEREC“), koordinované posouzení rizik, které má být prováděno podle článku 22 směrnice (EU) 2022/2555, a testování digitální provozní odolnosti podle nařízení Evropského parlamentu a Rady (EU) 2022/***255429***. Výběr odvětví by měl rovněž zohlednit doporučení Rady o celounijním koordinovaném přístupu za účelem posílení odolnosti kritické infrastruktury.

subjekty. Výběr odvětví a vypracování rizikových scénářů by měly zohlednit příslušná hodnocení rizik a scénáře rizik pro celou Unii, včetně potřeby vyhnout se zdvojování, jako jsou hodnocení rizik a rizikové scénáře, které požaduje Rada v závěrech o rozvoji kybernetické pozice Evropské unie, které mají provádět Komise, vysoký představitel a skupina pro spolupráci v oblasti bezpečnosti sítí a informací v koordinaci s příslušnými civilními i vojenskými orgány a agenturami a se zavedenými sítěmi včetně sítě EU CyCLONe, jakož i posouzení rizik komunikačních sítí a infrastruktur, které požaduje společná výzva ministrů z Nevers a které provádí skupina pro spolupráci v oblasti bezpečnosti sítí a informací za podpory Komise a agentury ENISA a ve spolupráci se Sdružením evropských regulačních orgánů v oblasti elektronických komunikací (dále jen „BEREC“), koordinované posouzení rizik, které má být prováděno podle článku 22 směrnice (EU) 2022/2555, a testování digitální provozní odolnosti podle nařízení Evropského parlamentu a Rady (EU) 2022/***2554[1]***. Výběr odvětví by měl rovněž zohlednit doporučení Rady o celounijním koordinovaném přístupu za účelem posílení odolnosti kritické infrastruktury.

[1] Nařízení Evropského parlamentu a Rady (EU) 2022/2554 ze dne 14. prosince 2022 o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014, (EU) č. 909/2014 a (EU) 2016/1011.

---

[29] Nařízení Evropského parlamentu a Rady (EU) 2022/2554 ze dne 14. prosince 2022 o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014, (EU) č. 909/2014 a (EU) 2016/1011.

[29] Nařízení Evropského parlamentu a Rady (EU) 2022/2554 ze dne 14. prosince 2022 o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014, (EU) č. 909/2014 a (EU) 2016/1011.

Pozměňovací návrh 22

Návrh nařízení
Bod odůvodnění 32

Znění navržené Komisí	*Pozměňovací návrh*
(32) Mechanismus pro mimořádné události v kybernetické oblasti by měl podporovat pomoc poskytovanou členskými státy členskému státu, který je postižen významným nebo rozsáhlým kybernetickým bezpečnostním incidentem, a to i prostřednictvím sítě CSIRT podle článku 15 směrnice (EU) 2022/2555. Členské státy poskytující pomoc by měly mít možnost předkládat žádosti o úhradu nákladů spojených s vysláním týmů odborníků v rámci vzájemné pomoci. Způsobilé náklady mohou zahrnovat cestovní výdaje, výdaje na ubytování a denní příspěvky pro odborníky na kybernetickou bezpečnost.	(32) Mechanismus pro mimořádné události v kybernetické oblasti by měl podporovat pomoc poskytovanou členskými státy členskému státu, který je postižen významným nebo rozsáhlým kybernetickým bezpečnostním incidentem, a to i prostřednictvím sítě CSIRT podle článku 15 směrnice (EU) 2022/2555. Členské státy poskytující pomoc by měly mít možnost předkládat žádosti o úhradu nákladů spojených s vysláním týmů odborníků v rámci vzájemné pomoci***, což by mělo zajistit účinnou koordinaci mezi příslušnými programy a nástroji EU, včetně Evropského mírového nástroje, SZBP a nástroje NDICI, při poskytování pomoci třetím zemím, zejména Ukrajině a Moldavsku***. Způsobilé náklady mohou zahrnovat cestovní výdaje, výdaje na ubytování a denní příspěvky pro odborníky na kybernetickou bezpečnost.

Pozměňovací návrh 23

Návrh nařízení
Bod odůvodnění 33

Znění navržené Komisí	*Pozměňovací návrh*
(33) Postupně by měla být zřízena rezerva pro kybernetickou bezpečnost na úrovni Unie, která by se skládala ze služeb soukromých poskytovatelů řízených bezpečnostních služeb na podporu reakce a okamžité obnovy v případě významných nebo rozsáhlých kybernetických bezpečnostních incidentů. Rezerva EU pro kybernetickou bezpečnost by měla zajistit dostupnost a připravenost služeb. Služby	(33) Postupně by měla být zřízena rezerva pro kybernetickou bezpečnost na úrovni Unie, která by se skládala ze služeb soukromých poskytovatelů řízených bezpečnostních služeb na podporu reakce a okamžité obnovy v případě významných nebo rozsáhlých kybernetických bezpečnostních incidentů. Rezerva EU pro kybernetickou bezpečnost by měla zajistit dostupnost a připravenost služeb. Služby

rezervy EU pro kybernetickou bezpečnost by měly sloužit jako podpora vnitrostátním orgánům při poskytování pomoci postiženým subjektům působícím v kritických nebo vysoce kritických odvětvích jako doplněk jejich vlastních opatření na vnitrostátní úrovni. Při žádosti o podporu z rezervy EU pro kybernetickou bezpečnost by členské státy měly upřesnit, jaká podpora byla dotčenému subjektu poskytnuta na vnitrostátní úrovni, a tato podpora by měla být zohledněna při posuzování žádosti členského státu. Služby rezervy EU pro kybernetickou bezpečnost mohou za podobných podmínek sloužit také na podporu orgánů, institucí nebo jiných subjektů Unie.	rezervy EU pro kybernetickou bezpečnost by měly sloužit jako podpora vnitrostátním orgánům při poskytování pomoci postiženým subjektům působícím v kritických nebo vysoce kritických odvětvích jako doplněk jejich vlastních opatření na vnitrostátní úrovni. Při žádosti o podporu z rezervy EU pro kybernetickou bezpečnost by členské státy měly upřesnit, jaká podpora byla dotčenému subjektu poskytnuta na vnitrostátní úrovni, a tato podpora by měla být zohledněna při posuzování žádosti členského státu. Služby rezervy EU pro kybernetickou bezpečnost mohou za podobných podmínek sloužit také na podporu orgánů, institucí nebo jiných subjektů Unie***, včetně misí SBOP***.

Pozměňovací návrh 24

Návrh nařízení
Bod odůvodnění 34

Znění navržené Komisí	*Pozměňovací návrh*
(34) Pro účely výběru soukromých poskytovatelů služeb, kteří budou poskytovat služby v rámci rezervy EU pro kybernetickou bezpečnost, je nezbytné stanovit soubor minimálních kritérií, která by měla být zahrnuta do výzvy k podávání nabídek za účelem výběru těchto poskytovatelů, aby bylo zajištěno naplnění potřeb orgánů členských států a subjektů působících v kritických nebo vysoce kritických odvětvích.	(34) Pro účely výběru soukromých poskytovatelů služeb, kteří budou poskytovat služby v rámci rezervy EU pro kybernetickou bezpečnost, je nezbytné stanovit soubor minimálních kritérií, která by měla být zahrnuta do výzvy k podávání nabídek za účelem výběru těchto poskytovatelů, aby bylo zajištěno naplnění potřeb orgánů členských států a subjektů působících v kritických nebo vysoce kritických odvětvích***, přičemž je rovněž nezbytné zohlednit rizika spojená s účastí poskytovatelů ze zemí konkurenčních ze strategického hlediska, neboť může způsobit hospodářská bezpečnostní rizika, jakož i důsledky pro strategickou bezpečnost Unie***.

Pozměňovací návrh 25

Návrh nařízení
Bod odůvodnění 36

Znění navržené Komisí	*Pozměňovací návrh*
(36) V zájmu podpory cílů tohoto nařízení, kterými jsou podpora sdíleného situačního povědomí, zvýšení odolnosti Unie a umožnění účinné reakce na významné a rozsáhlé kybernetické bezpečnostní incidenty, měly by mít síť EU-CyCLONe, síť CSIRT nebo Komise možnost požádat agenturu ENISA o přezkum a posouzení hrozeb, zranitelností a opatření ke zmírnění dopadů v souvislosti s konkrétním významným nebo rozsáhlým kybernetickým bezpečnostním incidentem. Po dokončení přezkumu a posouzení incidentu by agentura ENISA měla ve spolupráci s příslušnými zúčastněnými stranami, včetně zástupců soukromého sektoru, členských států, Komise a dalších příslušných orgánů, institucí a jiných subjektů EU, vypracovat zprávu o přezkumu incidentu. Pokud jde o soukromý sektor, agentura ENISA buduje cesty pro výměnu informací se specializovanými poskytovateli, včetně poskytovatelů řízených bezpečnostních řešení a prodejců, s cílem přispět k poslání agentury ENISA, kterým je dosáhnout vysoké společné úrovně kybernetické bezpečnosti v celé Unii. Na základě spolupráce se zúčastněnými stranami, včetně soukromého sektoru, by se zpráva o přezkumu konkrétních incidentů měla zaměřit na posouzení příčin, dopadů a zmírnění následků incidentu poté, co k němu došlo. Zvláštní pozornost by měla být věnována příspěvkům a zkušenostem sdíleným poskytovateli řízených bezpečnostních služeb, kteří splňují podmínky nejvyšší profesní bezúhonnosti, nestrannosti a požadované technické odbornosti dle požadavků tohoto nařízení. Zpráva by měla být předložena síti EU-CyCLONe, síti CSIRT a Komisi a měla by	(36) V zájmu podpory cílů tohoto nařízení, kterými jsou podpora sdíleného situačního povědomí, zvýšení odolnosti Unie a umožnění účinné reakce na významné a rozsáhlé kybernetické bezpečnostní incidenty, měly by mít síť EU-CyCLONe, síť CSIRT nebo Komise možnost požádat agenturu ENISA o přezkum a posouzení hrozeb, zranitelností a opatření ke zmírnění dopadů v souvislosti s konkrétním významným nebo rozsáhlým kybernetickým bezpečnostním incidentem. ***S ohledem na rozvoj bezpečného systému propojení vycházejícího z evropské kvantové komunikační infrastruktury (EuroQCI) a družicové komunikace Evropské unie v rámci státní správy (GOVSATCOM), zejména zavedení systému GALILEO GNSS pro uživatele obrany, by měl jakýkoli budoucí vývoj zohlednit nástup „hyperwaru“, který slučuje rychlost a sofistikovanost kvantové výpočetní techniky s vysoce autonomními vojenskými systémy, které mají schopnost devastovat společnost, a členské státy musí jako prioritu zajistit, aby byla upřednostněna ochrana celé elektronické komunikační sítě, jako jsou vzdušné, pozemní a podmořské systémy.*** Po dokončení přezkumu a posouzení incidentu by agentura ENISA měla ve spolupráci s příslušnými zúčastněnými stranami, včetně zástupců soukromého sektoru, členských států, Komise a dalších příslušných orgánů, institucí a jiných subjektů EU, vypracovat zprávu o přezkumu incidentu. Pokud jde o soukromý sektor, agentura ENISA buduje cesty pro výměnu informací se specializovanými poskytovateli, včetně poskytovatelů řízených bezpečnostních řešení a prodejců, s cílem přispět k poslání

být využita při jejich činnosti. Pokud se incident týká třetí země, předá Komise zprávu také vysokému představiteli.

agentury ENISA, kterým je dosáhnout vysoké společné úrovně kybernetické bezpečnosti v celé Unii. Na základě spolupráce se zúčastněnými stranami, včetně soukromého sektoru, by se zpráva o přezkumu konkrétních incidentů měla zaměřit na posouzení příčin, dopadů a zmírnění následků incidentu poté, co k němu došlo. Zvláštní pozornost by měla být věnována příspěvkům a zkušenostem sdíleným poskytovateli řízených bezpečnostních služeb, kteří splňují podmínky nejvyšší profesní bezúhonnosti, nestrannosti a požadované technické odbornosti dle požadavků tohoto nařízení. Zpráva by měla být předložena síti EU-CyCLONe, síti CSIRT a Komisi a měla by být využita při jejich činnosti. Pokud se incident týká třetí země, předá Komise zprávu také vysokému představiteli***, ESVČ a všem misím SBOP v zemi, které se incident týká, prostřednictvím jejich velitelství***.

Pozměňovací návrh 26

Návrh nařízení
Bod odůvodnění 37

Znění navržené Komisí	*Pozměňovací návrh*
(37) S ohledem na nepředvídatelnou povahu kybernetických bezpečnostních útoků a skutečnost, že se často neomezují na určitou zeměpisnou oblast a představují vysoké riziko přelévání, přispívá posílení odolnosti sousedních zemí a jejich schopnosti účinně reagovat na významné a rozsáhlé kybernetické bezpečnostní incidenty k ochraně Unie jako celku. Třetí země přidružené k programu Digitální Evropa proto ***mohou*** být podpořeny z rezervy EU pro kybernetickou bezpečnost, ***je-li to stanoveno*** v ***příslušné dohodě o přidružení*** k ***programu Digitální Evropa***. Financování přidružených třetích zemí by mělo být Unií podporováno v rámci příslušných partnerství a nástrojů	(37) S ohledem na nepředvídatelnou povahu kybernetických bezpečnostních útoků a skutečnost, že se často neomezují na určitou zeměpisnou oblast a představují vysoké riziko přelévání, přispívá posílení odolnosti sousedních zemí***, zejména Ukrajiny a Moldavska,*** a jejich schopnosti účinně reagovat na významné a rozsáhlé kybernetické bezpečnostní incidenty k ochraně Unie jako celku. Třetí země přidružené k programu Digitální Evropa ***by*** proto ***měly*** být podpořeny z rezervy EU pro kybernetickou bezpečnost***. Podpora by se měla vztahovat i na třetí země***, ***v nichž je nasazena mise SBOP se zvláštním mandátem k posílení odolnosti vůči hybridním hrozbám, včetně***

financování pro tyto země. Podpora by měla zahrnovat služby v oblasti reakce na významné nebo rozsáhlé kybernetické bezpečnostní incidenty a okamžité obnovy po těchto incidentech. Při poskytování podpory třetím zemím přidruženým k programu Digitální Evropa by měly platit podmínky stanovené v tomto nařízení pro rezervu EU pro kybernetickou bezpečnost a důvěryhodné poskytovatele.	***kybernetických hrozeb, nebo v nichž bylo přijato opatření pomoci*** v ***rámci Evropského mírového nástroje*** k ***posílení kybernetické odolnosti země***. Financování přidružených třetích zemí by mělo být Unií podporováno v rámci příslušných partnerství a nástrojů financování pro tyto země. Podpora by měla zahrnovat služby v oblasti reakce na významné nebo rozsáhlé kybernetické bezpečnostní incidenty a okamžité obnovy po těchto incidentech. Při poskytování podpory třetím zemím přidruženým k programu Digitální Evropa by měly platit podmínky stanovené v tomto nařízení pro rezervu EU pro kybernetickou bezpečnost a důvěryhodné poskytovatele.

Pozměňovací návrh 27

Návrh nařízení
Čl. 1 – odst. 1 – písm. c

Znění navržené Komisí	*Pozměňovací návrh*
c) zřízení evropského mechanismu pro kybernetické bezpečnostní incidenty, který bude přezkoumávat a posuzovat významné nebo rozsáhlé incidenty.	c) zřízení evropského mechanismu pro kybernetické bezpečnostní incidenty, který bude přezkoumávat a posuzovat významné nebo rozsáhlé incidenty ***či hrozby***.

Pozměňovací návrh 28

Návrh nařízení
Čl. 1 – odst. 2 – písm. a

Znění navržené Komisí	*Pozměňovací návrh*
a) posílit společné odhalování kybernetických hrozeb a incidentů v Unii a situační povědomí v této oblasti, což umožní posílit konkurenceschopnost odvětví průmyslu a služeb v Unii v celé digitální ekonomice a přispět k technologické ***suverenitě*** Unie v oblasti kybernetické bezpečnosti;	a) posílit společné odhalování kybernetických hrozeb a incidentů v Unii a situační povědomí v této oblasti, což umožní posílit konkurenceschopnost odvětví průmyslu a služeb v Unii v celé digitální ekonomice a přispět k technologické ***odolnosti*** Unie v oblasti kybernetické bezpečnosti;

Pozměňovací návrh 29

Návrh nařízení
Čl. 1 – odst. 2 – písm. b

Znění navržené Komisí	*Pozměňovací návrh*
b) posílit připravenost působících v kritických a vysoce kritických odvětvích v celé Unii a upevnit solidaritu vytvořením společných kapacit pro reakci na významné nebo rozsáhlé kybernetické bezpečnostní incidenty, včetně zpřístupnění podpory Unie při reakci na kybernetické bezpečnostní incidenty třetím zemím přidruženým k programu Digitální Evropa;	b) posílit připravenost působících v kritických a vysoce kritických odvětvích v celé Unii a upevnit solidaritu vytvořením společných kapacit pro reakci na významné nebo rozsáhlé kybernetické bezpečnostní incidenty, včetně zpřístupnění podpory Unie při reakci na kybernetické bezpečnostní incidenty třetím zemím přidruženým k programu Digitální Evropa ***nebo třetím zemím, které jsou kandidáty na přistoupení k Unii a nejsou v rozporu s bezpečnostními a obrannými zájmy Unie a jejích členských států stanovenými v rámci SZBP podle hlavy V Smlouvy o EU; Členské státy by měly považovat aktivní program kybernetické obrany za součást své vnitrostátní strategie kybernetické bezpečnosti, která zahrnuje pravidelná společná cvičení odborné přípravy mezi členskými státy a napříč mezinárodními organizacemi. Takovýto program by měl zajišťovat synchronizovanou kapacitu pro zjišťování, odhalování, analýzu a zmírňování hrozeb v reálném čase***;

Pozměňovací návrh 30

Návrh nařízení
Čl. 1 – odst. 2 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	2a. snížit systémová kybernetická rizika spojená se závislostí na kritickém vybavení ze zemí, které by byly v rozporu s bezpečnostními a obrannými zájmy Unie a jejích členských států, jak je stanoveno v rámci SZBP podle hlavy V Smlouvy o EU;

Pozměňovací návrh 31

Návrh nařízení
Čl. 2 – odst. 2 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	„komunitou kybernetické obrany“ orgány členských států v oblasti obrany s podporou orgánů, institucí a jiných subjektů EU, jak je uvedeno ve společném sdělení Politika kybernetické obrany EU[1]
	[1] Společné sdělení Evropskému parlamentu a Radě, Politika kybernetické obrany EU, JOIN/2022/49 final

Pozměňovací návrh 32

Návrh nařízení
Čl. 3 – odst. 2 – pododstavec 1 – písm. b a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	ba) pomoci modernizovat celé systémy kybernetické obrany, zvýšit kvalitu schopností kybernetické obrany zaváděním systémů UI a urychlit výměnu informací mezi národními bezpečnostními operačními středisky a přeshraničními bezpečnostními operačními středisky;

Pozměňovací návrh 33

Návrh nařízení
Čl. 3 – odst. 2 – pododstavec 1 – písm. d a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	da) provádět přezkum a hodnocení kritických technologií a zařízení v oblasti kybernetické bezpečnosti používaných bezpečnostními operačními středisky v reakci na kybernetické bezpečnostní incidenty u systémových rizik vyplývajících z kontroly vysoce rizikových

	poskytovatelů ze strany zemí, které by byly v rozporu s bezpečnostními a obrannými zájmy Unie a jejích členských států, jak je stanoveno v rámci SZBP podle hlavy V Smlouvy o EU.

Pozměňovací návrh 34

Návrh nařízení
Čl. 4 – odst. 1 – pododstavec 2

Znění navržené Komisí	*Pozměňovací návrh*
Má kapacitu působit jako referenční bod a brána pro další veřejné a soukromé organizace na vnitrostátní úrovni, které shromažďují a analyzují informace o kybernetických bezpečnostních hrozbách a incidentech a přispívají k přeshraničnímu bezpečnostnímu operačnímu středisku. Je vybaveno nejmodernějšími technologiemi schopnými zjišťovat, agregovat a analyzovat údaje týkající se kybernetických bezpečnostních hrozeb a incidentů.	Má kapacitu působit jako referenční bod a brána pro další veřejné a soukromé organizace na vnitrostátní úrovni, ***a případně vojenské subjekty,*** které shromažďují a analyzují informace o kybernetických bezpečnostních hrozbách a incidentech a přispívají k přeshraničnímu bezpečnostnímu operačnímu středisku. Je vybaveno nejmodernějšími technologiemi schopnými zjišťovat, agregovat a analyzovat údaje týkající se kybernetických bezpečnostních hrozeb a incidentů.

Pozměňovací návrh 35

Návrh nařízení
Čl. 4 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
2. Na základě výzvy k vyjádření zájmu vybere Evropské centrum kompetencí pro kybernetickou bezpečnost (dále jen „ECCC“) národní bezpečnostní operační střediska, která se budou podílet na společném zadávání zakázek týkajících se nástrojů a infrastruktury s centrem ECCC. Centrum ECCC může vybraným národním bezpečnostním operačním střediskům udělit granty na financování provozu těchto nástrojů a infrastruktur. Finanční příspěvek Unie pokrývá až 50 % nákladů na pořízení nástrojů a	2. Na základě výzvy k vyjádření zájmu vybere Evropské centrum kompetencí pro kybernetickou bezpečnost (dále jen „ECCC“) národní bezpečnostní operační střediska, která se budou podílet na společném zadávání zakázek týkajících se nástrojů a infrastruktury s centrem ECCC. Centrum ECCC může vybraným národním bezpečnostním operačním střediskům udělit granty na financování provozu těchto nástrojů a infrastruktur ***za přísné podmínky, že tyto nástroje a infrastruktura jsou poskytovány***

infrastruktury a až 50 % nákladů na provoz, přičemž zbývající náklady hradí členský stát. Před zahájením řízení za účelem pořízení nástrojů a infrastruktur uzavřou centrum ECCC a národní bezpečnostní operační středisko dohodu o hostingu a užívání, která upravuje používání nástrojů a infrastruktur.	***důvěryhodnými poskytovateli v souladu s článkem 16***. Finanční příspěvek Unie pokrývá až 50 % nákladů na pořízení nástrojů a infrastruktury a až 50 % nákladů na provoz, přičemž zbývající náklady hradí členský stát. Před zahájením řízení za účelem pořízení nástrojů a infrastruktur uzavřou centrum ECCC a národní bezpečnostní operační středisko dohodu o hostingu a užívání, která upravuje používání nástrojů a infrastruktur.

Pozměňovací návrh 36

Návrh nařízení
Čl. 5 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
2. Na základě výzvy k vyjádření zájmu vybere centrum ECCC hostitelské konsorcium, které se bude podílet na společném zadávání zakázek týkajících se nástrojů a infrastruktury s centrem ECCC. Centrum ECCC může hostitelskému konsorciu udělit grant na financování provozu těchto nástrojů a infrastruktur. Finanční příspěvek Unie pokrývá až 75 % nákladů na pořízení nástrojů a infrastruktury a až 50 % nákladů na provoz, přičemž zbývající náklady hradí hostitelské konsorcium. Před zahájením řízení za účelem pořízení nástrojů a infrastruktur uzavřou centrum ECCC a hostitelské konsorcium dohodu o hostingu a užívání, která upravuje používání nástrojů a infrastruktur.	2. Na základě výzvy k vyjádření zájmu vybere centrum ECCC hostitelské konsorcium, které se bude podílet na společném zadávání zakázek týkajících se nástrojů a infrastruktury s centrem ECCC. Centrum ECCC může hostitelskému konsorciu udělit grant na financování provozu těchto nástrojů a infrastruktur ***za přísné podmínky, že tyto nástroje a infrastruktura jsou poskytovány důvěryhodnými poskytovateli v souladu s článkem 16***. Finanční příspěvek Unie pokrývá až 75 % nákladů na pořízení nástrojů a infrastruktury a až 50 % nákladů na provoz, přičemž zbývající náklady hradí hostitelské konsorcium. Před zahájením řízení za účelem pořízení nástrojů a infrastruktur uzavřou centrum ECCC a hostitelské konsorcium dohodu o hostingu a užívání, která upravuje používání nástrojů a infrastruktur.

Pozměňovací návrh 37

Návrh nařízení
Čl. 5 – odst. 2 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	2a. Každá infrastruktura nebo poskytovatel pocházející z vysoce rizikové třetí země jsou automaticky vyloučeny.

Pozměňovací návrh 38

Návrh nařízení
Čl. 6 – odst. 1 – písm. b a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	ba) přímo podporuje posílení vojenských a obranných schopností zúčastněných členů nebo brání přímému a bezprostřednímu ohrožení jejich bezpečnosti. Vzhledem k tomu, že využití zranitelných míst v odvětví obrany může způsobit závažné narušení a škodu, vyžaduje kybernetická bezpečnost v obranném průmyslu zvláštní opatření k zajištění bezpečnosti dodavatelských řetězců, zejména pokud jde o subjekty, které jsou v dodavatelském řetězci na nižším místě a nevyžadují přístup k utajovaným informacím, ale mohly by představovat závažné riziko pro celé odvětví. Zvláštní pozornost by měla být věnována dopadu, který by jakékoli porušení mohlo mít, a hrozbě jakékoli potenciální manipulace se síťovými daty, která by mohla vést k tomu, že by kritické obranné prostředky byly zbytečné nebo by dokonce převažovaly nad příslušnými operačními systémy, což by je činilo zranitelnými vůči "únosu".

Pozměňovací návrh 39

Návrh nařízení
Čl. 6 – odst. 1 – písm. b a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	bb) podporuje posílení obranných schopností zúčastněných členů nebo

	předchází přímému a bezprostřednímu ohrožení jejich bezpečnosti, přičemž zajišťuje bezpečnost dodavatelských řetězců, zejména pokud jde o subjekty, které jsou v dodavatelském řetězci na nižším místě a nevyžadují přístup k utajovaným informacím, ale mohly by představovat závažné riziko pro celé odvětví.

Pozměňovací návrh 40

Návrh nařízení
Čl. 7 – odst. 1

Znění navržené Komisí	*Pozměňovací návrh*
1. Pokud přeshraniční bezpečnostní operační střediska získají informace týkající se potenciálního nebo probíhajícího rozsáhlého kybernetického bezpečnostního incidentu, poskytnou neprodleně příslušné informace síti EU-CyCLONe, síti CSIRT a Komisi s ohledem na jejich příslušné úlohy v oblasti řešení krizí v souladu se směrnicí (EU) 2022/2555.	1. Pokud přeshraniční bezpečnostní operační střediska získají informace týkající se potenciálního nebo probíhajícího rozsáhlého kybernetického bezpečnostního incidentu, poskytnou neprodleně příslušné informace síti EU-CyCLONe, síti CSIRT a Komisi***, mimo jiné vysokému představiteli a ESVČ v případě, že jde o třetí zemi,*** s ohledem na jejich příslušné úlohy v oblasti řešení krizí v souladu se směrnicí (EU) 2022/2555.

Pozměňovací návrh 41

Návrh nařízení
Čl. 8 – odst. 1

Znění navržené Komisí	*Pozměňovací návrh*
1. Členské státy, které se účastní evropského kybernetického štítu, zajistí vysokou úroveň bezpečnosti údajů a fyzické bezpečnosti infrastruktury evropského kybernetického štítu a zabezpečí, aby byla infrastruktura přiměřeně spravována a kontrolována tak, aby byla chráněna před hrozbami a aby byla zajištěna její bezpečnost a bezpečnost systémů, včetně bezpečnosti údajů vyměňovaných prostřednictvím této	1. Členské státy, které se účastní evropského kybernetického štítu, zajistí vysokou úroveň bezpečnosti údajů a fyzické bezpečnosti infrastruktury evropského kybernetického štítu a zabezpečí, aby byla infrastruktura přiměřeně spravována a kontrolována tak, aby byla chráněna před hrozbami a aby byla zajištěna její bezpečnost a bezpečnost systémů, ***jakož i snížení rizik a podpora technologického náskoku EU v kritických***

infrastruktury.	***odvětvích,*** včetně ***opatření k omezení či vyloučení vysoce rizikových dodavatelů a rovněž k ochraně*** bezpečnosti údajů vyměňovaných prostřednictvím této infrastruktury.

Pozměňovací návrh 42

Návrh nařízení
Čl. 8 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
2. Členské státy, které se účastní evropského kybernetického štítu, zajistí, aby sdílení informací v rámci evropského kybernetického štítu se subjekty, které nejsou veřejnoprávními subjekty členského státu, nemělo negativní dopad na bezpečnostní zájmy Unie.	2. Členské státy, které se účastní evropského kybernetického štítu, zajistí, aby sdílení informací v rámci evropského kybernetického štítu se subjekty, které nejsou veřejnoprávními subjekty členského státu, nemělo negativní dopad na bezpečnostní zájmy Unie ***a aby jakékoli sdílení informací s vysoce rizikovými poskytovateli bylo svým rozsahem omezeno a nebyla jím dotčena bezpečnost a strategické zájmy Unie***.

Pozměňovací návrh 43

Návrh nařízení
Čl. 8 – odst. 3

Znění navržené Komisí	*Pozměňovací návrh*
3. Komise může přijmout prováděcí akty, kterými stanoví technické požadavky na členské státy při plnění jejich povinností podle odstavců 1 a 2. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 21 odst. 2 tohoto nařízení. Komise přitom za podpory vysokého představitele zohlední příslušné normy zabezpečení na úrovni obrany, aby usnadnila spolupráci s vojenskými subjekty.	3. Komise může přijmout prováděcí akty, kterými stanoví technické požadavky na členské státy při plnění jejich povinností podle odstavců 1 a 2. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 21 odst. 2 tohoto nařízení. Komise přitom za podpory vysokého představitele zohlední příslušné normy zabezpečení na úrovni obrany, aby usnadnila spolupráci s vojenskými subjekty***, přičemž vhodným způsobem využívá celé řady možností obrany dostupných civilním a vojenským komunitám v zájmu širší bezpečnosti a obrany EU a informuje Evropský***

parlament.

Pozměňovací návrh 44

Návrh nařízení
Čl. 9 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
2. Akce, kterými se provádí mechanismus pro mimořádné události v kybernetické oblasti, jsou podporovány z finančních prostředků programu Digitální Evropa a prováděny v souladu s nařízením (EU) 2021/694, a zejména s jeho specifickým cílem č. 3**.**	2. Akce, kterými se provádí mechanismus pro mimořádné události v kybernetické oblasti, jsou podporovány z finančních prostředků programu Digitální Evropa a prováděny v souladu s nařízením (EU) 2021/694, a zejména s jeho specifickým cílem č. 3***, a dále jsou podporovány Evropským mírovým nástrojem při zajišťování opatření pomoci třetím zemím, zejména Ukrajině a Moldavsku;***

Pozměňovací návrh 45

Návrh nařízení
Čl. 10 – odst. 1 – písm. a

Znění navržené Komisí	*Pozměňovací návrh*
a) opatření v oblasti připravenosti, včetně koordinovaného testování připravenosti subjektů působících ve vysoce kritických odvětvích v celé Unii;	a) opatření v oblasti připravenosti, včetně koordinovaného testování připravenosti subjektů působících ve vysoce kritických odvětvích***, jako je veřejná infrastruktura, volební infrastruktura, doprava, finanční, telekomunikační, zdravotní péče, dodávky potravin a bezpečnost*** v celé Unii;

Pozměňovací návrh 46

Návrh nařízení
Čl. 10 – odst. 1 – písm. c

Znění navržené Komisí	*Pozměňovací návrh*
c) opatření vzájemné pomoci spočívající v poskytování pomoci	c) opatření vzájemné pomoci spočívající v poskytování pomoci

vnitrostátními orgány jednoho členského státu jinému členskému státu, zejména podle čl. 11 odst. 3 písm. f) směrnice (EU) 2022/2555.	vnitrostátními orgány jednoho členského státu jinému členskému státu, zejména podle čl. 11 odst. 3 písm. f) směrnice (EU) 2022/2555 ***a v kontextu čl. 42 odst. 7 SEU a článku 222 SFEU;***

Pozměňovací návrh 47

Návrh nařízení
Čl. 10 – odst. 1 – písm. c a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	ca) nahrazení a postupné vyřazení kritického zařízení od vysoce rizikových dodavatelů, kteří by byli v rozporu s bezpečnostními a obrannými zájmy Unie a jejích členských států, jak je stanoveno v rámci SZBP podle hlavy V Smlouvy o EU.

Pozměňovací návrh 48

Návrh nařízení
Čl. 11 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
2. Skupina pro spolupráci v oblasti bezpečnosti sítí a informací ve spolupráci s Komisí, agenturou ENISA ***a*** vysokým představitelem vypracuje společné rizikové scénáře a metodiky pro koordinované testování.	2. Skupina pro spolupráci v oblasti bezpečnosti sítí a informací ve spolupráci s Komisí, agenturou ENISA***,*** vysokým představitelem***, ESVČ a případně Evropskou obrannou agenturou*** vypracuje společné rizikové scénáře a metodiky pro koordinované testování.

Pozměňovací návrh 49

Návrh nařízení
Čl. 12 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
2. Rezerva EU pro kybernetickou bezpečnost se skládá ze služeb reakce na incidenty od důvěryhodných poskytovatelů vybraných v souladu s kritérii stanovenými	2. Rezerva EU pro kybernetickou bezpečnost se skládá ze služeb reakce na incidenty od důvěryhodných poskytovatelů vybraných v souladu s kritérii stanovenými

v článku 16. Rezerva zahrnuje předem přislíbené služby. Služby musí být možné provádět ve všech členských státech.	v článku 16. Rezerva zahrnuje předem přislíbené služby. Služby musí být možné provádět ve všech členských státech ***a třetích zemích, které splňují příslušné požadavky tohoto nařízení***.

Pozměňovací návrh 50

Návrh nařízení
Čl. 12 – odst. 3 – písm. b

Znění navržené Komisí	*Pozměňovací návrh*
b) orgány, instituce nebo jiné subjekty Unie.	b) orgány, instituce nebo jiné subjekty Unie***, včetně misí SBOP***.

Pozměňovací návrh 51

Návrh nařízení
Čl. 12 – odst. 4

Znění navržené Komisí	*Pozměňovací návrh*
4. Uživatelé uvedení v odst. 3 písm. a) využívají služby rezervy EU pro kybernetickou bezpečnost k reakci nebo k podpoře reakce na významné nebo rozsáhlé incidenty, které postihují subjekty působící v kritických nebo vysoce kritických odvětvích, a k okamžité obnově po těchto incidentech.	4. Uživatelé uvedení v odst. 3 písm. a) využívají služby rezervy EU pro kybernetickou bezpečnost k reakci nebo k podpoře reakce na významné nebo rozsáhlé incidenty, které postihují subjekty působící v kritických nebo vysoce kritických odvětvích, ***jako je veřejná infrastruktura, volební infrastruktura, doprava, zdravotnictví, finance, telekomunikace, dodávky potravin a bezpečnost,*** a k okamžité obnově po těchto incidentech.

Pozměňovací návrh 52

Návrh nařízení
Čl. 12 – odst. 5

Znění navržené Komisí	*Pozměňovací návrh*
5. Komise nese celkovou odpovědnost za provádění rezervy EU pro kybernetickou bezpečnost. Komise určí priority a vývoj rezervy EU pro	5. Komise nese celkovou odpovědnost za provádění rezervy EU pro kybernetickou bezpečnost. Komise určí priority a vývoj rezervy EU pro

kybernetickou bezpečnost v souladu s požadavky uživatelů uvedenými v odstavci 3, dohlíží na její provádění a zajišťuje doplňkovost, jednotnost, synergie a vazby s dalšími podpůrnými opatřeními podle tohoto nařízení i s jinými opatřeními a programy Unie.	kybernetickou bezpečnost v souladu s požadavky uživatelů uvedenými v odstavci 3, dohlíží na její provádění a zajišťuje doplňkovost, jednotnost, synergie a vazby s dalšími podpůrnými opatřeními podle tohoto nařízení i s jinými opatřeními a programy ***a cíli*** Unie***, zejména se strategickým cílem snížit závislosti na vysoce rizikových dodavatelích, kteří by byli v rozporu s bezpečnostními a obrannými zájmy Unie a jejích členských států, jak je stanoveno v rámci SZBP podle hlavy V Smlouvy o EU***.

Pozměňovací návrh 53

Návrh nařízení
Čl. 12 – odst. 7

Znění navržené Komisí	*Pozměňovací návrh*
7. S cílem podpořit Komisi při zřizování rezervy EU pro kybernetickou bezpečnost vypracuje agentura ENISA po konzultaci s členskými státy a Komisí mapování potřebných služeb. Agentura ENISA po konzultaci s Komisí připraví podobné mapování, aby určila potřeby třetích zemí způsobilých pro podporu z rezervy EU pro kybernetickou bezpečnost podle článku 17. Komise dle potřeby konzultuje s vysokým představitelem.	7. S cílem podpořit Komisi při zřizování rezervy EU pro kybernetickou bezpečnost vypracuje agentura ENISA po konzultaci s členskými státy a Komisí mapování potřebných služeb. Agentura ENISA po konzultaci s Komisí připraví podobné mapování, aby ***s podporou ESVČ*** určila potřeby třetích zemí způsobilých pro podporu z rezervy EU pro kybernetickou bezpečnost podle článku 17. Komise dle potřeby konzultuje s vysokým představitelem.

Pozměňovací návrh 54

Návrh nařízení
Čl. 14 – odst. 2 – písm. a a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	aa) dopad incidentu na bezpečnost a obranu Unie;

Pozměňovací návrh 55

Návrh nařízení
Čl. 15 – odst. 3

Znění navržené Komisí	*Pozměňovací návrh*
3. Po konzultaci s vysokým představitelem může podpora v rámci mechanismu pro mimořádné události v kybernetické oblasti doplňovat pomoc poskytovanou v rámci společné zahraniční a bezpečnostní politiky a společné bezpečnostní a obranné politiky, a to i prostřednictvím týmů rychlé kybernetické reakce. Může rovněž doplňovat pomoc poskytovanou jedním členským státem jinému členskému státu na základě čl. 42 odst. 7 Smlouvy o Evropské unii nebo k této pomoci přispívat.	3. Po konzultaci s vysokým představitelem může podpora v rámci mechanismu pro mimořádné události v kybernetické oblasti doplňovat pomoc poskytovanou v rámci společné zahraniční a bezpečnostní politiky a společné bezpečnostní a obranné politiky, a to i prostřednictvím týmů rychlé kybernetické reakce ***(CRRT), s cílem lépe podpořit členské státy EU, mise a operace SBOP a třetí země, které dosáhly souladu se společnou zahraniční a bezpečnostní politikou a společnou bezpečnostní a obrannou politikou EU, v jejich úsilí o budování kapacit kybernetické obrany, zejména Ukrajinu a Moldavsko***. Může rovněž doplňovat pomoc poskytovanou jedním členským státem jinému členskému státu na základě čl. 42 odst. 7 Smlouvy o Evropské unii nebo k této pomoci přispívat.

Pozměňovací návrh 56

Návrh nařízení
Čl. 16 – odst. 2 – písm. a a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	aa) poskytovatel prokáže, že jeho rozhodovací a řídící struktury nepodléhají jakémukoli nepatřičnému ovlivňování ze strany vlád států, které by byly v rozporu s bezpečnostními a obrannými zájmy Unie a jejích členských států, jak je stanoveno v rámci SZBP podle hlavy V SEU;

Pozměňovací návrh 57

Návrh nařízení
Čl. 16 – odst. 2 – písm. f

Znění navržené Komisí	*Pozměňovací návrh*
f) poskytovatel je vybaven hardwarovým a softwarovým technickým zařízením nezbytným pro podporu požadované služby;	f) poskytovatel je vybaven hardwarovým a softwarovým technickým zařízením nezbytným pro podporu požadované služby ***a splňuje požadavky stanovené v článku X nařízení XX/XXXX (akt o kybernetické odolnosti)***;

Pozměňovací návrh 58

Návrh nařízení
Čl. 16 – odst. 2 – písm. j a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	ja) není přípustný žádný poskytovatel pocházející z vysoce rizikové třetí země.

Pozměňovací návrh 59

Návrh nařízení
Čl. 16 – odst. 2 – písm. j b (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	jb) poskytovatel pokud možno úzce spolupracuje s příslušnými malými a středními podniky;

Pozměňovací návrh 60

Návrh nařízení
Čl. 17 – odst. 1

Znění navržené Komisí	*Pozměňovací návrh*
1. Třetí země mohou požádat o podporu z rezervy EU pro kybernetickou bezpečnost, pokud ***to stanoví dohody o přidružení týkající se jejich účasti v***	1. Třetí země mohou požádat o podporu z rezervy EU pro kybernetickou bezpečnost, pokud***:***

programu Digitální Evropa.

a) to stanoví dohody o přidružení týkající se jejich účasti v programu Digitální Evropa;

b) třetí země, v nichž je nasazena mise SBOP se zvláštním mandátem k posílení odolnosti vůči hybridním hrozbám, včetně kybernetických hrozeb, nebo v nichž bylo přijato opatření pomoci v rámci Evropského mírového nástroje k posílení kybernetické odolnosti země.

Pozměňovací návrh 61

Návrh nařízení
Čl. 17 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
2. Podpora z rezervy EU pro kybernetickou bezpečnost musí být v souladu s tímto nařízením a musí splňovat veškeré zvláštní podmínky stanovené v dohodách o přidružení uvedených v odstavci 1.	2. Podpora z rezervy EU pro kybernetickou bezpečnost musí být v souladu s tímto nařízením a musí splňovat veškeré zvláštní podmínky stanovené v dohodách o přidružení uvedených v odstavci ***s výjimkou třetích zemí, na něž se vztahují ustanovení odst.*** 1 ***písm. b)***.

Pozměňovací návrh 62

Návrh nařízení
Čl. 18 – odst. 1

Znění navržené Komisí	*Pozměňovací návrh*
1. Na žádost Komise, sítě EU-CyCLONe nebo sítě CSIRT agentura ENISA přezkoumá a posoudí hrozby, zranitelná místa a opatření ke zmírnění dopadů v souvislosti s konkrétním významným nebo rozsáhlým kybernetickým bezpečnostním incidentem. Po dokončení přezkumu a posouzení incidentu předá agentura ENISA síti CSIRT, síti EU-CyCLONe a Komisi zprávu o přezkumu incidentu, aby je podpořila při plnění jejich úkolů, zejména s	1. Na žádost Komise, sítě EU-CyCLONe nebo sítě CSIRT agentura ENISA přezkoumá a posoudí hrozby, zranitelná místa a opatření ke zmírnění dopadů v souvislosti s konkrétním významným nebo rozsáhlým kybernetickým bezpečnostním incidentem. Po dokončení přezkumu a posouzení incidentu předá agentura ENISA síti CSIRT, síti EU-CyCLONe a Komisi zprávu o přezkumu incidentu, aby je podpořila při plnění jejich úkolů, zejména s

ohledem na úkoly stanovené v článcích 15 a 16 směrnice (EU) 2022/2555. V případě potřeby Komise sdílí zprávu s vysokým představitelem.	ohledem na úkoly stanovené v článcích 15 a 16 směrnice (EU) 2022/2555. V případě potřeby***, zejména pokud se incident týká třetí země,*** Komise sdílí zprávu s vysokým představitelem ***a ESVČ***.

Pozměňovací návrh 63

Návrh nařízení
Čl. 18 – odst. 3 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	3a. Zpráva se sdílí s Evropským parlamentem v souladu s právními předpisy Unie nebo vnitrostátními právními předpisy o ochraně citlivých utajovaných informací.

Pozměňovací návrh 64

Návrh nařízení
Čl. 19 – odst. 1 – bod 1 – písm. a – bod 1
Nařízení (EU) 2021/694
Čl. 6 – odst. 1

Znění navržené Komisí	*Pozměňovací návrh*
aa) podporovat rozvoj kybernetického štítu EU, včetně vývoje, zavádění a provozu národních a přeshraničních platforem bezpečnostních operačních středisek, které přispívají k situačnímu povědomí v Unii a k posílení zpravodajských kapacit Unie v oblasti kybernetických ***hrozeb“***;	aa) podporovat rozvoj kybernetického štítu EU, včetně vývoje, zavádění a provozu národních a přeshraničních platforem bezpečnostních operačních středisek, které přispívají k situačnímu povědomí v Unii a k posílení zpravodajských kapacit Unie v oblasti kybernetických ***hrozeb a ke snížení závislosti Unie na vysoce rizikových poskytovatelích kritického zařízení nebo součástí v oblasti kybernetické bezpečnosti, kteří by byli v rozporu s bezpečnostními a obrannými zájmy Unie a jejích členských států, jak je stanoveno v rámci SZBP podle hlavy V SEU***;

Pozměňovací návrh 65

Návrh nařízení
Čl. 20 – odst. 1

Znění navržené Komisí	*Pozměňovací návrh*
Do ***[čtyř*** let ode dne použitelnosti tohoto ***nařízení]*** předloží Komise Evropskému parlamentu a Radě zprávu o hodnocení a přezkumu tohoto nařízení.	Do ***[tří*** let ode dne použitelnosti tohoto ***nařízení a poté každé dva roky]*** předloží Komise Evropskému parlamentu a Radě zprávu o hodnocení a přezkumu tohoto nařízení.

POSTUP VE VÝBORU POŽÁDANÉM O STANOVISKO

Název	Stanovení opatření k posílení solidarity Unie a jejích kapacit v oblasti odhalování kybernetických bezpečnostních hrozeb a incidentů a přípravy a reakce na ně
Referenční údaje	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)
Příslušný výbor Datum oznámení na zasedání	ITRE 1.6.2023
Výbor, který vypracoval stanovisko Datum oznámení na zasedání	AFET 1.6.2023
Zpravodaj(ka) Datum jmenování	Dragoş Tudorache 16.6.2023
Projednání ve výboru	18.9.2023
Datum přijetí	24.10.2023
Výsledek konečného hlasování	+: 39 –: 4 0: 0
Členové přítomní při konečném hlasování	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 přítomní při konečném hlasování	Attila Ara-Kovács, Lars Patrick Berg, Andrey Kovatchev, Georgios Kyrtsos, Sergey Lagodinsky, Giuliano Pisapia, Mick Wallace

JMENOVITÉ KONEČNÉ HLASOVÁNÍ
VE VÝBORU POŽÁDANÉM 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

Význam zkratek:
+ : pro
- : proti
0 : zdrželi se