



---

## PŘIJATÉ TEXTY

---

### P10\_TA(2026)0303

#### **Hybridní válka a ochrana územní celistvosti EU a kritické bezpečnostní a obranné infrastruktury**

**Usnesení Evropského parlamentu ze dne 16. září 2026 o hybridní válce a ochraně územní celistvosti EU a kritické bezpečnostní a obranné infrastruktury (2026/2024(INI))**

*Evropský parlament,*

- s ohledem na Chartu OSN a základní zásady mezinárodního práva,
- s ohledem na hlavu V Smlouvy o Evropské unii (SEU), zejména na kapitolu 2 oddíl 2 o ustanoveních o společné bezpečnostní a obranné politice,
- s ohledem na Smlouvu o fungování Evropské unie (SFEU),
- s ohledem na čl. 42 odst. 7 a článek 222 SEU,
- s ohledem na svá předchozí usnesení o Ukrajině, Rusku a Bělorusku, zejména na usnesení přijatá po ruské anexi Krymského poloostrova v únoru 2014 a po plošné ruské invazi na Ukrajinu v únoru 2022,
- s ohledem na mezinárodní právní rámec pro předcházení terorismu a boj proti němu, včetně rezoluce Rady bezpečnosti OSN 2341 o ochraně kritické infrastruktury před teroristickými činy, která byla přijata dne 13. února 2017,
- s ohledem na nařízení Evropského parlamentu a Rady (EU) 2019/452 ze dne 19. března 2019, kterým se stanoví rámec pro prověřování přímých zahraničních investic směřujících do Unie<sup>1</sup>,
- s ohledem na dokument nazvaný „Strategický kompas pro bezpečnost a obranu – za Evropskou unii, která chrání své občany, hodnoty a zájmy a přispívá k mezinárodnímu míru a bezpečnosti“, který schválila Rada dne 21. března 2022 a potvrdila Evropská rada

---

<sup>1</sup> Úř. věst. L 79 I, 21.3.2019, s. 1, ELI:  
<http://data.europa.eu/eli/reg/2019/452/oj>.

dne 25. března 2022,

- s ohledem na závěry Rady ze dne 21. června 2022 o rámci pro koordinovanou reakci EU na hybridní kampaně,
- s ohledem na směrnici Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022 o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES<sup>2</sup>,
- s ohledem na závěrečnou hodnotící zprávu pracovní skupiny EU-NATO pro odolnost kritické infrastruktury ze dne 29. června 2023,
- s ohledem na zprávu ze dne 30. října 2024, kterou vypracoval Sauli Niinistö pod názvem „Společně bezpečnější – posílení civilní a vojenské pohotovosti a připravenosti Evropy“ (Niinistöva zpráva),
- s ohledem na sdělení Komise ze dne 11. prosince 2024 o boji proti hybridním hrozbám vyplývajícím ze zneužívání migrace jako zbraně a o posílení bezpečnosti na vnějších hranicích EU (COM(2024)0570),
- s ohledem na nařízení Evropského parlamentu a Rady (EU) 2025/37 ze dne 19. prosince 2024, kterým se mění nařízení (EU) 2019/881, pokud jde o řízené bezpečnostní služby<sup>3</sup>,
- s ohledem na nařízení Evropského parlamentu a Rady (EU) 2025/38 ze dne 19. prosince 2024, kterým se stanovují opatření k posílení solidarity a kapacit v Unii pro odhalování kybernetických hrozeb a incidentů a pro připravenost a reakci na ně a mění nařízení (EU) 2021/694 (nařízení o kybernetické solidaritě)<sup>4</sup>,
- s ohledem na společné sdělení Komise a vysoké představitelky Unie pro zahraniční věci a bezpečnostní politiku ze dne 21. února 2025 s názvem „Akční plán EU o bezpečnosti kabelů“ (JOIN(2025)0009),
- s ohledem na své usnesení ze dne 12. března 2025 o bílé knize o budoucnosti evropské obrany<sup>5</sup>,
- s ohledem na společnou bílou knihu Komise a vysoké představitelky Unie pro zahraniční věci a bezpečnostní politiku ze dne 19. března 2025 nazvané „Společná bílá kniha o budoucnosti evropské obrany 2030“ (JOIN(2025)0120),
- s ohledem na společné sdělení Komise a vysoké představitelky Unie

---

<sup>2</sup> Úř. věst. L 333, 27.12.2022, s. 164, ELI:  
<http://data.europa.eu/eli/dir/2022/2557/oj>.

<sup>3</sup> Úř. věst. L, 2025/37, 15.1.2025, ELI:  
<http://data.europa.eu/eli/reg/2025/37/oj>.

<sup>4</sup> Úř. věst. L, 2025/38, 15.1.2025, ELI:  
<http://data.europa.eu/eli/reg/2025/38/oj>.

<sup>5</sup> Úř. věst. C, C/2025/3151, 20.6.2025, ELI:  
<http://data.europa.eu/eli/C/2025/3151/oj>.

pro zahraniční věci a bezpečnostní politiku ze dne 26. března 2025 o Strategii unie připravenosti (JOIN(2025)0130),

- s ohledem na sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů ze dne 1. dubna 2025 nazvané ProtectEU: Evropská strategie vnitřní bezpečnosti (COM(2025)0148),
- s ohledem na prohlášení ze summitu Severoatlantické rady v Haagu, které přijaly hlavy států a předsedové vlád účastníci se zasedání Severoatlantické rady dne 25. června 2025,
- s ohledem na své usnesení ze dne 9. října 2025 o společné reakci na nedávné narušení vzdušného prostoru a kritické infrastruktury členských států EU Ruskem<sup>6</sup>,
- s ohledem na neoficiální dokument italského ministra obrany z listopadu 2025 nazvaný „Boj proti hybridní válce: aktivní strategie“,
- s ohledem na návrh hlavních směrů pro transevropské energetické sítě, který předložila Komise dne 10. prosince 2025 (COM/2025/1006),
- s ohledem na své usnesení ze dne 18. prosince 2025 o pokračujících běloruských hybridních útocích proti Litvě<sup>7</sup>,
- s ohledem na sdělení Komise ze dne 18. února 2026 o východních regionech EU sousedících s Ruskem, Běloruskem a Ukrajinou (COM(2026)0082),
- s ohledem na své usnesení ze dne 21. ledna 2026 o provádění společné bezpečnostní a obranné politiky – výroční zpráva za rok 2025<sup>8</sup>,
- s ohledem na závěry Rady ze dne 16. března 2026 o posílení schopnosti EU bojovat proti hybridním hrozbám,
- s ohledem na článek 55 jednacího řádu,
- s ohledem na zprávu Výboru pro bezpečnost a obranu (A10-0212/2026),
- s ohledem na prohlášení ze summitu Severoatlantické rady, které přijaly hlavy států a předsedové vlád účastníci se zasedání Severoatlantické rady dne 8. července 2026 v Ankaře,

---

<sup>6</sup> Úř. věst. C, C/2026/1530, 15.4.2026, ELI: <http://data.europa.eu/eli/C/2026/1530/oj>.

<sup>7</sup> Úř. věst. C, C/2026/2161, 6.5.2026, ELI: <http://data.europa.eu/eli/C/2026/2161/oj>.

<sup>8</sup> Přijaté texty, P10\_TA(2026)0013.

- A. vzhledem k tomu, že intenzita a rozsah hybridních útoků proti EU se od začátku ruské válečné agrese proti Ukrajině výrazně zvýšily a že tyto incidenty jsou opakovaně spojovány s autoritářskými státy, zejména s Ruskem, Běloruskem, Čínou, Íránem a Severní Koreou;
- B. vzhledem k tomu, že Rusko představuje pro EU a její členské státy primární a největší bezpečnostní hrozbu; vzhledem k tomu, že Rusko soustavně porušuje zásadu územní celistvosti a politické nezávislosti stanovenou v čl. 2 odst. 4 Charty OSN; vzhledem k tomu, že hybridní útoky ohrožují demokracii v EU a v jejích členských státech;
- C. vzhledem k tomu, že tyto útoky jsou nyní mnohem závažnější a představují hrubé porušení svrchovanosti členských států, územní celistvosti EU a mezinárodního práva; vzhledem k tomu, že hybridní válka je nyní strukturální rys současného geopolitického prostředí;
- D. vzhledem k tomu, že mezi poslední hybridní útoky lze zahrnout i nepovolená vniknutí dronů, „pašerácké balony“, narušení vzdušného prostoru, tajné tunely pro infiltraci a pašování, sabotáže a špionáže kritické bezpečnostní a obranné infrastruktury, sabotáže podmořských kabelů a energetické infrastruktury, narušování GPS a spoofing navigace, kybernetické útoky, žhářství a atentáty, zneužívání migrace a organizované trestné činnosti jako zbraně, získávání elit, skryté zahraniční investice, hospodářský nátlak, exfiltraci údajů, jinou politickou podvratnou činnost a pronikání do ekonomiky, zahraniční manipulaci s informacemi a vměšování a zásahy do politických a volebních procesů;
- E. vzhledem k tomu, že v létě 2026 zažila EU zintenzivnění fyzických hybridních činností a útoků na celém svém území; vzhledem k tomu, že to zahrnovalo pokus o útok výbušnými drony namířený proti ukrajinským nákladním letadlům na letišti Lipsko/Halle v Německu, pokus o útok výbušným námořním dronem na rumunský projekt těžby plynu na moři, zmařený sabotérský a špionážní plán řízený Ruskem a zaměřený na vojenskou infrastrukturu a ukrajinská nákladní letadla v Rumunsku, žhářský útok namířený proti dodavateli v oblasti obrany v Estonsku, záměrné sabotérské a žhářské útoky namířené proti obranným zařízením a zařízením na výrobu dronů v Polsku, ruskou střelu s plochou dráhou letu, která narušila polský vzdušný prostor a spadla v oblasti Lublinu, a zmařený žhářský plán na Slovensku zaměřený na ukrajinského výrobce dronů; vzhledem k tomu, že útok na letiště Lipsko/Halle, útoky na rumunský projekt těžby plynu na moři a sabotérský plán zaměřený na vojenskou infrastrukturu a ukrajinská nákladní letadla v Rumunsku připsaly příslušné vnitrostátní orgány veřejně Rusku; vzhledem k tomu, že po útoku na letiště Lipsko/Halle německé orgány uzavřely ruský konzulát v Bonnu a Ruský dům v Berlíně;
- F. vzhledem k tomu, že svrchovanost a územní celistvost každého členského státu jsou základními zásadami EU; vzhledem k tomu, že

nepřátelské státní subjekty, zejména Rusko, útočí na územní celistvost EU na dvou frontách: prostřednictvím přímých fyzických útoků na členské státy a prostřednictvím informačních vlivových operací, jejichž cílem je oslabit jednotu EU přípravou kroků mířících k vystoupení členských států z EU;

- G. vzhledem k tomu, že hybridní hrozby mají stále více dopad na EU jako celek, včetně zámořských zemí a území, jako je Grónsko, avšak útoky hrozí obzvláště regionům při vnějších hranicích EU a námořním oblastem EU; vzhledem k tomu, že tyto útoky míří také na kandidátské země a země sousedící s EU, zejména na Ukrajinu, Moldavsko, Arménii, Gruzii a západní Balkán; vzhledem k tomu, že územní celistvost zemí v sousedství EU je klíčem k zajištění míru, stability a bezpečnosti v Evropě i ve světě;
- H. vzhledem k tomu, že vměšování třetích zemí do záležitostí Grónska, zejména štvavé narativy a hybridní akce na území Grónska, jakož i výslovné výhrůžky vlády Spojených států týkající se svrchovanosti Grónska, vyvolaly obavy o grónskou svrchovanost a územní celistvost;
- I. vzhledem k tomu, že Gruzie je příklad úspěšného ruského hybridního vměšování, které vedlo k tomu, že orgány vedené pro-kremelským Gruzínským snem kopírují ruský scénář hybridních operací a používají jej proti vlastní občanské společnosti a demokratickým institucím Gruzie;
- J. vzhledem k tomu, že ruské zpravodajské služby stále častěji provádějí sabotáže za pomoci zprostředkovatelů, zranitelných sociálních skupin, včetně nezletilých osob a agentů „na jedno použití“, což komplikuje prisuzování odpovědnosti za takové činy a reakce na ně; vzhledem k tomu, že náboženské instituce, včetně ruské pravoslavné církve a sítě napojených na Muslimské bratrstvo, jsou zneužívány k zasahování do záležitostí EU, což oslabuje demokratické hodnoty, právní stát a schopnost EU bránit se;
- K. vzhledem k tomu, že účelem těchto útoků je nejen vyvolat chaos a destabilizovat členské státy EU, ale také podkopat demokratickou integritu, manipulovat rozhodovací procesy, prohloubit politické rozdělení, oslabit sociální soudržnost, zasévat strach a nedůvěru mezi občany EU a oslabit obrannou připravenost a podporu EU Ukrajině, což má kaskádové účinky v celé EU;
- L. vzhledem k tomu, že uplatnění článku 5 NATO po teroristických útocích ze dne 11. září 2001 ukázalo, že kolektivní obrana může být zahájena nejen v důsledku útoků souvisejících s jednáním státního subjektu, ale také útoků, za nimiž stojí nestátní subjekty a komplexní sítě působící přes státní hranice; vzhledem k tomu, že tento precedens zdůrazňuje vyvíjející se povahu bezpečnostních hrozeb a potřebu odpovídajícím způsobem přizpůsobit mechanismy kolektivní

reakce, a to i lepšími společnými normami a postupy pro přisouzení odpovědnosti za útoky;

- M. vzhledem k tomu, že spolu se zahraničními manipulacemi s informacemi a vměšováním drastickým způsobem zesílila kognitivní válka; vzhledem k tomu, že podle čtvrté výroční zprávy Evropské služby pro vnější činnost (ESVČ) o hrozbách zahraniční manipulace s informacemi a vměšováním se očekává, že ruská činnost v oblasti zahraniční manipulace s informacemi a vměšováním se v roce 2026 zintenzivní, přičemž se předpokládá, že rozpočet na státem kontrolované sdělovací prostředky dosáhne přibližně 1,56 miliardy EUR, což je o 7 % více než v roce 2025, přičemž mezi hlavní terče bude patřit region Baltského moře a arktický region;
- N. vzhledem k tomu, že při zahraniční manipulaci s informacemi a vměšováním se používají sofistikované kognitivně-psychologické metody, včetně reflexivní kontroly, což je technika zakořeněná v sovětské vojenské teorii, která zavádí konkrétní informační vstupy za účelem omezení vnímaných možností cílového subjektu a směřování jeho rozhodnutí ke strategickým cílům influencera;
- O. vzhledem k tomu, že strategie národní bezpečnosti Ruska z let 2015 a 2021 vymezují prosazování takzvaných tradičních hodnot a „ruského světa“ coby nástrojů jeho širší strategie hybridní války a geopolitického vlivu; vzhledem k tomu, že Rusko jako součást své strategie hybridní války využívá historické, náboženské, kulturní a hodnotově orientované narativy s cílem ovlivnit veřejný diskurz a dynamiku církevního života, oslabit sociální soudržnost, demokratickou odolnost a transatlantickou integraci;
- P. vzhledem k tomu, že průřezový charakter kognitivní oblasti vyžaduje, aby kognitivní ukazatele byly zcela začleněny do společného operačního kontextu používaného strukturami kybernetické, zpravodajské, donucovací, vojenské a kritické infrastruktury;
- Q. vzhledem k tomu, že úspěch moderních vojenských operací a efektivita veřejných institucí závisí stále více na kontrole kyberprostoru a na strategickém využívání digitálních zdrojů a informačních systémů;
- R. vzhledem k tomu, že vnitřní bezpečnost je i nadále v kompetenci členských států, ačkoliv přeshraniční, propojená a mnohorozměrná povaha těchto hybridních útoků vyžaduje posílenou spolupráci, systematické sdílení informací a koordinovanou činnost na úrovni EU, která by se opírala o odpovídající financování a byla by doplněna dlouhodobými strategiemi k posílení společenské odolnosti a ochraně institucionální integrity;
- S. vzhledem k tomu, že agentury EU působící v oblasti spravedlnosti a vnitřních věcí (SVV) hrají ve spolupráci s vnitrostátními orgány klíčovou úlohu při vytváření a udržování společného situačního

povědomí o rizicích souvisejících s těmito hrozbami a při pomoci členským státům v přední linii v krizových situacích; vzhledem k tomu, že Komise zahrnula do svých stěžejních iniciativ na volební období 2024–2029 posílení Evropské agentury pro pohraniční a pobřežní stráž (Frontex), jakož i revizi mandátů Agentury Evropské unie pro spolupráci v oblasti prosazování práva (Europol) a Agentury Evropské unie pro justiční spolupráci v trestních věcech (Eurojust); vzhledem k tomu, že možná i další iniciativy, např. Hlídka východního křídla, pomohou posílit ochranu vnějších hranic a zvýšit odolnost vůči hybridním hrozbám;

- T. vzhledem k tomu, že pokročilé systémy umělé inteligence strukturálním způsobem narušují stávající systémy kybernetické bezpečnosti a vedou k tomu, že již neplatí modely hrozeb a obranné předpoklady vypracovávané v předchozích desetiletích; vzhledem k tomu, že nepřátelské státní a nestátní subjekty již využívají schopností umělé inteligence ke zvýšení rychlosti, rozsahu a přesnosti hybridních operací, včetně kybernetických zásahů, otravy dat, dezinformačních kampaní a útoků na kritickou infrastrukturu; vzhledem k tomu, že kolektivní rámce EU pro kybernetickou odolnost musí být přizpůsobeny tak, aby řešily nová zranitelná místa;
- U. vzhledem k tomu, že navzdory značnému úsilí členských států a rozvoji nástrojů a mechanismů pro boj proti hybridním hrozbám je reakce EU na hybridní útoky i nadále poznamenána mezerami v právních předpisech, absencí harmonizovaného přístupu členských států, rozdílnými úrovněmi informovanosti a absencí specializované struktury nebo subjektu pro monitorování těchto útoků; vzhledem k tomu, že navzdory naléhavé situaci členské státy EU proto dosud nepřipravily plně koordinovanou a soudržnou reakci na hybridní válku, a to ani individuálně ani na evropské úrovni nebo případně ve spolupráci s NATO;
- V. vzhledem k tomu, že pro vnitrostátní výdaje na obranu by byla užitečná větší koordinace a sdružování členských států nebo další investice do evropských projektů spolupráce; vzhledem k tomu, že díky výraznému zvýšení výdajů členských států na obranu v kombinaci s obrannými iniciativami EU, jako je SAFE, a s dalšími opatřeními v rámci obranné připravenosti 2030 se začínají řešit dlouhodobé nedostatky ve schopnostech, ale k lepší ochraně EU, jejích členských států a jejích občanů před hybridními hrozbami je zapotřebí, aby se toto zvýšení rychleji odrazilo v konkrétních operačních schopnostech; vzhledem k tomu, že v této oblasti stále existuje další potenciál pro technologie dvojího užití; vzhledem k tomu, že další reakce je rovněž nutná v oblasti vnitřní bezpečnosti;
- W. vzhledem k tomu, že odpovědnost za národní bezpečnost nesou i nadále předně členské státy a veškerá opatření a iniciativy koordinované nebo navrhované na úrovni EU musí být koncipovány a prováděny tak, aby byly plně respektovány výlučné pravomoci

členských států, a musí být v souladu se souborem nástrojů EU pro hybridní hrozby, zahraniční manipulaci s informacemi a vměšování a diplomacii v oblasti kybernetiky;

- X. vzhledem k tomu, že závislost EU na zahraničních subjektech a technologiích vyrobených v zahraničí, pokud jde o kritickou infrastrukturu a dodavatelské řetězce, včetně získávání surovin ze třetích zemí, je jednou z největších slabin EU a tím pádem i klíčovou výzvou pro evropskou bezpečnost a strategickou autonomii;
- Y. vzhledem k tomu, že současnou bezpečnostní situaci, v níž se EU nachází, necharakterizuje ani mír, ani otevřený ozbrojený konflikt, ale nulová fáze války, v níž protivníci nasazují hybridní nástroje k tomu, aby využili propast mezi správnými strukturami EU v době míru a rozhodností potřebnou k odrazování a k reakci; vzhledem k tomu, že stávající rámce zahraniční a bezpečnostní politiky EU nastavené pro jednání založená na konsenzu vytvářejí strukturální latentní stav, který protivníci aktivně zneužívají; vzhledem k tomu, že tento mezistav vyžaduje zásadní přehodnocení struktury rozhodování EU v oblasti bezpečnosti a obrany;
- Z. vzhledem k tomu, že důvěryhodnost odstrašování nezávisí pouze na materiálních schopnostech a technologickém náskoku evropských a spojeneckých sil, ale rozhodně i na politické vůli, strategické soudržnosti a společném porozumění hrozbě; vzhledem k tomu, že hybridní strategie Ruska je nastavena tak, aby nahlodala právě tyto kvality, a to prostřednictvím nejednoznačnosti, rozdělení a podprahového tlaku, s cílem poškodit důvěryhodnost závazků v oblasti kolektivní obrany před dosažením jakékoli kinetické prahové hodnoty;

### ***Hybridní válka: na pomezí války a míru***

1. zdůrazňuje, že hybridní operace jsou záměrné, kombinované, na zpravodajských informacích založené a koordinované činy států, a to i prostřednictvím nestátních subjektů, zprostředkovatelů a zástupných subjektů, které jsou prováděny v několika oblastech současně; zdůrazňuje, že jsou navrženy tak, aby vypadaly jako ojedinělé incidenty a nepřekročily práh ozbrojeného konfliktu, avšak zároveň mají potenciál vyvolat účinky srovnatelné s konvenční agresí, což výrazně ztěžuje přisuzování odpovědnosti a účinnou reakci; vyzývá EU a členské státy, aby uznaly, že hybridní operace mohou představovat formu války bez ohledu na to, zda je použita konvenční síla či nikoliv;
2. poukazuje na to, že hlavním cílem hybridní války je destabilizovat, rozdělit a oslabit EU a její členské státy využitím systémových slabin a oslabením jejich bezpečnosti, odolnosti, demokratických základů a obranné připravenosti, a to narušením průmyslové základny obrany a kritické infrastruktury EU, ochromením veřejné a politické podpory

pro obranu EU a posílením politických sil nakloněných pachatelům pomocí systematických zásahů do demokratických procesů;

3. potvrzuje, že Rusko, které jedná přímo nebo prostřednictvím řady zástupných subjektů, například Běloruska, je státním aktérem, který pro EU a její členské státy představuje největší hybridní hrozbu; konstatuje, že Čína, Írán, Severní Korea a další provádějí hybridní kampaně, jejichž cílem je oslabení evropských demokracií a narušení bezpečnostních zájmů EU; zdůrazňuje, že EU musí zaujmout komplexní přístup k hybridním hrozbám, v jehož rámci se bude zabývat nejen ruskými a běloruskými aktivitami, ale také silící strategickou úlohou Číny, Íránu a Severní Koreje, pokud jde o umožňování a posilování nepřátelských akcí namířených proti evropským zájmům a evropské bezpečnosti; se znepokojením konstatuje, že nestátní subjekty – včetně teroristických skupin, organizovaných zločineckých skupin, oligarchických a kleptokratických sítí, náboženských institucí a sítí, soukromých vojenských společností, extremistických hnutí a subjektů provádějících ovlivňování na zakázku – mohou rovněž vést nebo umožňovat hybridní kampaně namířené proti evropským demokraciím;
4. vyzývá Komisi a Radu, aby posoudily přiměřenost stávajících právních rámců EU pro řešení hybridních hrozeb, odstranily zjištěné nedostatky a považovaly podprahové hybridní operace, které nelze řešit pouze vymáháním práva, za záležitosti kolektivní bezpečnosti, které vyžadují kombinovanou civilně-vojenskou reakci;

### ***Informační válka, kognitivní bezpečnost a společenská odolnost***

5. upozorňuje na to, že informační válka je jedním z klíčových prvků hybridní války; vyjadřuje znepokojení nad rostoucím rozsahem kognitivní války a zahraničních manipulací s informacemi a vměšováním, jejichž cílem je narušit důvěru společnosti v demokratické instituce, zvýšit polarizaci ve společnosti a oslabit demokratické rozhodovací procesy a podporu vyjadřovanou veřejností evropské bezpečnosti a obraně, jakož i Ukrajině;
6. poukazuje na to, že o dosažení výše uvedených cílů (viz odstavec 5) se usiluje převážně sofistikovanými a koordinovanými operacemi, které zasahují do mnoha oblastí společenského života a využívají strategické kognitivní-psychologické metody určené k utváření rozhodovacích procesů, individuálního a kolektivního vnímání, identity, kulturních norem, historické paměti, morálních rámců a systémů náboženského přesvědčení a zároveň zneužívají technologickou infrastrukturu, mediální ekosystémy a hospodářská nebo politická slabá místa; se znepokojením konstatuje, že zahraniční manipulace s informacemi a vměšováním využívají sofistikované kognitivně-psychologické metody, včetně reflexivní kontroly, které je obtížné odhalit, zjistit, kdo je za ně odpovědný, nebo proti nim

bojovat konvenčními postupy; zdůrazňuje proto, že soubor nástrojů EU týkající se zahraničních manipulací s informacemi a vměšování musí výslovně zahrnovat protiopatření proti těmto pokročilým technikám ovlivňování, má-li být zajištěna integrita rozhodování EU;

7. varuje před tím, že jednotlivé kinetické incidenty mohou vyvolat okamžité, synchronizované a organizované zahraniční manipulace s informacemi a vměšování nebo mohou být záměrně navrženy tak, aby takové operace kryly, přičemž nepřátelské subjekty využívají prodlev před vydáním úředních prohlášení k ovlivňování vnímání veřejnosti; vyzývá k tomu, aby se problém této informační prodlevy řádně řešil posílením evropské koordinace, zejména zlepšením koordinace veřejného a soukromého sektoru v informační oblasti; zdůrazňuje, že je třeba vyvinout společné nástroje, jako jsou komunikační příručky, které umožní rychlejší, koordinovanou a přesnou komunikaci před tím, než informační prostor zaplní nepřátelské narativy;
8. vyjadřuje znepokojení nad tím, že Rusko používá historický revizionismus, zejména ve vztahu ke druhé světové válce a k odkazu Sovětského svazu, zahraniční manipulace s informacemi a vměšování a selektivní výklad historických událostí jako nástroje hybridní války, jejichž cílem je polarizovat veřejné mínění, oslabit společenskou soudržnost a demokratickou odolnost a delegitimizovat územní celistvost svrchovaných států;
9. zdůrazňuje, že zahraniční manipulace s informacemi a vměšování přesahují rámec tradičních sdělovacích prostředků a zasahují do vzdělávací, kulturní a náboženské oblasti; poukazuje na strategické využívání náboženských institucí a sítí, včetně účelového využívání ruské pravoslavné církve, k prosazování morální autority, šíření státem podporovaných narativů a postupnému oslabování odolnosti společnosti a demokratické soudržnosti; dále vyzývá EU, aby pracovala na odhalování hybridních hrozeb využívajících náboženské kanály a školila úředníky EU v oblasti mezináboženské angažovanosti, náboženské gramotnosti a v identifikaci finančního vlivu, zmocňování se organizací a manipulací s informacemi, což jsou praktiky, které podkopávají demokratické hodnoty a sociální soudržnost;
10. odsuzuje zneužívání on-line platform nepřátelskými aktéry k hybridním činnostem; vyzývá k důslednějšímu prosazování stávajících pravidel EU týkajících se transparentnosti doporučovacích systémů, politické reklamy, koordinovaného neautentického chování a rychlého šíření zmanipulovaného obsahu nebo obsahu vytvořeného umělou inteligencí v souvislosti s nepřátelským zahraničním vměšováním;
11. zdůrazňuje, že nepřátelské subjekty používají stále sofistikovanější a přizpůsobivější hybridní techniky; zdůrazňuje, že nástroje umělé inteligence – deepfake, algoritmické šíření a automatizované sítě

účtů – urychlují a zlevňují informační vlivové operace a zároveň ztěžují jejich odhalování; domnívá se, že reakce EU na zahraniční manipulaci s informacemi a vměšování založené na umělé inteligenci musí k umělé inteligenci přistupovat jednak jako k vektoru hrozeb a jednak jako ke kritické schopnosti obrany;

12. konstatuje, že odpověď EU na zahraniční manipulace s informacemi a vměšování je i nadále reaktivní, chybí jí trvalé monitorování v reálném čase, přisuzování odpovědnosti a schopnost být proaktivní; trvá na tom, že zahraniční manipulace s informacemi a vměšování je třeba považovat za vážnou bezpečnostní hrozbu, která vyžaduje operativní přístup, lepší koordinaci a spolupráci členských států na všech úrovních, včetně včasného odhalení, přiměřených možností reakce a důkladnější ochrany demokratických procesů, zejména během období voleb;
13. vítá činnost ESVC v oblasti monitorování a odhalování zahraniční manipulace s informacemi a vměšování a reakce na ně a podtrhuje význam systému rychlého varování EU pro koordinovanou společnou reakci na dezinformace; vyzývá Komisi a členské státy, aby posoudily doporučení zvláštního výboru pro Evropský štít pro demokracii (EUDS) a vycházely z nich; vyzývá k dalšímu posílení systému rychlého varování tak, aby mohl řešit manipulace s informacemi v reálném čase a aby byly jasně dány provozní povinnosti; vyzývá k zavedení standardizovaných mechanismů předběžného vyvracení nepravdivých informací a mechanismů rychlé reakce v celé Unii a ve spolupráci s partnerskými zeměmi, včetně strukturovaných komunikačních kanálů včasného varování; vybízí k rozvoji proaktivních nástrojů strategické komunikace, které by uměly předem varovat obyvatelstvo před očekávanými dezinformačními taktikami, vzorci narativů a vykonstruovaným obsahem v obdobích před kritickými událostmi, jako jsou volby, jednání o energetice nebo bezpečnostní krize;
14. vyzývá Komisi, vysokou představitelku a členské státy, aby důsledně a koordinovaně využívaly soubor nástrojů proti zahraničním manipulacím s informacemi a vměšování a uvedly jej plně do praxe a uplatňovaly příručku proti zahraničním manipulacím s informacemi a vměšování, a to i prostřednictvím koordinovaného přisuzování odpovědnosti a případně prostřednictvím omezujících opatření zaměřených nejen na jednotlivé incidenty, ale i na nezákonné finanční toky, technickou infrastrukturu a zprostředkovatelské a zástupné sítě, které podporují zahraniční manipulace s informacemi a vměšování;
15. zdůrazňuje, že hlavním terčem ruských hybridních operací je i nadále evropské veřejné mínění; připomíná, že desetiletí míru vytvořila stav strategické lhostejnosti, který nepřátelské informační vlivové operace zneužívají a posilují; domnívá se, že vlády a orgány EU společně odpovídají za to, aby veřejnost chápala povahu a blízkost

hybridní hrozby, a že pokud to nezajistí, dochází k oslabování připravenosti a odstrašujícího účinku zevnitř;

16. vyzývá členské státy, aby uplatňovaly komplexní vládní a celospolečenský přístup a kladly předně důraz na odolnost a připravenost, jak je zdůrazněno v Niinistově zprávě; připomíná, že terčem hybridních hrozeb je společnost jako celek, neboť nepřátelské subjekty využívají slabiny ve vzájemně propojených oblastech, službách, komunitách a informačních prostorech; domnívá se, že důvěra a sociální soudržnost mají zásadní význam pro odolnost společnosti; zdůrazňuje proto, že odolnost vůči hybridním hrozbám musí jít nad rámec vojenských, technických a institucionálních opatření a že je k ní zapotřebí propojení veřejných orgánů, soukromého sektoru, občanské společnosti – včetně místních komunit a voličů, které je obtížné oslovit, – akademické obce a nezávislých sdělovacích prostředků za účelem posílení demokratické důvěry, informovanosti veřejnosti a společenské připravenosti, čímž se podpoří nová evropská bezpečnostní kultura;
17. zdůrazňuje, že je třeba posílit odolnost veřejnosti vůči zahraniční manipulaci s informacemi a vměšování prostřednictvím občanské výchovy, mediální gramotnosti, strategické komunikace, podpory nezávislých sdělovacích prostředků, včetně investigativní žurnalistiky, sítí pro ověřování faktů, jako je Evropské středisko pro sledování digitálních médií, a nástrojů umělé inteligence pro odhalování a analýzu dezinformačních kampaní ve velkém měřítku; vyzývá k užší spolupráci se sdělovacími prostředky a subjekty audiovizuálního průmyslu při odhalování zahraničních manipulací s informacemi a vměšování, přisuzování odpovědnosti za ně a reakcích na ně; vyzývá k pobídkám k odhalování manipulací s informacemi a vměšování, mimo jiné prostřednictvím iniciativ veřejného a soukromého sektoru, k analýzám těchto manipulací a tohoto vměšování a přisuzování odpovědnosti za ně, k bezpečným mechanismům sdílení údajů a interoperabilním systémům včasného varování;
18. vyjadřuje znepokojení nad informacemi o neustálém zahraničním vměšování do evropských voleb, mimo jiné pomocí kybernetických útoků a dezinformací využívajících umělou inteligenci; připomíná, že integrita a odolnost volebních procesů jsou úhelným kamenem demokratických základů EU a klíčovým terčem hybridních operací; zdůrazňuje, že zahraniční manipulace s informacemi a vměšování se během voleb obvykle zintenzivňují, a že pro zajištění integrity voleb a demokratické stability v celé EU a v partnerských zemích, včetně kandidátských zemí a potenciálních kandidátů, je proto nezbytná nepřetržitá ostražitost a koordinace; vítá společné sdělení s názvem „Evropský štít pro demokracii: podpora silných a odolných demokracií“, vítá i zřízení Evropského střediska pro odolnost demokracie a vyzývá k jasnému vymezení jeho úkolů, aby se zabránilo opakování stávajících iniciativ;

19. vyzývá k tomu, aby byla v nadcházející bezpečnostní strategii EU brána v potaz a řešena zranitelná místa v kognitivních procesech v souvislosti s hybridní válkou a aby Komise podnikla další kroky tím, že zajistí mapování těchto zranitelných míst a poskytne referenční hodnoty odolnosti;

### ***Kybernetická bezpečnost***

20. zdůrazňuje, že kybernetické útoky se staly ústředním prvkem hybridních kampaní a že využívají rostoucí digitalizaci kritických odvětví, jako je zdravotní péče, finance a energetika, což způsobuje kaskádová narušení, která mohou mít závažné hospodářské a společenské důsledky;
21. konstatuje, že kyberprostor se stal pátou válečnou doménou a hlavním nástrojem hybridních hrozeb; zdůrazňuje, že s ohledem na rostoucí závislost vojenských platforem, kritické infrastruktury a velících, řídicích, komunikačních a zpravodajských systémů na digitálních technologiích je kybernetická bezpečnost nezbytná pro operační převahu a odolnost ve všech doménách; zdůrazňuje proto, že za účelem neutralizace hrozeb a zajištění věrohodného odstrašování jsou nutné suverénní kybernetické kapacity v oblasti detekce, přisuzování odpovědnosti, reakce a zpravodajství, včetně ofenzivních kapacit;
22. zdůrazňuje blízkost zahraničních manipulací s informacemi a vměšování na jedné straně a kybernetické bezpečnosti na straně druhé a konstatuje, že ke kybernetickým útokům často dochází v raných fázích kampaní zahraniční manipulace s informacemi a vměšování; vyzývá k tomu, aby mechanismy pro boj proti zahraniční manipulaci s informacemi a vměšování byly systematicky propojovány se schopnostmi v oblasti kybernetické bezpečnosti s cílem odhalit, přisoudit odpovědnost a narušit koordinovanou manipulativní infrastrukturu v rané fázi;
23. varuje před riziky, která s sebou nesou konvergentní kybernetické operace, při nichž subjekty napojené na stát aktivně přebírají operační profily, metodiky a osobnostní profily nezávislých aktivistických hackerů nebo komerčně motivovaných pachatelů kybernetické kriminality s cílem skrýt odpovědné aktéry a sladit kybernetickou činnost s geopolitickými událostmi, volbami nebo kinetickými operacemi; zdůrazňuje, že v zájmu ochrany základních svobod a zároveň i účinnějšího přičítání odpovědnosti za kybernetické útoky, vyvozování odpovědnosti a odrazujícího účinku musí reakce na hybridní kybernetické hrozby jasně rozlišovat mezi legitimními formami projevu politického názoru nebo občanského nesouhlasu a finančně motivovanou kyberkriminalitou a státem podporovanými operacemi;

24. varuje před tím, že s rozšířením internetu věcí se zvyšuje riziko, že kybernetické útoky budou mít fyzické dopady na kritickou infrastrukturu a základní služby, a vyzývá k tomu, aby byly stanoveny povinnosti týkající se bezpečnosti již od návrhu, díky nimž by se zajistilo, aby se připojená zařízení nestala vstupními body pro hybridní operace s reálnými důsledky;
25. upozorňuje, že stoprocentní kybernetická ochrana neexistuje a že je třeba přeorientovat se na kybernetickou odolnost; zdůrazňuje, že kybernetickou odolnost Evropy je třeba vybudovat prostřednictvím častých a realistických kybernetických cvičení; zdůrazňuje, že kybernetická odolnost se týká nejen systémů, ale také ochrany údajů, které jsou jednak terčem a jednak nástrojem hybridních hrozeb; dále zdůrazňuje, že je třeba posílit kybernetickou odolnost v celé evropské hospodářské struktuře, a to i mezi malými a středními podniky a poskytovateli základních digitálních služeb;
26. podtrhuje přidanou hodnotu EU, která spočívá v tom, že pomáhá členským státům při propojování vnitrostátních kapacit, vytváření společného situačního povědomí a usnadnění rychlejších a soudržnějších reakcí na hybridní hrozby; doporučuje, aby Komise prozkoumala návrhy jednotnějšího rámce na podporu členských států při plánování, operativní koordinaci a provádění kybernetických operací; vítá dokončení projektu stálé strukturované spolupráce (PESCO) týkající se Koordinačního střediska pro kybernetický a informační prostor (CIDCC) a pokrok směrem k jeho přeměně na stálé koordinační středisko EU pro kybernetickou obranu (EU CDCC);
27. vyzývá k větší harmonizaci povinností hlásit incidenty a klíčových právních pojmů napříč EU pro kybernetickou bezpečnost a odolnost s cílem snížit roztržitost, zlepšit interoperabilitu a zajistit, aby v hybridních krizových scénářích byla i nadále hlavní prioritou rychlá obnova základních služeb;
28. bere na vědomí rezervu EU pro kybernetickou bezpečnost, kterou spravuje Agentura Evropské unie pro kybernetickou bezpečnost (ENISA) na základě nařízení o kybernetické solidaritě, jako strategickou kybernetickou kapacitu EU rychlé reakce; vyzývá k tomu, aby její financování bylo přizpůsobeno operační poptávce, a zdůrazňuje, že její první nasazení v Moldavsku je důležitým krokem k posílení operační kybernetické odolnosti EU a podpory partnerských zemí; vyzývá orgány členských států pro kybernetickou bezpečnost, aby podporovaly strukturovanou spolupráci s důvěryhodnými poskytovateli rezervy, a plně tak využívaly dostupné schopnosti reakce na incidenty, pokud se objeví hybridní hrozby v souvislosti s významnými nebo rozsáhlými kybernetickými incidenty;
29. znovu potvrzuje význam týmů rychlé kybernetické reakce v rámci PESCO jako stálé kapacity kybernetické obrany, kterou lze nasadit

na žádost členských států, partnerských zemí a misí společné bezpečnostní a obranné politiky (SBOP) čelících kybernetickým útokům s důsledky pro bezpečnost a obranu, a vyzývá k odpovídajícímu financování těchto týmů ze strany EU;

30. opakuje, že je důležité plně využívat soubor nástrojů pro diplomacii v oblasti kybernetiky s cílem předcházet kybernetickým hrozbám a nepřátelským činnostem v kyberprostoru, odrazovat od nich a reagovat na ně; bere na vědomí, že v březnu 2026 byl spuštěn první stálý globální mechanismus OSN pro kybernetickou bezpečnost, a domnívá se, že EU by se měla zaměřit na oblasti, v nichž existuje jasná evropská přidaná hodnota, a zároveň by měla dále posílit evropskou diplomacii v oblasti kybernetiky;
31. zdůrazňuje, že kybernetická odolnost a obranná opatření nestačí k zajištění věrohodného odrazování od hybridních hrozeb, jak je zdůrazněno ve společné bílé knize o budoucnosti evropské obrany 2030; vyzývá Komisi a členské státy, aby ve spolupráci s NATO přezkoumaly právní, procesní a provozní požadavky pro přiměřená kybernetická protipatření, která budou v souladu s právními předpisy; vítá pokrok, kterého bylo dosaženo směrem ke zřízení koordinačního střediska EU pro kybernetickou spolupráci, a vyzývá k jeho urychlenému zprovoznění a k provedení mandátu v souladu se závěry Rady ohledně politiky EU v oblasti kybernetické obrany s cílem zajistit důvěryhodnější a schopnější kybernetickou obranu EU;
32. varuje před tím, že umělá inteligence není pouze nástrojem používaným při hybridních kybernetických činnostech, ale také kritickou technologií, která může být sama o sobě terčem, může být manipulována nebo poškozena vkládáním podvržených pokynů, zmanipulováním trénovacích dat a útoky na dodavatelský řetězec; zdůrazňuje, že vzhledem k rostoucí závislosti na komerčních systémech umělé inteligence a systémech dvojího užití umělé inteligence v civilním, bezpečnostním a obranném kontextu musí EU zaujmout jasný postoj ke kybernetické bezpečnosti, odolnosti a správě umělé inteligence dvojího užití, včetně záruk integrity modelů, důvěryhodných dodavatelských řetězců a dohledu na hranici mezi civilními, obrannými a vnitrostátními bezpečnostními aplikacemi;
33. zdůrazňuje, že je nutná větší ochrana kritické veřejné digitální infrastruktury a registrů citlivých a státem spravovaných údajů, včetně volební infrastruktury, neboť ty jsou potenciálním terčem hybridních hrozeb vzhledem k jejich úloze v zajišťování digitální identity, veřejné správy, správy dat, bezpečné komunikace, přístupu k základním službám a integrity demokratických procesů;

### ***Kritická infrastruktura***

34. odsuzuje hybridní útoky, jejichž terčem je kritická infrastruktura EU, zejména energetická, dopravní, komunikační a družicová infrastruktura, včetně infrastruktury pro vojenskou mobilitu, což jsou jak kritické nástroje, tak i strategická aktiva kolektivní obrany, odolnosti a civilní ochrany EU; zdůrazňuje, že tato kritická infrastruktura funguje jako propojený systém, který nelze chránit izolovaně, a že větší digitální konektivita zvyšuje zranitelnost; vítá skutečnost, že se Komise v návrhu nařízení o vojenské mobilitě (COM(2025)0847), jakož i v návrhu hlavních směrů pro transevropskou energetickou infrastrukturu (COM(2025)1006) zaměřuje na ochranu a odolnost energetické infrastruktury a infrastruktury vojenské mobility; vyzývá Komisi a členské státy, aby přijaly veškerá opatření nezbytná k zajištění její ochrany;
35. zdůrazňuje, že doména vesmíru je stále důležitějším bojištěm, na němž se odehrává hybridní válka, přičemž nepřátelské subjekty se zaměřují na družicové komunikace, navigační a pozorovací systémy prostřednictvím kybernetických operací, fyzických útoků, rušení a spoofingu nebo zneužívání strategických závislostí; zdůrazňuje, že narušení kosmických prostředků může mít značné důsledky pro civilní bezpečnost EU, kritickou infrastrukturu, vojenskou mobilitu a schopnosti reakce na krize; vyzývá proto k zajištění větší odolnosti kosmických systémů EU, včetně lepšího získávání poznatků o situaci ve vesmíru, ochrany pozemní infrastruktury, požadavků na kybernetickou bezpečnost, bezpečnosti dodavatelského řetězce, pravidelných cvičení a alternativních nebo záložních schopností v oblasti určování polohy, navigace a určování času; dále vyzývá k začlenění domény vesmíru do širšího rámce EU pro boj proti hybridním hrozbám;
36. konstatuje, že nepřátelské subjekty, zejména Rusko, stále více využívají energetickou infrastrukturu, trhy s energií a energetickou závislost jako zbraň k politickému nátlaku; zdůrazňuje strategický význam kritické energetické infrastruktury pro obranné i civilní potřeby; naléhavě vyzývá Komisi a členské státy EU, aby na základě příštího víceletého finančního rámce na období 2028–2034 vytvořily právní a finanční rámec EU, který by zajistil dostatečnou ochranu a odolnost kritické energetické infrastruktury, přičemž prioritou by měly být návrhy Komise týkající se hlavních směrů pro transevropskou energetickou infrastrukturu (COM(2025)1006) a Nástroj pro propojení Evropy (COM(2025)0547);
37. odsuzuje aktivity ruské stínové flotily, které zvyšují riziko námořních nehod, kryjí sabotáže napojené na stát a ohrožují kritickou infrastrukturu, jako jsou podmořské kabely, zařízení na výrobu energie na moři a přístavní zařízení; vyzývá k posílení monitorovacích, inspekčních a vymáhacích opatření v evropských vodách a vyzývá EU, aby zintenzivnila reakce na hybridní hrozby v námořních zónách; vybízí Komisi, aby na základě Bezpečnostní iniciativy proti šíření zbraní jakožto vzoru prozkoumala právní a

operační rámce, které by umožnily vstup na palubu plavidel napojených na stínové flotily, a vyzývá Finanční akční výbor, aby více prostudoval úlohu neprůhledných vlastnických struktur, rejstříků vlajek a souvisejících finančních sítí při napomáhání k obcházení sankcí a k nezákonným finančním tokům;

38. zdůrazňuje, že podmořské kabely představují kvůli své fyzické expozici a potenciálu systémového narušení klíčové strategické zranitelné místo a terč pro hybridní sabotáže, neboť zajišťují převážnou většinu mezikontinentálního internetového provozu; oceňuje doporučení Komise o bezpečných a odolných podmořských kabelových infrastrukturách z roku 2024<sup>9</sup> a společné sdělení o akčním plánu EU o bezpečnosti kabelů z roku 2025 (JOIN(2025)0009) jako první důležité kroky k posílení bezpečnosti a odolnosti podmořské kabelové infrastruktury; dále volá po kapacitách pro informovanost o situaci na moři, které by integrovaly údaje ze satelitních, povrchových a podmořských senzorů s cílem odhalovat a monitorovat fyzická ohrožení podmořských kabelů a energetické infrastruktury na moři ve strategických námořních oblastech a přisuzovat za ně odpovědnost, a to včetně oblastí Baltského moře, Severního moře a arktické oblasti; doporučuje přísná ustanovení o trestní odpovědnosti s cílem odrazovat od těchto útoků, jakož i redundantní systémy pro zajištění odolnosti; dále zdůrazňuje, že je nutné zaujmout komplexní a víceúrovňový přístup kombinující technologické inovace, posílenou integraci zpravodajských služeb, lepší schopnosti přičítání odpovědnosti za útoky a posílenou spolupráci mezi NATO, členskými státy EU a příslušnými subjekty soukromého sektoru s cílem zajistit soudržnou ochranu podmořské infrastruktury;
39. vyzývá Komisi a členské státy, aby vypracovaly koordinovaný a celounijní výklad Úmluvy Organizace spojených národů o mořském právu (UNCLOS) s cílem zajistit soudržné potírání a účinnou kriminalizaci hybridních činností, sabotáží a porušování svrchovaných práv v námořních oblastech EU, jakož i účinné odrazování od těchto činností, zejména v Baltském moři, a zároveň připomíná cíl úmluvy UNCLOS zajistit mírové využívání moří; vybízí Komisi a členské státy, aby se inspirovaly australským příkladem zřízení tzv. zón ochrany kabelů doprovázených poskytnutím právních záruk a kriminalizací škod na podmořských kabelech za hranicí teritoriálního moře vymezenou 12 námořními mílemi, spolu s aktivním sledováním, dohledem a reakcí ve spolupráci s příslušnými partnery ze třetích zemí;

---

<sup>9</sup> Doporučení Komise (EU) 2024/779 ze dne 26. února 2024 o bezpečných a odolných podmořských kabelových infrastrukturách (Úř. věst. L, 2024/779, 8.3.2024, ELI: <http://data.europa.eu/eli/reco/2024/779/oj>).

40. vyzývá členské státy a Evropskou obrannou agenturu (EDA), aby pokračily v projektech PESCO Ochrany kritické infrastruktury na mořském dně (CSIP), přístavního a námořního dohledu a ochrany (HARMSPRO), Integrovaného víceúrovňového systému protivzdušné a protiraketové obrany (IMLAMD) a Systému pro obranu proti bezpilotním vzdušným prostředkům (C-UAS) s cílem posílit schopnosti dohledu, detekce a obrany před vzdušnými a námořními hrozbami; vyzývá Komisi, aby ve spolupráci s vysokou představitelkou a po konzultaci s členskými státy navrhla evropský obranný projekt společného zájmu zaměřený na integrovanou obranu mořského prostředí a mořského dna;
41. vítá přijetí směrnice o odolnosti kritických subjektů (CER)<sup>10</sup> a směrnice NIS2<sup>11</sup> jako důležité kroky k posílení odolnosti vůči hybridním útokům, zdůrazňuje však, že zpoždění při jejich provádění v jednotlivých členských státech jsou společnou slabinou, kterou je třeba bezodkladně řešit, a vyzývá k plnému a včasnému uplatňování těchto směrnic; naléhavě vyzývá Komisi, aby plně využívala svých monitorovacích a donucovacích pravomocí; vyzývá členské státy, aby začleňovaly odolnost již od návrhu jako standardní požadavek do všech nových a revidovaných právních předpisů;
42. vyjadřuje znepokojení nad zahraničním vlastnictvím kritické infrastruktury v EU, zejména ze strany Ruska a Číny, což výrazně zvyšuje riziko špionáže, vměšování a strategické závislosti; vítá politickou dohodu dosaženou mezi Parlamentem a Radou o posílení mechanismu EU pro prověřování přímých zahraničních investic; vyzývá členské státy, aby toto nařízení urychleně provedly, a pokud možno jej rozšířily o přístup „nakupovat v Evropě“, pokud jde o kritickou infrastrukturu a obranné vybavení, s cílem posílit strategickou autonomii EU;
43. je si vědom toho, že významná část kritické infrastruktury související se základními veřejnými službami a vojenskými schopnostmi je v soukromém vlastnictví nebo je provozována soukromými subjekty; vyzývá k vytvoření stálých a strukturovaných rámců pro spolupráci veřejného a soukromého sektoru, včetně sdílení informací, pohotovostního plánování a koordinovaného řešení krizí; zdůrazňuje, že pokud soukromá infrastruktura podporuje základní služby a citlivé údaje, musí veřejné orgány zajistit účinnou regulační a operační

---

<sup>10</sup> Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022 o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES (Úř. věst. L 333, 27.12.2022, s. 164, ELI: <http://data.europa.eu/eli/dir/2022/2557/oj>).

<sup>11</sup> 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 (směrnice NIS 2) (Úř. věst. L 333, 27.12.2022, s. 80, ELI: <http://data.europa.eu/eli/dir/2022/2555/oj>).

kontrolu; vyzývá k systematickému začleňování požadavků na obranu do plánování, navrhování a financování civilní infrastruktury; trvá na tom, že infrastruktura financovaná EU musí splňovat normy pro odolnost týkající se obrany, což je podmínkou pro podporu EU; dále vyzývá k tomu, aby byli vývojáři obranných technologií a poskytovatelé bezpečnosti systematicky zapojováni do raných fází posuzování hrozeb pro kritickou infrastrukturu a pohotovostního plánování, aby se zajistilo, že dostupné technologické kapacity budou zohledňovány ve vnitrostátních i unijních rámcích pro zvyšování odolnosti; uznává přínos malých a středních podniků, startupů a poskytovatelů inovativních technologií k odolnosti a ochraně kritické infrastruktury a vyzývá k tomu, aby se více zapojovaly do příslušných programů EU, systémů zadávání veřejných zakázek a partnerství veřejného a soukromého sektoru;

44. vyzývá členské státy, aby kritickou infrastrukturu podrobovaly pravidelným cvičením zaměřeným na připravenost a odolnost, včetně společných cvičení, a aby urychleně realizovaly prioritní schopnosti stanovené v bílé knize o evropské obraně, zejména protivzdušnou a protiraketovou obranu, drony a protidronové systémy, vojenskou mobilitu, kybernetickou a elektronickou válku a námořní schopnosti;
45. je znepokojen strukturální závislostí EU na vysoce rizikových zemích mimo EU, zejména na Číně, pokud jde o dodávky aktiv v podobě hardwaru a softwaru připojených k síti, jako jsou solární invertory, větrné turbíny, propojená vozidla a spotřebitelská digitální zařízení, která umožňují vzdálený přístup k systémům, jejich přenos nebo ovládání, a proto představují významnou zranitelnost; vyzývá Komisi, aby hodnocení bezpečnosti dodavatelského řetězce systematicky rozšiřovala na všechna odvětví kritické infrastruktury a více usilovala o omezování strategických závislostí; vyzývá členské státy, aby na tato hodnocení navazovaly, diverzifikovaly dodavatelské řetězce a, kdykoli to bezpečnostní aspekty vyžadují, upřednostňovaly ve strategických odvětvích podobně smýšlející dodavatele; vítá skutečnost, že cílem navrhované revize aktu o kybernetické bezpečnosti je poskytnout rámec pro zákaz součástí připojených k síti od vysoce rizikových dodavatelů a že strategický plán pro digitalizaci a umělou inteligenci v odvětví energetiky, který je součástí balíčku týkajícího se evropské technologické suverenity, stanoví přezkum rámce pro bezpečnost dodávek energie; vyzývá k urychlenému přijetí těchto opatření;
46. zdůrazňuje, že je důležité diverzifikovat dodavatelské trasy prostřednictvím bezpečných a odolných dopravních sítí s důvěryhodnými partnery s cílem snížit strategické závislosti a posílit hospodářskou bezpečnost a odolnost dodavatelského řetězce EU;
47. zdůrazňuje, že kritické a nově nastupující technologie, včetně umělé inteligence, cloudové infrastruktury, pokročilých polovodičů, kvantových technologií a bezpečných kybernetických, vesmírných,

autonomních a komunikačních systémů, jsou součástí kritické bezpečnostní infrastruktury EU, a to vzhledem k jejich zásadní úloze v oblasti obranné připravenosti, hospodářské odolnosti a provozní kontinuity; domnívá se, že odolná a konkurenceschopná digitální infrastruktura EU – včetně bezpečných místních datových center, svrchovaného cloudu EU, edge computingu a gigabitových sítí – je důležitým pilířem evropské bezpečnosti; zdůrazňuje, že schopnost EU odhalovat hybridní kampaně, odolávat jim a reagovat na ně závisí na její schopnosti vyvíjet, zabezpečovat a rozšiřovat tyto technologie v rámci odolné evropské průmyslové a technologické základny podporované dostatečnými investicemi EU, včetně investic do bezpečných, interoperabilních a odolných systémů sdílení informací a místních datových center, na něž se nevztahují extrateritoriální právní předpisy;

### ***Informovanost o situaci***

48. zdůrazňuje, že účinný boj proti hybridním hrozbám vyžaduje prevenci, včasné předvídání hrozeb a průběžné monitorování strategických zranitelností, aby bylo možné neutralizovat nepřátelské akce dříve, než budou mít systémové dopady, a také sdílený přehled o hrozbách, neboť cílová odvětví nemohou účinně reagovat na základě izolovaných zpráv o incidentech; vyzdvihuje v této souvislosti potenciální jedinečnou přidanou hodnotu EU při sdružování přeshraničních dat, které umožňuje odhalovat vzorce koordinovaných hybridních kampaní, jež žádný členský stát nedokáže identifikovat sám, i při koordinaci rozvoje postupů pro společné získávání poznatků o situaci a připisování hrozeb, společných rámců, metodik, taxonomií a protokolů interoperability mezi příslušnými unijními a vnitrostátními orgány a strukturami, které by podporovaly operativní spolupráci mezi členskými státy; vyzývá k tomu, aby tyto funkce byly formálně uznány jako koordinační a podpůrné pravomoci EU;
49. konstatuje, že středisko EU pro hybridní hrozby v rámci společné zpravodajsko-analytické složky (SIAC) zůstává ústředním orgánem EU s výhradní odborností v oblasti analýzy hybridních hrozeb ze všech dostupných zdrojů, který poskytuje povědomí o situaci na základě zpravodajských informací; opakuje, že jedinou bránou pro zpravodajské informace v orgánech EU by mělo být středisko SIAC, a zdůrazňuje jeho zvláštní postavení v rámci bezpečnostní architektury EU; podporuje analýzu hybridních trendů jako klíčový nástroj pro analýzu hybridních hrozeb a odhalování vzorců a její řádné zapojování do procesů tvorby politik;
50. připomíná nedostatečný pokrok při plnění cíle stanoveného ve Strategickém kompasu a společném dokumentu vysokého představitele a členských států o posílení společné zpravodajsko-analytické složky EU (ESVČ(2024) 2014), kterým je posílit středisko SIAC poskytnutím dodatečných zdrojů ke shromažďování, analýze a

integraci příslušných informací, aby mohlo účinně vytvářet a poskytovat zpravodajské informace v oblastech kybernetických a hybridních hrozeb, jimž EU čelí; vyzývá Komisi, vysokou představitelku a členské státy, aby se pevně zavázaly k účinnému posílení SIAC;

51. naléhavě vyzývá členské státy, aby posílily sdílení zpravodajských informací, a to i se střediskem EU INTCEN a zpravodajským ředitelstvím Vojenského štábu Evropské unie (EUMS), a zároveň respektovaly svrchovanost členských států, zásadu „vědět jen to nejn nutnější“ a ochranu vnitrostátních utajovaných informací; zdůrazňuje, že je třeba, aby do plánování, řešení krizí a rozvoje politik EU byla systematicky zahrnována posouzení založená na zpravodajských informacích;
52. vyzývá orgány EU, aby ve spolupráci s členskými státy a ESVČ prozkoumaly bezpečný systém sdílení informací, které je „třeba vědět“ a „třeba sdílet“, v jehož rámci by EU působila jako zprostředkovatel propojující veřejné orgány, příslušné unijní, vnitrostátní a mezinárodní orgány, provozovatele kritické infrastruktury, soukromé společnosti a důvěryhodné zdroje informací o hrozbách s cílem posílit kolektivní informovanost o situaci a zároveň zajistit maximální ochranu citlivých informací; domnívá se, že takový systém by zúčastněné subjekty motivoval ke sdílení informací tím, že by jim umožňoval těžit z ucelenějšího přehledu hrozeb a kvalitnějších zpravodajských produktů a zároveň by vedl k postupnému budování důvěry potřebné pro smysluplné sdílení informací;
53. vyzývá k sestavení „černé knihy hybridní agrese ze strany Ruska, Číny a dalších zemí“ s cílem veřejně zdokumentovat každou hybridní operaci proti EU a jejím členským státům za posledních 10 let; trvá na tom, aby „černá kniha“ byla projednávána v Radě a každoročně předkládána Parlamentu s cílem uvalit na dotčené státy další náklady;

### ***Od roztříštěnosti ke koordinované a rozhodné evropské reakci***

54. zdůrazňuje, že účinně reagovat na stupňující se hybridní a konvenční hrozby může EU pouze prostřednictvím hlubší integrace, koordinace, zvýšené evropské obranné připravenosti a schopností, mimo jiné prostřednictvím dalšího rozvoje evropské technologické a průmyslové základny obrany;
55. domnívá se, že EU musí přejít od reaktivní k proaktivní strategii, tj. mimo jiné využívat své kapacity k eliminaci, odvracení a řešení hybridních hrozeb, a věrohodně zvýšit cenu, kterou bude třeba za nepřátelské akce zaplatit; zdůrazňuje, že každé porušení svrchovanosti členských států musí narazit na účinná, přiměřená a koordinovaná odvetná opatření;

56. zdůrazňuje, že aby bylo možné proti hybridním hrozbám účinně bojovat a odrazovat od nich, musí existovat sdílený a komplexní přehled hrozeb, který závisí na společných rámcích, metodikách, taxonomii a operačních normách; zdůrazňuje, že aby bylo možné hybridním operacím předcházet, odhalovat je, identifikovat a reagovat na ně, je třeba kombinovat diplomatická, právní, hospodářská a omezující opatření, včetně asymetrických opatření ve všech příslušných oblastech; vyzývá Komisi, vysokou představitelku a Radu, aby vypracovaly meziodvětvový akční plán proti hybridní válce, který by zahrnoval posílenou civilně-vojenskou spolupráci, operační scénáře a koordinované a efektivní protokoly reakce, včetně kalibrovaných odvetných možností EU úměrných závažnosti nepřátelských akcí a jasných řetězců reakce, které jsou interoperabilní s řetězcem NATO a doplňují je, a zároveň zachovávají schopnost EU a členských států jednat v případě potřeby nezávisle; vyzývá k určení jednotného koordinačního místa mezi Komisí a ESVČ s cílem zavést skutečně celounijní přístup k hybridním hrozbám;
57. vítá probíhající iniciativy na posílení operační kapacity, včetně týmů rychlé reakce EU na hybridní hrozby a zahájení Hlídky východního křídla EU a Iniciativy pro evropskou dronovou obranu; vyzývá k rychlému pokroku při jejich zavádění; zdůrazňuje strategický význam regionálních obranných a bezpečnostních klastrů a vyzývá k vytvoření zvláštních položek EU pro jejich financování, aby bylo možné začleňovat jejich know-how a kapacity do přeshraničních projektů, které zvyšují evropskou odolnost;
58. vítá oznámení Komise a vysoké představitelky o nové globální bezpečnostní strategii EU a vyzývá k tomu, aby komplexně řešila celé spektrum hybridních hrozeb;
59. trvá na tom, že je třeba urychleně pokračovat směrem ke skutečné evropské obranné unii jakožto silnějšímu evropskému pilíři NATO, který bude oddělitelný, ale nikoli oddělený, a který EU a jejím členským státům umožní jednat v případě potřeby nezávisle; vyzývá k rozšíření uvádění doložky o vzájemné obraně (čl. 42 odst. 7 SEU) do praxe v případech ozbrojené agrese a závažných hybridních scénářů; dále vyzývá k vypracování příručky týkající se čl. 42 odst. 7 – stručné, ale komplexní operační příručky pro vlády členských států a orgány EU, která by vysvětlovala, co se děje před aktivací tohoto článku některým členským státem, v jejím průběhu a poté; navrhuje, aby byla tato příručka pravidelně testována v situacích závažných hybridních krizí a prostřednictvím komplexních meziodvětvových cvičení;
60. zdůrazňuje, že některé z hybridních útoků Ruska proti EU a jejím členským státům mohou představovat státem podporovaný terorismus; vybízí členské státy, aby v boji proti těmto útokům využívaly všechny dostupné právní nástroje, včetně doložky solidarity

(článek 222 SFEU), a plně přitom využívaly mechanismy spolupráce a koordinace, které jsou při aktivaci této doložky k dispozici;

61. vítá práci odvedenou v rámci stávajících sankčních režimů zaměřených na hybridní činnosti, zejména sankčního režimu zavedeného v říjnu 2024, který se zaměřuje na destabilizační činnosti Ruska, a režimu horizontálních kybernetických sankcí zavedeného v roce 2019; vyjadřuje politování nad tím, že sankční rámec EU je složitý a roztržitý mezi různé typy hybridních hrozeb; vyzývá k dalšímu posílení restriktivních opatření EU v reakci na hybridní hrozby, včetně okamžitého vytvoření horizontálního sankčního rámce EU – speciálně navrženého pro hybridní hrozby s cílem zaplnit mezery ve stávajících režimech a zvýšit odrazující účinek –, který by existoval souběžně se sankčním režimem vůči Rusku za hybridní činnost s cílem zdůraznit aktivní zapojení Ruska do hybridních operací na globální úrovni a zároveň umožnit rychlejší a systematičtější uvalování sankcí na subjekty odpovědné za hybridní kampaně; vyzývá k dalšímu posílení a účinnějšímu využívání souboru nástrojů EU pro hybridní hrozby, zahraniční manipulaci s informacemi a vměšování a kybernetickou diplomacii;
62. zdůrazňuje, že je třeba zajistit vyvozování odpovědnosti za hybridní operace a trestání viníků, včetně zástupných sil jednajících jménem státních aktérů, a to s plným využitím stávajících a specializovaných nástrojů; vyzývá EU a členské státy, aby přijaly naléhavá opatření k zastavení a narušení finančních toků, které financují útoky na demokracii, mimo jiné zapojováním bankovních regulačních orgánů, orgánů činných v trestním řízení a sankčních orgánů s cílem sledovat a prověřovat nezákonné zdroje financování, včetně kryptoměn; vyzývá EU a její členské státy, aby odstranily finanční a algoritmické pobídky, které umožňují šíření dezinformací, a to i řešením vazeb mezi nezákonným financováním, příjmy z reklamy, obchodními modely platform založenými na upoutávání pozornosti a manipulativním obsahem;
63. zastává názor, že by měly být uplatňovány a případně dále rozvíjeny všechny trestněprávní nástroje dostupné na úrovni členských států a EU s cílem předcházet nezákonnému jednání, jehož cílem je narušovat demokratické instituce a procesy, a bojovat proti němu; zdůrazňuje, že je třeba, aby příslušné vnitrostátní orgány byly vybaveny vhodnými nástroji a komunikačními kanály pro prevenci, vyšetřování, odhalování a stíhání trestných činů souvisejících se zahraničním vměšováním; domnívá se, že korupce a zastrašování volených a veřejných činitelů zločineckými sítěmi by měly být řešeny v rámci reakce EU na hybridní hrozby, a to prostřednictvím posílené spolupráce mezi specializovanými protikorupčními agenturami, donucovacími orgány a příslušnými orgány Unie; žádá Komisi, aby posoudila přidanou hodnotu zavedení minimálních pravidel v právu EU týkajících se definice trestného činu vědomé účasti na organizované činnosti vměšování ve prospěch zahraničních mocností

a sankcí za tento trestný čin; konstatuje, že nadcházející revize mandátů agentur EU v oblasti spravedlnosti a vnitřních věcí je příležitostí k posílení akceschopnosti EU v operační oblasti; vyzývá Komisi, aby prozkoumala možnost vytvoření platformy nebo pracovní skupiny pro členské státy, v jejímž rámci by členské státy mohly na dobrovolné bázi koordinovat vnitrostátní legislativní reakce a sdílet osvědčené postupy;

### ***Zeměpisné aspekty***

64. důrazně odsuzuje účelové využívání migrace třetími zeměmi nebo nepřátelskými nestátními subjekty s cílem destabilizovat některý členský stát nebo vyvíjet tlak na EU; bere na vědomí zvláštní ustanovení o účelovém využívání migrace, která byla nedávno zahrnuta do klíčových právních předpisů EU; bere na vědomí skutečnost, že Komise oznámila revizi mandátu agentury Frontex; zdůrazňuje, že tato revize by měla poskytnout nezbytný právní základ, analytické kapacity a odpovídající potřebné lidské, finanční a technické zdroje, což by rovněž pomohlo posílit reakci EU na hybridní hrozby;
65. důrazně odsuzuje útok na jižní hranici EU ve městě Ceuta, k němuž došlo ve dnech 30. a 31. července 2026, i následnou invazi do Ceuty, která představuje útok na územní celistvost a svrchovanost členského státu; vyjadřuje nesouhlas s využíváním nelegálních migračních toků jako nástroje hybridní války namířené proti stabilitě a bezpečnosti členského státu, a vyzývá proto k nezávislému a komplexnímu vyšetřování, aby se vyjasnila odpovědnost za plánování a provedení tohoto útoku a zjistily sledované cíle;
66. důrazně odsuzuje systematické narušování vzdušného prostoru drony a přeshraniční provokace ze strany Ruska zaměřené na členské státy podél východního křídla EU jako promyšlenou kampaň s cílem zastrašit civilní obyvatelstvo; vítá sdělení Komise o východních regionech EU sousedících s Ruskem, Běloruskem a Ukrajinou a jeho výslovné uznání toho, že východní příhraniční regiony EU čelí strukturálním a trvalým hrozbám ze strany Ruska a Běloruska; vyzývá Komisi, aby toto uznání promítla do zvláštních toků financování v rámci víceletého finančního rámce na období 2028–2034, včetně vyčleněných finančních prostředků na posílení kapacit integrované ochrany hranic a modernizaci fyzické a digitální infrastruktury pro ostrahu hranic na vnějších pozemních hranicích EU v souladu se standardy NATO; zdůrazňuje, že je třeba se zaměřovat na pokročilé systémy detekce, monitorování a protipatření proti bezpilotním vzdušným systémům s cílem chránit kritickou infrastrukturu, jako jsou letiště, energetická zařízení a dopravní uzly, a podporovat členské státy při zavádění interoperabilních systémů pro sledování vzdušného prostoru, opatření elektronické ochrany a kapacit pro rychlou reakci na incidenty; zdůrazňuje, že opatření musí být přiměřená, defenzivní a

zaměřená na ochranu civilního obyvatelstva a musí zajišťovat kontinuitu základních služeb a svobodu pohybu v rámci schengenského prostoru;

67. zdůrazňuje, že hybridní hrozby mají na EU jako celek stále větší dopad, přičemž v různých regionech nabývají odlišných forem; v tomto ohledu zdůrazňuje vystavení pobaltského, seversko-baltského a černomořského regionu hrozbám namířeným proti námořní a vzdušné bezpečnosti, jakož i účelové využívání migrace, zranitelnost středomořských a jižních pohraničních regionů vůči hrozbám zaměřeným na námořní infrastrukturu, energetické sítě, logistické koridory, strategické dopravní trasy, dezinformační kampaně a účelové využívání migračních toků, vystavení jihovýchodní Evropy hospodářskému nátlaku, energetické závislosti a koordinované manipulaci s informacemi spojené s děním v sousedních regionech a specifickou zranitelnost velkých městských a digitálních informačních prostorů v celé EU vůči kognitivní válce, polarizaci a zahraničnímu vměšování; zdůrazňuje rostoucí strategický význam arktické oblasti pro evropskou bezpečnost, včetně ochrany kritické infrastruktury, svobody plavby, družicové komunikace a nově vznikajících dopravních koridorů; vyzývá EU a NATO, aby ve svých strategiích, včetně nadcházející bezpečnostní strategie EU, zohledňovaly geografické aspekty hybridních hrozeb a zároveň zachovaly 360stupňový přístup k bezpečnosti, pokud jde o odolnost, připravenost a reakci; zdůrazňuje, že financování boje proti hybridním hrozbám by mělo být založeno na míře strategického vystavení těmto hrozbám, operačních potřebách a prokázaných zranitelných místech, přičemž musí být zajištěna podpora všem regionům, které hybridním hrozbám čelí;

### ***Koordinace a spolupráce EU a NATO***

68. znovu potvrzuje, že NATO zůstává základním kamenem kolektivní obrany svých členů; vyzývá k prohloubení spolupráce mezi EU a NATO s cílem posílit evropskou připravenost, odolnost a odrazující účinek vůči hybridním hrozbám; v této souvislosti zdůrazňuje význam ochrany kritické infrastruktury, vojenské mobility, kybernetické odolnosti a připravenosti; zdůrazňuje potřebu systematictější výměny zkušeností získaných z války na Ukrajině v oblasti hybridních hrozeb;
69. zdůrazňuje, že činnost EU a NATO v oblasti hybridních hrozeb musí být doplňková, vzájemně se posilující a operativně koordinovaná, přičemž musí být zajištěna schopnost EU v případě potřeby jednat, a to na pozadí sladování minimálních požadavků EU na připravenost se základními požadavky NATO;
70. konstatuje, že revidovaná hybridní strategie NATO z roku 2025 znamená posun od odolnosti k aktivnímu odstrašování; vítá předem dohodnuté možnosti vojenské reakce a rozšířené pravomoci vrchního velitele spojeneckých sil v Evropě (SACEUR), které umožňují

rychlejší akci na začátku hybridního útoku, a zkracují tak prodlevu mezi odhalením hrozby a reakcí na ni, při současném zachování politického dohledu;

71. vítá mechanismus NATO pro sledování hybridních hrozeb, což je nástroj pro agregaci zpravodajských informací prostřednictvím společné zpravodajské a bezpečnostní divize NATO, který spojencům poskytuje konsolidovaný přehled o hrozbách na základě informací vnitrostátních zpravodajských služeb; uznává probíhající spolupráci mezi NATO a EU v oblasti zpravodajských služeb a vyzývá Komisi a ESVČ, aby v rámci střediska pro hybridní hrozby vytvořily strukturované rozhraní s tímto mechanismem, aby bylo pravidelně a systematicky sledováno situační povědomí EU a přehled NATO o hybridních hrozbách;
72. poukazuje na důležitou úlohu operací NATO Arktická stráž, Baltská stráž a Východní stráž jakožto flexibilních nástrojů pro reakci na hybridní hrozby v operačně relevantních časových rámcích, zejména pokud jde o ochranu námořní kritické infrastruktury a zásobovacích tras a o sledování hybridních činností v těchto regionech; konstatuje, že jejich účinnost omezují vysoké náklady na zachycování dronů, nedostatky v přehledu o situaci a roztržitost regulačních rámců pro boj proti dronům v jednotlivých členských státech; vyzývá k urychlenému provádění akčního plánu EU pro dronovou a protidronovou bezpečnost, včetně poskytnutí vyčleněných finančních prostředků na kapacity víceúrovňové obrany v členských státech v přední linii s cílem kineticky i elektronicky bojovat proti meteorologickým balonům a dronům, a k systematickému sledování tohoto akčního plánu s operačními požadavky NATO, čímž budou zajištěny harmonizované a dostatečně financované kapacity pro boj proti dronům ve všech členských státech; dále podporuje větší spolupráci při vývoji a zavádění nákladově efektivních protidronových technologií v celé Unii;
73. vítá rámec paralelních a koordinovaných cvičení EU-NATO (PACE) jako cenný nástroj pro testování a zlepšování společné kapacity, rozsahu a působnosti reakce a pro systematické začleňování získaných poznatků do politiky, plánování a institucionálního uspořádání EU; vyzývá k pravidelným cvičením EU a NATO simulujícím scénáře hybridních útoků, včetně sabotáží namířeným proti infrastruktuře vojenské mobility, koordinovaných kybernetických útoků, rozsáhlých kampaní zahraniční manipulace s informacemi a vměšování, narušování vzdušného prostoru a útoků na kritickou infrastrukturu;
74. vyzývá Komisi, ESVČ, aby v úzké koordinaci s NATO a členskými státy vypracovaly společné pojetí hybridních hrozeb a zavedly soudržný mechanismus reakce pro EU a NATO;

75. uznává cennou úlohu, kterou při posilování připravenosti, odolnosti, kybernetické obrany a schopnosti čelit hybridním hrozbám v celé Evropě hrají specializovaná střediska excelence, včetně Evropského střediska pro boj proti hybridním hrozbám v Helsinkách a střediska excelence NATO pro spolupráci v oblasti kybernetické obrany v Tallinnu; dále vítá činnost pracovní skupiny EU-NATO pro odolnost kritické infrastruktury, zejména při prohlubování spolupráce v oblasti energetiky, dopravy, digitální infrastruktury a podmořské konektivity;
76. vyzývá členské státy, aby harmonizovaly své právní předpisy s cílem odstranit právní mezery, které spojeneckému personálu brání v účasti na operacích proti hybridnímu působení pod prahem otevřeného konfliktu; vítá nedávno přijaté změny estonského zákona o organizaci obranných sil jako konkrétní krok tímto směrem;

### ***Partnerské země: spolupráce a podpora***

77. zdůrazňuje, že ruské hybridní operace mimo EU mají za cíl změnit zahraniční politiku třetích zemí v souladu se zájmy Moskvy, narušit vztahy EU s jejími partnery a oslabit mezinárodní podporu Ukrajiny; opakuje proto, že je důležité úzce spolupracovat s mezinárodními partnery a organizacemi s cílem zlepšit informovanost o situaci a účinněji předcházet hybridním hrozbám, odrazovat od nich a reagovat na ně; uznává význam prohlubování bilaterálních odvětvových dialogů a konzultací s podobně smýšlejícími partnery o hybridních hrozbách, zejména v rámci partnerství v oblasti bezpečnosti a obrany;
78. zdůrazňuje, že posílená spolupráce s Ukrajinou, Moldavskem, Arménií a partnery na západním Balkáně je strategickou nezbytností, neboť tyto země čelí neustálým útokům ze strany Ruska a představují klíčové testovací pole pro ruskou hybridní taktiku, která kombinuje zahraniční manipulaci s informacemi a vměšováním, kybernetické operace, síť skrytého vlivu, nátlak na energetiku a vliv založený na korupci s cílem oslabit demokratické instituce, společenskou soudržnost a vyhlídky na integraci do EU a NATO; vyzývá členské státy, aby přebíraly poznatky získané z těchto zemí a zavedly strukturované mechanismy pro systematickou výměnu osvědčených postupů a operačních zkušeností, mimo jiné pokud jde o schopnost Ukrajiny udržet základní služby, kontinuitu činnosti vlády, ochranu kritické infrastruktury, strategickou komunikaci a fungování a odolnost společnosti za neustálých útoků; opětovně vyjadřuje svou silnou podporu postupnému přistoupení Ukrajiny k EU a jejímu vstupu do NATO po splnění příslušných podmínek;
79. zdůrazňuje strategický význam pokračování a prohlubování podpory hybridní odolnosti poskytované kandidátským, potenciálním kandidátským a partnerským zemím, které jsou často primárními cíli ruských hybridních činností a jejichž odolnost přímo přispívá k

bezpečnosti EU; vítá aktivní příspěvek EU a členských států k posilování jejich odolnosti prostřednictvím nástroje zahraniční politiky, strategické komunikace, týmů rychlé reakce na hybridní hrozby, průzkumu hybridních rizik a misí SBOP v partnerských zemích, včetně Ukrajiny, Moldavska, Arménie a Černé Hory; vyzývá k pořádání pravidelných společných cvičení, simulačních scénářů a školicích programů zaměřených na zvyšování připravenosti, zlepšování kapacit rychlé reakce a podporu interoperability při řešení hybridních hrozeb; s uznáním bere na vědomí koordinovanou reakci EU a NATO v Moldavsku, včetně souběžného nasazení týmu EU pro reakci na hybridní hrozby a podpůrného týmu NATO pro boj proti hybridním hrozbám s doplňujícími se mandáty; vybízí kandidátské a potenciální kandidátské země, aby dosáhly plného souladu se společnou zahraniční a bezpečnostní politikou EU (SZBP), včetně omezujících opatření, což je klíčový aspekt procesu integrace do EU;

80. oceňuje proevropské síly v Moldavsku a Arménii za jejich demokratickou odolnost během parlamentních voleb v letech 2025 a 2026 i v období, které jim předcházelo, čímž prokázaly silný odpor vůči dlouhodobým ruským kampaním zaměřeným na zahraniční manipulaci s informacemi a vměšování; zdůrazňuje efektivitu přístupu celé vlády jakožto operačního modelu, včetně využití donucovacích opatření proti sítím, které provádějí hybridní operace ve prospěch Ruska; vyzývá členské státy a Komisi, aby ve spolupráci s ESVČ vypracovaly rámce na úrovni EU, které umožní přijímat srovnatelná opatření v oblasti prosazování práva; bere na vědomí důležitou roli, kterou hrají orgány EU, státní instituce, občanská společnost a nezávislá média v boji proti zahraniční manipulaci s informacemi a vměšování, včetně rozsáhlých koordinovaných kampaní zaměřených na manipulaci s informacemi za využití umělé inteligence, což přispívá k pozoruhodně vysoké úrovni povědomí veřejnosti o hybridních hrozbách;
81. vyzývá k posílené spolupráci v oblasti hybridních hrozeb s podobně smýšlejícími partnery mimo EU, zejména se Spojeným královstvím a Norskem jakožto klíčovými evropskými bezpečnostními partnery, jakož i s Kanadou, Japonskem, Korejskou republikou, Austrálií, Novým Zélandem, Tchaj-wanem a dalšími podobně smýšlejícími partnery, mimo jiné prostřednictvím partnerství v oblasti bezpečnosti a obrany, sdílení informací a spolupráce v oblasti kybernetiky, námořní bezpečnosti, vesmíru a odolnosti, pokud je to možné; zdůrazňuje, že státy EHP/ESVO a jejich obranný průmysl by měly být plně zahrnuty do rámců EU pro odolnost proti hybridním hrozbám a programů pro rozvoj schopností, čímž by byl uznán jejich přímý přínos k evropské bezpečnosti a společné vystavení hybridním hrozbám;
82. vyjadřuje politování nad tím, že nedávný posun v politice USA oslabil společnou frontu demokracií v době sílících hybridních hrozeb;

zdůrazňuje, že transatlantická jednota zůstává pro boj proti nim zásadní;

83. zdůrazňuje, že ruské vlivové operace v Africe, Latinské Americe a Karibiku nejsou pro evropskou bezpečnost okrajovou záležitostí, neboť se snaží narušit partnerství EU, oslabit podporu Ukrajiny a podkopat evropskou diplomacii, bezpečnostní pomoc a rozvojovou spolupráci; konstatuje, že v Africe tyto operace většinou spoléhají na státní média a kulturní a náboženské fronty, zatímco v Latinské Americe a Karibiku Rusko vybudovalo španělskojazyčný vlivový ekosystém, který doplňuje jeho protievropský narativ v jiných částech světa; vyzývá EU a členské státy, aby posílily strategickou komunikaci, podporovaly nezávislé a důvěryhodné místní sdělovací prostředky, angažovaly důvěryhodné místní hlasy a posílily spolupráci s partnery v obou regionech s cílem odhalovat nepřátelské informační operace a bojovat proti nim;
84. zdůrazňuje význam zkušeností států Perského zálivu, Jordánska a dalších příslušných partnerů při řešení hybridních vlivových sítí spojených s Muslimským bratrstvem, a to i prostřednictvím přístupů zaměřených na správu věcí veřejných, regulaci a společenskou odolnost, a vyzývá ke strukturované výměně osvědčených postupů s těmito partnery s cílem prohloubit chápání hybridních hrozeb ze strany EU, zlepšit politické reakce a zintenzivnit spolupráci v boji proti zahraničnímu vměšování a současně respektovat základní práva a rozmanitost právních a politických systémů;
85. konstatuje, že Tchaj-wan má s obranou proti hybridním útokům Číny a zahraniční manipulaci s informacemi a vměšování bohaté zkušenosti; oceňuje komplexní tchajwanský model v oblasti odolnosti, včetně zřízení výboru pro obranu a odolnost celé společnosti, rozsáhlého výcviku v oblasti civilní obrany, spolupráce s organizacemi občanské společnosti, sítí digitální odolnosti a iniciativ usilujících o připravenost veřejnosti; zdůrazňuje, že zkušenost Taiwanu ukazuje, že společenská odolnost není druhořadým aspektem obrany, ale ústředním pilířem národní bezpečnosti, zejména pokud se hybridní nátlak zaměřuje na kritickou infrastrukturu, důvěru veřejnosti a sociální soudržnost; vyzývá k pravidelným výměnám mezi EU a jejími tchajwanskými protějšky o příslušných bezpečnostních otázkách a k užší spolupráci v tomto ohledu v boji proti zahraniční manipulaci s informacemi a vměšování a kognitivní válce, ochraně kritické infrastruktury a podmořských kabelů a posilování odolnosti celé společnosti mezi EU a Tchaj-wanem; vyzývá EU, aby rozšířila obchodní a průmyslovou spolupráci s Tchaj-wanem, zejména v oblasti technologicky vyspělých součástí a strategických technologií, které mají zásadní význam pro odolnost a bezpečnost základní infrastruktury a dodavatelských řetězců, včetně polovodičů, telekomunikačních zařízení 5G/6G, dronů a zboží dvojího užití; zdůrazňuje rovněž, že je třeba Tchaj-wanu a Ukrajině

poskytnout IRIS<sup>2</sup> (družicová infrastruktura pro odolnost, propojení a bezpečnost);

◦

◦ ◦

86. pověřuje svou předsedkyni, aby předala toto usnesení Radě, vysoké představitelce a Komisi.