



Zittingsdocument

A10-0212/2026

20.7.2026

VERSLAG

over de hybride oorlogvoering en de bescherming van de territoriale integriteit
en de kritieke beveiligings- en defensie-infrastructuur van de EU
(2026/2024(INI))

Commissie veiligheid en defensie

Rapporteur: Rasa Juknevičienė

INHOUD

	Blz.
ONTWERPRESOLUTIE VAN HET EUROPEES PARLEMENT	3
TOELICHTING	29
BIJLAGE: BEKENDMAKING VAN INPUT	32
INFORMATIE OVER DE GOEDKEURING IN DE BEVOEGDE COMMISSIE	33
HOOFDELIJKE EINDSTEMMING IN DE BEVOEGDE COMMISSIE	34

ONTWERPRESOLUTIE VAN HET EUROPEES PARLEMENT

over de hybride oorlogvoering en de bescherming van de territoriale integriteit en de kritieke beveiligings- en defensie-infrastructuur van de EU

(2026/2024(INI))

Het Europees Parlement,

- gezien het VN-Handvest en de fundamentele beginselen van het internationaal recht,
- gezien titel V van het Verdrag betreffende de Europese Unie (VEU), en met name hoofdstuk 2, afdeling 2, over de bepalingen inzake het gemeenschappelijk veiligheids- en defensiebeleid,
- gezien het Verdrag betreffende de werking van de Europese Unie (VWEU),
- gezien op artikel 42, lid 7, en artikel 222 VEU,
- gezien zijn eerdere resoluties over Oekraïne, Rusland en Belarus, met name die welke zijn aangenomen sinds de annexatie door Rusland van het schiereiland de Krim in februari 2014 en de grootschalige invasie van Oekraïne door Rusland in februari 2022,
- gezien het internationale rechtskader voor het voorkomen en bestrijden van terrorisme, met inbegrip van resolutie 2341 van de VN-Veiligheidsraad over de bescherming van kritieke infrastructuur tegen terroristische daden, aangenomen op 13 februari 2017,
- gezien Verordening (EU) 2019/452 van het Europees Parlement en de Raad van 19 maart 2019 tot vaststelling van een kader voor de screening van buitenlandse directe investeringen in de Unie¹,
- gezien het “Strategisch kompas voor veiligheid en defensie – Voor een Europese Unie die haar burgers, waarden en belangen beschermt en bijdraagt aan de internationale vrede en veiligheid”, zoals aangenomen door de Raad op 21 maart 2022 en bekrachtigd door de Europese Raad op 25 maart 2022,
- gezien de conclusies van de Raad van 21 juni 2022 over een kader voor een gecoördineerde EU-respons op hybride campagnes,
- gezien Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad van 14 december 2022 betreffende de weerbaarheid van kritieke entiteiten en tot intrekking van Richtlijn 2008/114/EG van de Raad²,
- gezien het definitieve beoordelingsverslag van de EU-NAVO-taskforce van 29 juni 2023 over de veerkracht van kritieke infrastructuur,
- gezien het rapport van Sauli Niinistö van 30 oktober 2024 getiteld “Safer Together —

¹ PB L 79 I van 21.3.2019, blz. 1, ELI: <http://data.europa.eu/eli/reg/2019/452/oj>.

² PB L 333 van 27.12.2022, blz. 164, ELI: <http://data.europa.eu/eli/dir/2022/2557/oj>.

Strengthening Europe's Civilian and Military Preparedness and Readiness" (Samen veiliger — Versterking van de civiele en militaire paraatheid en gereedheid van Europa) (rapport-Niinistö),

- gezien de mededeling van de Commissie van 11 december 2024 over de bestrijding van hybride dreigingen die voortvloeien uit de inzet van migratie als wapen, en de versterking van de veiligheid aan de buitengrenzen van de EU ([COM\(2024\) 570](#)),
- gezien Verordening (EU) 2025/37 van het Europees Parlement en de Raad van 19 december 2024 tot wijziging van Verordening (EU) 2019/881 wat betreft beheerde beveiligingsdiensten³,
- gezien Verordening (EU) 2025/38 van het Europees Parlement en de Raad van 19 december 2024 tot vaststelling van maatregelen ter versterking van de solidariteit en de capaciteit in de Unie om cyberdreigingen en -incidenten op te sporen, zich erop voor te bereiden en erop te reageren en tot wijziging van Verordening (EU) 2021/694 (verordening cybersolidariteit)⁴,
- gezien de gezamenlijke mededeling van de Commissie en de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid van 21 februari 2025 getiteld "EU-actieplan inzake kabelbeveiliging" (JOIN(2025)0009),
- gezien zijn resolutie van 12 maart 2025 over het witboek over de toekomst van de Europese defensie⁵,
- gezien het gezamenlijke witboek van de Commissie en de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid van 19 maart 2025 getiteld "Gezamenlijk witboek over de gereedheid van de Europese defensie 2030" (JOIN(2025)0120),
- gezien de gezamenlijke mededeling van de Commissie en de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid van 26 maart 2025 over de strategie voor een paraatheidsunie (JOIN(2025)0130),
- gezien de mededeling van de Commissie van 1 april 2025 aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's over ProtectEU: een Europese strategie voor interne veiligheid ([COM\(2025\) 0148 final](#)),
- gezien de verklaring van de top van de Noord-Atlantische Raad in Den Haag, aangenomen door de staatshoofden en regeringsleiders die op 25 juni 2025 aan de vergadering van de Noord-Atlantische Raad hebben deelgenomen,
- gezien zijn resolutie van 9 oktober 2025 over een eendrachtig antwoord op recente Russische schendingen van het luchtruim en bedreigingen van kritieke infrastructuur van de EU-lidstaten⁶,

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

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

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

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

- gezien de bijdrage van de Italiaanse minister van Defensie van november 2025 getiteld “Countering hybrid warfare: an active strategy”,
 - gezien het voorstel van de Commissie van 10 december 2025 betreffende richtsnoeren voor de trans-Europese energie-infrastructuur ([COM\(2025\)1006](#)),
 - gezien zijn resolutie van 18 december 2025 over de voortdurende hybride aanvallen van Belarus op Litouwen⁷,
 - gezien de mededeling van de Commissie van 18 februari 2026 over de oostelijke regio’s van de EU die grenzen aan Rusland, Belarus en Oekraïne ([COM\(2026\)0082](#)),
 - gezien zijn resolutie van 21 januari 2026 over de uitvoering van het gemeenschappelijk veiligheids- en defensiebeleid — jaarverslag 2025⁸,
 - gezien de conclusies van de Raad van 16 maart 2026 over het versterken van het vermogen van de Europese Unie om hybride dreigingen tegen te gaan,
 - gezien artikel 55 van zijn Reglement,
 - gezien het verslag van de Commissie veiligheid en defensie (A10-0212/2026),
- A. overwegende dat de intensiteit en reikwijdte van hybride aanvallen op de EU sinds het begin van de Russische aanvalsoorlog tegen Oekraïne aanzienlijk zijn toegenomen, waarbij incidenten herhaaldelijk in verband worden gebracht met autoritaire staten, met name Rusland, Belarus, China, Iran en Noord-Korea;
 - B. overwegende dat Rusland de grootste en voornaamste veiligheidsdreiging vormt voor de EU en haar lidstaten; overwegende dat Rusland het beginsel van territoriale integriteit en politieke onafhankelijkheid als bedoeld in artikel 2, lid 4, van het Handvest van de VN voortdurend heeft geschonden; overwegende dat hybride aanvallen een bedreiging vormen voor de democratie in de EU en haar lidstaten;
 - C. overwegende dat de ernst van deze aanvallen drastisch is toegenomen en dat deze een flagrante schending van de soevereiniteit van de lidstaten, de territoriale integriteit van de EU en het internationaal recht vormen; overwegende dat hybride oorlogvoering een structureel kenmerk van het huidige geopolitieke klimaat is geworden;
 - D. overwegende dat recente hybride aanvallen kunnen bestaan uit het ongeoorloofd binnendringen van het luchtruim met drones, “smokkelballonnen”, schendingen van het luchtruim, voor infiltratie en smokkel gebruikte clandestiene tunnels, sabotage en spionage van kritieke veiligheids- en defensie-infrastructuur, sabotage van onderzeese kabels en energie-infrastructuur, verstoring van gps-signalen en spoofing van navigatiesystemen, cyberaanvallen, brandstichtings- en moordcomplotten, het instrumentalisieren van migratie en georganiseerde misdaad, het inzetten van politieke en economische elites, niet-transparante buitenlandse investeringen, economische dwang, gegevensdiefstal en andere gevallen van politieke ondermijning en het verzwakken van de vijand via economische weg, buitenlandse informatiemanipulatie en

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

⁸ Aangenomen teksten, P10_TA(2026)0013.

inmenging (FIMI), en inmenging in politieke en electorale processen;

- E. overwegende dat de soevereiniteit en territoriale integriteit van alle lidstaten fundamentele beginselen van de EU zijn; overwegende dat vijandige overheidsactoren, in het bijzonder Rusland, de territoriale integriteit van de EU op twee fronten aanvallen: door rechtstreekse fysieke aanvallen op lidstaten en door beïnvloedingsoperaties die erop gericht zijn de eenheid van de EU te ondermijnen, door lidstaten ertoe aan te zetten zich uit de EU terug te trekken;
- F. overwegende dat hybride dreigingen weliswaar in toenemende mate een zorg worden voor de EU als geheel, met inbegrip van landen en gebieden overzee zoals Groenland, maar dat de regio's aan de buitengrenzen van de EU en de maritieme gebieden van de EU in het bijzonder kwetsbaar zijn voor aanvallen; overwegende dat deze aanvallen ook gericht zijn op kandidaat-lidstaten en buurlanden van de EU, met name Oekraïne, Moldavië, Armenië, Georgië en de Westelijke Balkan; overwegende dat de territoriale integriteit van de buurlanden van de EU van cruciaal belang is voor het waarborgen van vrede, stabiliteit en veiligheid in Europa en de rest van de wereld;
- G. overwegende dat de inmenging van niet-EU-landen in Groenland, met name door middel van opruiende taal en hybride acties op Groenlands grondgebied, alsook de expliciete dreigingen die de Amerikaanse regering tegen de soevereiniteit van Groenland heeft geuit, aanleiding zijn voor bezorgdheid over de soevereiniteit en de territoriale integriteit van Groenland;
- H. overwegende dat Georgië een voorbeeld is van succesvolle Russische hybride inmenging die ertoe heeft geleid dat de autoriteiten onder leiding van de Georgische Droom, dat het Kremlin gunstig gezind is, Ruslands draaiboek van hybride operaties tegen het eigen maatschappelijk middenveld en de democratische instellingen van Georgië hebben overgenomen;
- I. overwegende dat sabotageactiviteiten door Russische inlichtingendiensten steeds vaker worden uitgevoerd met behulp van tussenpartijen, kwetsbare groepen in de samenleving, met inbegrip van minderjarigen, gelieerde actoren en agenten voor eenmalige inzet, waardoor het moeilijker wordt verantwoordelijken aan te wijzen en een respons te formuleren; overwegende dat religieuze instellingen, waaronder de Russische orthodoxe kerk en netwerken die banden hebben met de Moslimbroederschap, zijn misbruikt om inmengingsoperaties in de EU uit te voeren met het oog op ondermijning van democratische waarden, de rechtsstaat en het vermogen van de EU om zichzelf te verdedigen;
- J. overwegende dat deze aanvallen niet alleen tot doel hebben chaos te creëren en de lidstaten van de EU te destabiliseren, maar ook om de democratische integriteit te ondermijnen, besluitvormingsprocessen te manipuleren, politieke verschillen te vergroten, sociale cohesie te verzwakken, angst alsook wantrouwen ten aanzien van de overheid te zaaien onder EU-burgers, en de defensiegereedheid en de steun van de EU aan Oekraïne te verzwakken, hetgeen in de hele EU een domino-effect teweegbrengt;
- K. overwegende dat het invoeren van artikel 5 van het NAVO-Verdrag na de terreuraanslagen van 9/11 laat zien dat collectieve verdediging naar aanleiding van een aanval niet alleen kan worden geactiveerd door acties van een statelijke actor, maar ook door aanslagen waarbij niet-statale actoren en complexe, internationaal opererende

netwerken betrokken zijn; overwegende dat dit precedent de veranderende aard van veiligheidsdreigingen onderstreept, alsook de noodzaak om de mechanismen voor collectieve respons dienovereenkomstig aan te passen, onder meer met verbeterde gemeenschappelijke normen en procedures voor toerekening;

- L. overwegende dat cognitieve oorlogvoering samen met FIMI drastisch is toegenomen; overwegende dat volgens het vierde jaarverslag van de Europese Dienst voor extern optreden (EDEO) over FIMI-dreigingen de Russische FIMI-activiteiten in 2026 naar verwachting zullen toenemen, waarbij het budget voor door de staat gecontroleerde media naar verwachting ongeveer 1,56 miljard EUR zal bedragen, 7 % hoger dan in 2025, en waarbij de Oostzee- en de Arctische regio naar verwachting tot de voornaamste doelwitten zullen behoren;
- M. overwegende dat FIMI-operaties gebruikmaken van geavanceerde cognitieve psychologische methoden, waaronder reflexieve controle, een techniek die zijn oorsprong heeft in de militaire theorie van de Sovjet-Unie en die specifieke informatie-input introduceert om de gepercipieerde keuzemogelijkheden van een doelwit te beperken en beslissingen in de richting van de strategische doelstellingen van de initiator te sturen;
- N. overwegende dat de nationale veiligheidsstrategieën van Rusland van 2015 en 2021 het kader vormen voor het stimuleren van zogenaamde traditionele waarden en de “Russische wereld” als zijnde instrumenten van de bredere strategie voor hybride oorlogvoering en geopolitieke invloed; overwegende dat Rusland in het kader van zijn strategie voor hybride oorlogvoering op strategische wijze historische, religieuze, culturele narratieven als ook een waardennarratief heeft ingezet om het publieke debat en de kerkelijke dynamiek te beïnvloeden, de sociale cohesie te verzwakken en democratische veerkracht en trans-Atlantische integratie te ondermijnen;
- O. overwegende dat, gezien de transversale aard van het cognitieve domein, cognitieve indicatoren volledig moeten worden geïntegreerd in het gemeenschappelijk operationeel beeld dat wordt gebruikt door instanties op het gebied van cyberbeveiliging, inlichtingendiensten, rechtshandhaving, het leger en kritieke infrastructuur;
- P. overwegende dat het succes van moderne militaire operaties en de doeltreffendheid van overheidsinstellingen in toenemende mate afhangen van de controle over cyberspace en van het strategische gebruik van digitale middelen en informatiesystemen;
- Q. overwegende dat interne veiligheid weliswaar een verantwoordelijkheid van de lidstaten blijft, maar dat er in het licht van het grensoverschrijdende, onderling verweven en multidimensionale karakter van dergelijke hybride aanvallen versterkte samenwerking, systematische informatie-uitwisseling en gecoördineerde actie op EU-niveau nodig zijn, ondersteund door toereikende financiering en aangevuld met langetermijnstrategieën voor het versterken van de maatschappelijke weerbaarheid en het beschermen van de institutionele integriteit;
- R. overwegende dat de EU-agentschappen op het gebied van justitie en binnenlandse zaken in samenwerking met de nationale autoriteiten een sleutelrol moeten spelen bij de totstandbrenging en handhaving van een gemeenschappelijk situationeel bewustzijn van de risico's in verband met dergelijke dreigingen en bij de verlening van bijstand aan lidstaten in de frontlinie in crisissituaties; overwegende dat de Commissie de

versterking van het Europees Grens- en kustwachtagentschap (Frontex) heeft opgenomen in haar vlaggenschipinitiatieven voor de zittingsperiode 2024-2029, naast een herziening van de mandaten van het Agentschap van de Europese Unie voor samenwerking op het gebied van rechtshandhaving (Europol) en het Agentschap van de Europese Unie voor justitiële samenwerking in strafzaken (Eurojust); overwegende dat andere initiatieven, zoals de “oostflankwacht”, kunnen helpen om de bescherming van de buitengrenzen te versterken en de weerbaarheid tegen hybride dreigingen te vergroten;

- S. overwegende dat de opkomst van geavanceerde AI-systemen de bestaande cyberbeveiligingsarchitecturen structureel verstoort, waardoor in de afgelopen decennia ontwikkelde dreigingsmodellen en aannames over defensie, niet langer opgaan; overwegende dat vijandige statelijke en niet-statelijke actoren reeds de mogelijkheden van AI benutten om de snelheid, omvang en precisie van hybride operaties te vergroten, waaronder cyberinbraken, AI-vergiftiging, desinformatiecampagnes en aanvallen op kritieke infrastructuur; overwegende dat de collectieve cyberweerbaarheidskaders van de EU moeten worden aangepast om deze nieuwe kwetsbaarheden aan te pakken;
- T. overwegende dat, ondanks de aanzienlijke inspanningen van de lidstaten en de ontwikkeling van instrumenten en mechanismen om hybride dreigingen tegen te gaan, de respons van de EU op hybride aanvallen nog steeds te lijden heeft onder lacunes in de wetgeving, het gebrek aan een geharmoniseerde aanpak tussen de lidstaten, verschillende niveaus van bewustzijn en het ontbreken van een specifieke structuur of entiteit om dergelijke aanvallen te monitoren; overwegende dat de EU-lidstaten als gevolg daarvan en ondanks de urgentie nog geen volledig gecoördineerde en coherente respons op hybride oorlogvoering hebben ontwikkeld, zowel individueel als op Europees niveau en in voorkomend geval samen met de NAVO;
- U. overwegende dat nationale defensie-uitgaven baat zouden hebben bij meer coördinatie en bundeling tussen de lidstaten of bij verdere investeringen in Europese samenwerkingsprojecten; overwegende dat aanzienlijke verhogingen van de defensie-uitgaven van de lidstaten, in combinatie met de defensie-initiatieven van de EU, zoals SAFE en andere maatregelen in het kader van het programma 2030 voor de gereedheid van de Europese defensie, de al lang bestaande capaciteitstekorten beginnen te verhelpen, maar dat een snellere omzetting in concrete operationele vermogens nodig is om de EU, haar lidstaten en hun burgers beter te beschermen tegen hybride dreigingen; overwegende dat er op dit gebied nog potentieel is voor het gebruik van technologieën voor tweërlei gebruik; overwegende dat er voorts verdere maatregelen nodig zijn op het gebied van de interne veiligheid;
- V. overwegende dat de verantwoordelijkheid voor nationale veiligheid primair bij de lidstaten ligt, en dat alle op EU-niveau gecoördineerde of voorgestelde maatregelen en initiatieven moeten worden ingekaderd en uitgevoerd met volledige inachtneming van de exclusieve bevoegdheden van de lidstaten en moeten worden afgestemd op de EU-instrumentaria inzake hybride dreigingen, FIMI en cyberdiplomatie;
- W. overwegende dat de afhankelijkheid van de EU van buitenlandse actoren en in het buitenland vervaardigde technologieën in kritieke infrastructuur en toeleveringsketens, met inbegrip van de inkoop van grondstoffen uit derde landen, een van de belangrijkste kwetsbaarheden van de EU vormt en een grote uitdaging is voor de veiligheid en

strategische autonomie van Europa;

- X. overwegende dat de huidige veiligheidssituatie van de EU wordt gekenmerkt door de afwezigheid van zowel vrede als openlijk gewapend conflict, maar een voorstadium van oorlogvoering is waarin tegenstanders hybride instrumenten inzetten om de discrepantie te benutten tussen de bestuursstructuren van de EU voor vreedstijd en de daadkracht die nodig is voor afschrikking en respons; overwegende dat de bestaande kaders voor het buitenlands en veiligheidsbeleid van de EU, die zijn ingesteld op het bereiken van consensus via beraadslaging, structurele vertraging veroorzaken die door tegenstanders actief wordt uitgebuit; overwegende dat deze “tussen”-situatie een fundamentele herziening vereist van de besluitvormingsarchitectuur van de EU op veiligheids- en defensiegebied;
- Y. overwegende dat geloofwaardige afschrikking niet alleen berust op de materiële vermogens en de technologische voorsprong van de Europese en geallieerde strijdkrachten, maar dat politieke wil, strategische samenhang en een gemeenschappelijk begrip van de dreiging daarbij de doorslag geven; overwegende dat de hybride strategie van Rusland erop gericht is juist deze kwaliteiten te ondermijnen — door ambiguïteit aan te wakkeren, verdeeldheid te stoken en druk uit te oefenen zonder dat een gewapend conflict in gang wordt gezet — teneinde de geloofwaardigheid van collectieve defensie-inzet aan te tasten nog voordat gewapend conflict daadwerkelijk aan de orde is;

Hybride oorlogvoering: tussen oorlog en vrede

- 1. benadrukt dat hybride operaties opzettelijke, gecombineerde, door inlichtingen gestuurde en gecoördineerde handelingen van staten zijn — onder meer via niet-overheidsactoren, tussenpartijen en gelieerde actoren — die meerdere domeinen tegelijkertijd bestrijken; benadrukt dat deze zo zijn opgezet dat ze lijken op geïsoleerde incidenten en onder de drempel van een gewapend conflict blijven, maar wel in potentie gevolgen hebben die vergelijkbaar zijn met die van traditionele agressie, waardoor het aanzienlijk moeilijker wordt verantwoordelijkheid toe te schrijven en er doeltreffend tegen op te treden; verzoekt de EU en de lidstaten daarom te erkennen dat hybride acties een vorm van oorlogvoering kunnen vormen, ongeacht of er gebruik wordt gemaakt van conventioneel geweld;
- 2. benadrukt dat hybride oorlogvoering in de eerste plaats tot doel heeft de EU en haar lidstaten te destabiliseren, verdelen en ondermijnen door systemische kwetsbaarheden uit te buiten, de grondvesten van hun veiligheid, weerbaarheid en democratie te verzwakken, alsmede hun defensiegereedheid, door de industriële defensiebasis en kritieke infrastructuur van de EU te verstoren, publieke en politieke steun voor de defensie van de EU te ondermijnen en via systematische inmenging in democratische processen de politieke krachten die welwillend zijn tegenover de daders te versterken;
- 3. bevestigt dat Rusland, rechtstreeks of via meerdere gelieerde machten waaronder Belarus, de overheidsactor is waarvan de meest ernstige hybride dreiging uitgaat richting de EU en haar lidstaten; merkt op dat China, Iran, Noord-Korea en andere landen hybride campagnes hebben gevoerd om de Europese democratieën te ondermijnen en de veiligheidsbelangen van de EU uit te hollen; onderstreept dat de EU een alomvattende aanpak ten opzichte van hybride dreigingen moet hanteren die niet

alleen gericht is op Russische en Belarussische activiteiten, maar ook op de groeiende strategische rol van China, Iran en Noord-Korea bij het faciliteren en versterken van vijandige acties die gericht zijn tegen de belangen en veiligheid van Europa; constateert met bezorgdheid dat niet-statelijke actoren — waaronder terroristische groepen, georganiseerde misdaadnetwerken, oligarchische en kleptocratische netwerken, religieuze instituties en geloofsnetwerken, particuliere militaire bedrijven, extremistische bewegingen en actoren die tegen betaling aan beïnvloeding doen — ook hybride campagnes tegen Europese democratieën kunnen uitvoeren of faciliteren;

4. verzoekt de Commissie en de Raad de toereikendheid van de bestaande rechtskaders van de EU voor de aanpak van hybride dreigingen te beoordelen, vastgestelde lacunes op te vullen en hybride operaties die nog geen gewapend conflict vormen en die niet door middel van rechtshandhaving alleen kunnen worden aangepakt, te behandelen als collectieve veiligheidskwesties die een gecombineerde civiel-militaire respons vereisen;

Informatieoorlog, cognitieve veiligheid en maatschappelijke weerbaarheid

5. onderstreept dat informatieoorlogvoering een van de kernelementen van hybride oorlogvoering is; uit zijn bezorgdheid over de toenemende omvang van cognitieve oorlogvoering in combinatie met FIMI, die tot doel heeft het maatschappelijk vertrouwen in democratische instellingen uit te hollen, polarisatie te vergroten en democratische besluitvorming en de publieke steun voor de Europese veiligheid en defensie, met inbegrip van steun voor Oekraïne, te ondermijnen;
6. benadrukt dat bovengenoemde doelen (zie paragraaf 5) voornamelijk worden nagestreefd door middel van geraffineerde en gecoördineerde operaties die op meerdere domeinen van het maatschappelijke leven kunnen treffen, en dat daarbij strategische cognitieve en psychologische technieken worden ingezet die zijn bedacht om besluitvormingsprocessen, individuele en collectieve perceptie, identiteitsvorming, culturele normen, historisch geheugen, morele kaders en religieuze overtuigingen te beïnvloeden, waarbij technologische infrastructuur, het medialandschap en economische en politieke kwetsbaarheden worden uitgebuit; stelt met bezorgdheid vast dat FIMI-operaties gebruikmaken van geavanceerde cognitief-psychologische methoden, waaronder reflexieve controle, die moeilijk op te sporen, toe te schrijven of tegen te gaan zijn met een conventionele respons; benadrukt daarom dat in de FIMI-toolkit van de EU uitdrukkelijk tegenmaatregelen tegen dergelijke geavanceerde beïnvloedingstechnieken moeten worden opgenomen teneinde de integriteit van de besluitvorming van de EU te waarborgen;
7. waarschuwt dat afzonderlijke gewapende incidenten de aanleiding kunnen vormen, of opzettelijk kunnen worden geësceneerd als dekmantel, voor onmiddellijke, gesynchroniseerde en gecoördineerde FIMI-operaties, waarbij vijandige actoren de tijdspanne voordat officiële verklaringen worden uitgebracht, benutten om de publieke perceptie te beïnvloeden; dringt erop aan deze informatiekloof terdege aan te pakken middels versterkte Europese coördinatie, met name door de publiek-private coördinatie in het informatiedomein te verbeteren; benadrukt dat er gemeenschappelijke instrumenten moeten worden ontwikkeld, zoals communicatiedraaiboeken die snellere, gecoördineerde en nauwkeurige communicatie mogelijk maken voordat vijandige narratieven de informatieruimte verzadigen;

8. uit zijn bezorgdheid over het gebruik door Rusland van historisch revisionisme, met name met betrekking tot de Tweede Wereldoorlog en de erfenis van de Sovjet-Unie, FIMI, en de selectieve herinterpretatie van historische gebeurtenissen als instrumenten van hybride oorlogvoering die gericht is op het polariseren van de publieke opinie, het ondermijnen van de maatschappelijke cohesie en de democratische veerkracht, en het delegitimiseren van de territoriale integriteit van soevereine staten;
9. onderstreept dat FIMI niet beperkt blijft tot traditionele media, maar zich ook uitstrekt tot onderwijs, cultuur en religie; wijst op het strategische gebruik van religieuze instituties en geloofsnetwerken, waaronder de instrumentalisering van de Russisch-Orthodoxe Kerk, om moreel gezag uit te stralen, door de staat gepropageerde narratieven te verspreiden en de maatschappelijke veerkracht en de democratische cohesie geleidelijk te ondermijnen; verzoekt de EU voorts hybride dreigingen die gebruikmaken van religieuze kanalen op te sporen en EU-ambtenaren op te leiden in interreligieuze betrekkingen en kennis van religies, en in het identificeren van financiële beïnvloeding, organisatorische overname en informatiemanipulatie die democratische waarden en sociale cohesie ondermijnen;
10. veroordeelt het gebruik van onlineplatforms door vijandige actoren voor hybride activiteiten; dringt aan op een strengere handhaving van de bestaande EU-regels inzake de transparantie van aanbevelingssystemen, politieke reclame, gecoördineerd niet-authentiek gedrag en de snelle verspreiding van gemanipuleerde of door AI gegenereerde inhoud in verband met vijandige buitenlandse inmenging;
11. onderstreept dat vijandige actoren steeds geavanceerdere en adaptieve hybride technieken gebruiken; benadrukt dat AI-tools — deepfakes, algoritmische versterking en netwerken van geautomatiseerde accounts — dergelijke beïnvloedingsoperaties sneller, goedkoper en moeilijker op te sporen maken; is van mening dat de respons van de EU op door AI gefaciliteerde FIMI eruit moet bestaan deze te behandelen als zowel een dreigingsvector als een kritiek defensievermogen;
12. merkt op dat de respons van de EU op FIMI reactief is, waarbij realtime monitoring, toerekening en proactieve responscapaciteiten ontbreken; dringt erop aan dat FIMI moet worden behandeld als een ernstige bedreiging voor de veiligheid die een operationele aanpak en betere coördinatie en samenwerking tussen lidstaten op alle niveaus vereist, met inbegrip van vroegtijdige opsporing, toereikende responsopties en een betere bescherming van de democratische processen, met name in verkiezingstijd;
13. is ingenomen met de werkzaamheden van de EDEO op het gebied van het monitoren en opsporen van en reageren op FIMI en onderstreept het belang van het EU-systeem voor snelle waarschuwingen (RAS) voor een gecoördineerde gezamenlijke respons op desinformatie; verzoekt de Commissie en de lidstaten kennis te nemen van de aanbevelingen van de Bijzondere Commissie inzake het Europees schild voor de democratie (EUDS) en hiermee aan de slag te gaan; dringt erop aan het systeem voor snelle waarschuwingen verder te versterken om informatiemanipulatie in realtime aan te pakken, met duidelijke operationele verantwoordelijkheden; dringt aan op gestandaardiseerde preventie- en snellereactiemechanismen in de hele EU en met partnerlanden, met inbegrip van gestructureerde communicatiekanalen voor vroegtijdige waarschuwing; pleit voor de ontwikkeling van proactieve strategische communicatie-instrumenten waarmee de bevolking vooraf kan worden gewaarschuwd voor verwachte

desinformatietactieken, narratieve patronen en verzonden inhoud in de aanloop naar cruciale gebeurtenissen zoals verkiezingen, onderhandelingen over energiebeleid of veiligheids crises;

14. verzoekt de Commissie, de hoge vertegenwoordiger en de lidstaten voorts het FIMI-instrumentarium volledig operationeel te maken en op consistente en gecoördineerde wijze te benutten en het FIMI-afschrikkingshandboek toe te passen, onder meer door middel van gecoördineerde, openbare toerekening en, in voorkomend geval, het gebruik van beperkende maatregelen, waarbij niet alleen losse incidenten worden aangepakt, maar ook de illegale geldstromen, de technische infrastructuur en de netwerken van tussenpersonen en gelieerde groeperingen die FIMI-operaties ondersteunen;
15. benadrukt dat de Europese publieke opinie een primair doelwit blijft van Russische hybride operaties; herinnert eraan dat decennia van vrede omstandigheden van strategische zelfgenoegzaamheid hebben gecreëerd die door vijandelijke beïnvloedingsoperaties worden uitgebuit en verdiept; is van mening dat regeringen en EU-instellingen een gedeelde verantwoordelijkheid hebben om het publiek te informeren over de aard en de nabijheid van de hybride dreiging, en dat door het nalaten hiervan de paraatheid en afschrikking van binnenuit worden ondermijnd;
16. verzoekt de lidstaten een overheidsbrede en maatschappijbrede aanpak te hanteren, waarbij prioriteit wordt gegeven aan veerkracht en paraatheid, zoals benadrukt in het rapport-Niinistö; herinnert eraan dat hybride dreigingen gericht zijn op de samenleving als geheel, aangezien vijandige actoren gebruikmaken van kwetsbaarheden ten aanzien van allerlei gebieden, diensten, gemeenschappen en informatieruimten die onderling met elkaar in verband staan; is van mening dat vertrouwen en sociale cohesie van fundamenteel belang zijn voor maatschappelijke weerbaarheid; onderstreept daarom dat weerbaarheid tegen hybride dreigingen verder moet gaan dan militaire, technische en institutionele maatregelen door overheidsinstanties, de particuliere sector, het maatschappelijk middenveld — met inbegrip van lokale gemeenschappen en moeilijk te bereiken groepen — de academische wereld en onafhankelijke media samen te brengen om het democratische vertrouwen, het publieke bewustzijn en de maatschappelijke paraatheid te versterken en zo een nieuwe Europese veiligheidscultuur te bevorderen;
17. benadrukt dat burgers beter bestand moeten worden gemaakt tegen FIMI door middel van burgerschapsvorming, mediageletterdheid, strategische communicatie, steun aan onafhankelijke media, met inbegrip van onderzoeksjournalistiek, fact-checkers zoals het Europees Waarnemingscentrum voor digitale media, en tools die met behulp van AI op grote schaal desinformatiecampagnes opsporen en analyseren; dringt aan op nauwere samenwerking met de media en audiovisuele actoren bij het opsporen van FIMI, het aanwijzen van verantwoordelijken en bij de respons; dringt erop aan de opsporing, analyse en toerekening van FIMI, alsook veilige mechanismen voor gegevensuitwisseling en interoperabele systemen voor vroegtijdige waarschuwing te stimuleren, onder meer door middel van publiek-private initiatieven;
18. uit zijn bezorgdheid over de aanhoudende meldingen van buitenlandse inmenging in Europese verkiezingen, onder meer door middel van cyberaanvallen en door AI gefaciliteerde desinformatie; herinnert eraan dat de integriteit en weerbaarheid van verkiezingsprocessen de kern vormen van de democratische grondslagen van de EU en een belangrijk doelwit vormen van hybride operaties; benadrukt dat FIMI vaak

toeneemt in verkiezingstijd en dat voortdurende waakzaamheid en coördinatie daarom essentieel zijn om de integriteit van verkiezingen en democratische stabiliteit in de EU en in partnerlanden, met inbegrip van kandidaat-lidstaten en potentiële kandidaat-lidstaten, te waarborgen; is ingenomen met de gezamenlijke mededeling “Europees schild voor de democratie: zorgen voor sterke en veerkrachtige democratieën” en de oprichting van het Europees Centrum voor democratische veerkracht en dringt aan op een duidelijke omschrijving van de taken ervan om overlapping met bestaande initiatieven te voorkomen;

19. dringt erop aan cognitieve kwetsbaarheden in de context van hybride oorlogvoering te erkennen en aan te pakken in de komende veiligheidsstrategie van de EU en verzoekt de Commissie verdere stappen te ondernemen door cognitieve kwetsbaarheden in kaart te brengen en benchmarks inzake weerbaarheid vast te stellen;

Cyberbeveiliging

20. benadrukt dat cyberaanvallen een centraal element van hybride campagnes zijn geworden, waarbij misbruik wordt gemaakt van de toenemende digitalisering van kritieke sectoren zoals de gezondheidszorg, de financiële sector en energie, en cascaderende verstoringen worden veroorzaakt met mogelijk ernstige economische en maatschappelijke gevolgen;
21. merkt op dat cyberspace het vijfde militaire domein en een centrale facilitator van hybride dreigingen is geworden; onderstreept dat cyberbeveiliging, gelet op de toenemende mate waarin militaire platforms, kritieke infrastructuur en commando-, controle-, communicatie- en inlichtingensystemen afhankelijk zijn van digitale technologieën, van essentieel belang is voor operationele superioriteit en weerbaarheid in alle domeinen; benadrukt daarom dat er soevereine cybervermogens nodig zijn op het gebied van opsporing, toerekening, respons en inlichtingen, met inbegrip van offensieve vermogens om dreigingen te neutraliseren en te zorgen voor een geloofwaardige afschrikking;
22. onderstreept de samenhang tussen FIMI en cyberbeveiliging, en merkt op dat cyberaanvallen vaak plaatsvinden in de vroege stadia van FIMI-campagnes; dringt erop aan mechanismen ter bestrijding van FIMI systematisch te koppelen aan cyberbeveiligingscapaciteit om gecoördineerde manipulatie-infrastructuur in een vroeg stadium op te sporen, de verantwoordelijkheid ervoor toe te schrijven en te verstoren;
23. waarschuwt voor de risico's van convergerende cyberoperaties, waarbij door staten aangestuurde actoren zich actief de operationele profielen, methoden en persona's van onafhankelijke activistische hackers of commercieel gemotiveerde cybercriminelen eigen maken, zodat niet duidelijk is wie er achter de operatie zit, en hun cyberactiviteiten laten samenvallen met geopolitieke gebeurtenissen, verkiezingen of gevechtsoperaties; benadrukt dat bij de respons op hybride cyberdreigingen een duidelijk onderscheid moet worden gemaakt tussen legitieme vormen van politieke meningsuiting of maatschappelijk ongenoegen en financieel gemotiveerde cybercriminaliteit en door staten aangestuurde operaties, teneinde de fundamentele vrijheden te beschermen en tegelijkertijd de toerekening, verantwoordingsplicht en afschrikking te verbeteren;

24. waarschuwt dat de uitbreiding van het internet der dingen het risico vergroot dat cyberaanvallen fysieke gevolgen hebben voor kritieke infrastructuur en essentiële diensten, en dringt aan op verplichtingen inzake beveiliging als ontwerpprincipe om ervoor te zorgen dat verbonden apparaten geen toegangspunten worden voor hybride operaties met gevolgen in de fysieke omgeving;
25. waarschuwt dat volledige cyberbescherming niet bestaat en dat een mentaliteitsverandering in de richting van cyberweerbaarheid nodig is; benadrukt dat de cyberweerbaarheid van Europa moet worden opgebouwd aan de hand van frequente en realistische cyberoefeningen; onderstreept dat cyberweerbaarheid niet alleen betrekking heeft op systemen, maar ook op gegevensbescherming, hetgeen tegelijkertijd doelwit en facilitator van hybride dreigingen is; onderstreept voorts dat de cyberweerbaarheid in het gehele economische weefsel van Europa moet worden versterkt, met inbegrip van kleine en middelgrote ondernemingen (kmo's) en aanbieders van essentiële digitale diensten;
26. benadrukt dat de EU aanzienlijke toegevoegde waarde biedt door lidstaten te helpen nationale capaciteiten te koppelen, een gemeenschappelijk situationeel bewustzijn op te bouwen en een snellere, meer samenhangende respons op hybride dreigingen te faciliteren; beveelt de Commissie aan voorstellen te onderzoeken om te komen tot een meer uniform kader ter ondersteuning van lidstaten bij de planning, operationele coördinatie en uitvoering van cyberoperaties; is ingenomen met het project in het kader van de permanente gestructureerde samenwerking (PESCO) inzake het coördinatiecentrum voor het cyber- en informatiedomein (CIDCC) en het voorstel voor een EU-coördinatiecentrum voor cyberdefensie (EU CDCC);
27. dringt aan op verdere harmonisatie van de verplichtingen inzake het melden van incidenten en van belangrijke juridische begrippen in de EU-kaders voor cyberbeveiliging en weerbaarheid, teneinde fragmentatie tegen te gaan, de interoperabiliteit te verbeteren en ervoor te zorgen dat een snel herstel van essentiële diensten een belangrijke prioriteit blijft in hybride-crisesscenario's;
28. erkent de EU-cyberbeveiligingsreserve, die in het kader van de verordening cybersolidariteit wordt beheerd door het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa), als een strategische EU-capaciteit voor snelle cyberrespons; dringt erop aan de financiering ervan af te stemmen op de operationele behoefte en benadrukt dat de eerste inzet ervan in Moldavië een belangrijke stap is geweest in het versterken van de operationele cyberweerbaarheid van de EU en de steun aan partnerlanden; verzoekt de cyberbeveiligingsautoriteiten van de lidstaten om gestructureerde samenwerking te bevorderen met de vertrouwde aanbieders van de cyberbeveiligingsreserve, teneinde de beschikbare incidentresponscapaciteit ten volle te benutten wanneer zich hybride dreigingen voordoen in de vorm van significante of grootschalige cyberincidenten;
29. wijst nogmaals op het belang van en dringt aan op voldoende EU-middelen voor de snellereactieteams bij cyberincidenten van PESCO als zijnde een permanente cyberdefensiecapaciteit die kan worden ingezet op verzoek van lidstaten, partnerlanden en missies in het kader van het gemeenschappelijk veiligheids- en defensiebeleid (GVDB) die te maken hebben met cyberaanvallen met gevolgen voor de veiligheid en defensie;

30. herhaalt dat het belangrijk is ten volle gebruik te maken van het instrumentarium voor cyberdiplomatie om cyberdreigingen en kwaadwillige cyberactiviteiten te voorkomen, te ontmoedigen en erop te reageren; neemt kennis van de lancering in maart 2026 van het eerste permanente mondiale VN-mechanisme voor cyberbeveiliging, en is van mening dat de EU moet focussen op gebieden die een duidelijke Europese toegevoegde waarde vertegenwoordigen, en tegelijkertijd de Europese cyberdiplomatie verder moet versterken;
31. benadrukt dat cyberweerbaarheid en defensieve maatregelen ontoereikend zijn om een geloofwaardige afschrikking tegen hybride dreigingen te waarborgen, zoals benadrukt in het gezamenlijk witboek 2030 over de gereedheid van de Europese defensie; verzoekt de Commissie en de lidstaten om in samenwerking met de NAVO de juridische, procedurele en operationele voorwaarden voor evenredige, juridisch conforme cybertegenmaatregelen te onderzoeken; herhaalt zijn standpunt waarin wordt opgeroepen tot de onverwijlde oprichting van het EU CDCC en dringt aan op de snelle uitvoering van een mandaat in overeenstemming met de conclusies van de Raad over het EU-beleid inzake cyberdefensie, teneinde een geloofwaardigere en slagvaardigere cyberdefensie voor de EU tot stand te brengen;
32. waarschuwt in dit verband dat AI niet alleen een instrument is dat bij hybride cyberactiviteiten wordt gebruikt, maar ook een kritieke technologie is die zelf doelwit kan worden, kan worden gemanipuleerd of gecompromitteerd door middel van de invoering van prompts, de vervuiling van trainingsgegevens en aanvallen op de toeleveringsketen; benadrukt dat de EU, gezien de toenemende afhankelijkheid van commerciële en voor tweërlei doeleinden gebruikte AI-systemen in civiele, veiligheids- en defensiesituaties, een duidelijk standpunt moet ontwikkelen over de cyberbeveiliging, weerbaarheid en het beheer van AI voor tweërlei gebruik, met inbegrip van waarborgen voor de integriteit van modellen, betrouwbare toeleveringsketens en toezicht op het snijvlak tussen civiele, defensie- en nationale veiligheidstoepassingen;
33. benadrukt de noodzaak van betere bescherming van kritieke publieke digitale infrastructuur en door de overheid beheerde registers met gevoelige gegevens, zoals verkiezingsinfrastructuur, aangezien dit potentiële doelwitten zijn van hybride dreigingen, gezien de rol van die infrastructuur ten aanzien van digitale identiteit, openbaar bestuur, gegevensbeheer, beveiligde communicatie, toegang tot essentiële diensten en de integriteit van democratische processen;

Kritieke infrastructuur

34. veroordeelt de hybride aanvallen op kritieke onderdelen van de infrastructuur in de EU — met name energie-, vervoers-, communicatie- en satellietinfrastructuur, waaronder die voor militaire mobiliteit — als zijnde kritieke facilitators en strategische goederen voor de collectieve defensie, veerkracht en civiele bescherming van de EU; wijst erop dat deze kritieke infrastructuur functioneert als een systeem met vele onderlinge verbindingen, dat niet afzonderlijk kan worden beschermd, en hoe meer digitale verbindingen er zijn des te groter de kwetsbaarheid van het systeem; is ingenomen met de focus op bescherming en weerbaarheid van infrastructuur voor energie en militaire mobiliteit in het voorstel van de Commissie voor een verordening inzake militaire mobiliteit ([COM\(2025\)0847](#)) en in het voorstel van de Commissie betreffende

richtsnoeren voor de trans-Europese energie-infrastructuur ([COM\(2025\)1006](#)); verzoekt de Europese Commissie en de lidstaten alle nodige maatregelen te nemen om de bescherming van kritieke infrastructuur te waarborgen;

35. onderstreept dat de ruimte een steeds belangrijker strijdtoneel voor hybride oorlogvoering is geworden, waarbij vijandige actoren satellietgebaseerde communicatie, navigatie- en observatiesystemen aanvallen door middel van cyberoperaties, fysieke aanvallen, signaalverstoring en spoofing; benadrukt dat verstoring van in de ruimte gestationeerde infrastructuur aanzienlijke gevolgen kan hebben voor de civiele veiligheid, de kritieke infrastructuur, de militaire mobiliteit en de crisisresponscapaciteit van de EU; dringt daarom aan op versterking van de weerbaarheid van EU-ruimtesystemen, onder meer in de vorm van een vergroot situationeel bewustzijn inzake de ruimte, bescherming van grondinfrastructuur, cyberbeveiligingseisen, beveiliging van de toeleveringsketen, regelmatige oefeningen en alternatieve of reserve PNT-vermogens (plaatsbepaling, navigatie en tijdsbepaling); dringt voorts aan op de integratie van het ruimtedomein in het bredere EU-kader voor de bestrijding van hybride dreigingen;
36. merkt op dat vijandige actoren, met name Rusland, energie-infrastructuur, energiemarkten en energieafhankelijkheid steeds meer als wapen gebruiken om politieke druk uit te oefenen; benadrukt het strategische belang van kritieke energie-infrastructuur voor zowel defensie- als civiele behoeften; dringt er bij de Commissie en de EU-lidstaten op aan een rechtskader en, onder het volgende meerjarig financieel kader 2028-2034, een financieel kader voor de EU vast te stellen dat zorgt voor voldoende bescherming en weerbaarheid van kritieke energie-infrastructuur, waarbij de voorstellen van de Commissie voor richtsnoeren voor de trans-Europese energie-infrastructuur ([COM\(2025\)1006](#)) en de Connecting Europe Facility ([COM\(2025\) 0547](#)) met voorrang behandeld worden;
37. veroordeelt de activiteiten van de Russische schaduwvloot die het risico op ongevallen op zee vergroten, door staten aangestuurde sabotage verbergen en kritieke infrastructuur zoals onderzeese kabels, offshore-energie-installaties en havenfaciliteiten in gevaar brengen; dringt aan op betere monitoring, inspectie en handhavingsmaatregelen in de Europese wateren en verzoekt de EU haar respons op hybride dreigingen in maritieme zones op te voeren; moedigt de Commissie aan om — naar voorbeeld van het veiligheidsinitiatief tegen proliferatie — juridische en operationele kaders te onderzoeken die het mogelijk maken aan boord te gaan van schepen die tot een schaduwvloot behoren, en verzoekt de Financiële-actiegroep verder onderzoek te doen naar de rol van ondoorzichtige eigendomsstructuren, vlagregisters en bijbehorende financiële netwerken bij het faciliteren van de omzeiling van sancties en van illegale geldstromen;
38. benadrukt dat onderzeese kabels een belangrijke strategische kwetsbaarheid en een doelwit van hybride sabotage-, spionage- en beïnvloedingsoperaties vormen, vanwege hun fysieke blootstelling en mogelijkheid tot het veroorzaken van systemische verstoring, aangezien het overgrote deel van het intercontinentale internetverkeer over deze kabels loopt; prijst de aanbeveling van de Commissie van 2024 over veilige en weerbare onderzeese kabelinfrastructuren⁹ en de gezamenlijke mededeling van 2025

⁹ Aanbeveling (EU) 2024/779 van de Commissie van 26 februari 2024 over veilige en weerbare onderzeese kabelinfrastructuren (PB L, 2024/779, 8.3.2024, ELI: <http://data.europa.eu/eli/reco/2024/779/oj>).

over het EU-actieplan inzake kabelbeveiliging (JOIN(2025)0009) als belangrijke eerste stappen om de beveiliging en weerbaarheid van onderzeese kabelinfrastructuur te versterken; dringt voorts aan op situationele bewustzijnsvermogens op zee, waarbij gegevens van satellieten, sensoren aan het oppervlak en onder water worden geïntegreerd voor de opsporing, monitoring en toerekening van fysieke dreigingen voor onderzeese-kabel- en offshore-energie-infrastructuur in strategische maritieme gebieden, waaronder de Oostzee, de Noordzee, de Zwarte Zee, het noordpoolgebied en het Middellandse zeegebied; pleit voor strenge bepalingen inzake strafrechtelijke aansprakelijkheid om dergelijke aanvallen te ontmoedigen, alsook voor reservesystemen om de weerbaarheid te waarborgen; benadrukt voorts de noodzaak van een alomvattende benadering met meerdere lagen op basis van een combinatie van technologische innovatie, verbeterde inlichtingenintegratie, verbeterde toerekeningsvermogens en verbeterde samenwerking tussen de NAVO, de EU-lidstaten en relevante actoren uit de particuliere sector teneinde onderzeese infrastructuur op coherente wijze te kunnen beschermen;

39. verzoekt de Commissie en de lidstaten te komen tot een gecoördineerde, EU-brede interpretatie van het VN-Zeerechtverdrag (Unclos) teneinde te zorgen voor een coherent optreden en een doeltreffende strafrechtelijke benadering en doeltreffende afschrikking ten aanzien van hybride activiteiten, sabotage en schendingen van soevereine rechten in de maritieme gebieden van de EU, met name in de Oostzee, en herinnert daarbij aan de doelstelling van Unclos om een vreedzaam gebruik van de zee te waarborgen; spoort de Commissie en de lidstaten aan om een voorbeeld te nemen aan Australië, waar “kabelbeschermingszones” zijn ingesteld, waardoor wettelijke waarborgen gelden en schade aan onderzeese kabels buiten de territoriale zee grens van twaalf zeemijl strafbaar is gesteld, in combinatie met actieve monitoring, surveillance en respons in samenwerking met relevante partners uit derde landen;
40. verzoekt de lidstaten en het Europees Defensieagentschap (EDA) voortgang te maken met de PESCO-projecten “Critical Seabed Infrastructure Protection” (CSIP), “Harbour & Maritime Surveillance and Protection” (HARMSPRO), “Integrated Multi-Layer Air and Missile Defence System” (IMLAMD) en “Counter Unmanned Aerial System” (C-UAS) om de surveillance-, opsporings- en defensievermogens tegen bedreigingen vanuit de lucht en vanaf zee te versterken; verzoekt de Commissie om in samenwerking met de hoge vertegenwoordiger en in overleg met de lidstaten een Europees defensieproject van gemeenschappelijk belang voor te stellen dat gericht is op de geïntegreerde verdediging van het maritieme milieu en de zeebodem;
41. is ingenomen met de aanneming van de richtlijn betreffende de weerbaarheid van kritieke entiteiten (CER-richtlijn)¹⁰ en de NIS 2-richtlijn¹¹ als belangrijke stappen voor het versterken van de weerbaarheid tegen hybride aanvallen, maar benadrukt dat verdragen bij de uitvoering in de lidstaten een gezamenlijk en urgent kwetsbaar punt vormen, en dringt aan op volledige en tijdige uitvoering; dringt er bij de Commissie op

¹⁰ Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad van 14 december 2022 betreffende de weerbaarheid van kritieke entiteiten en tot intrekking van Richtlijn 2008/114/EG van de Raad (PB L 333 van 27.12.2022, blz. 164, ELI: <http://data.europa.eu/eli/dir/2022/2557/oj>).

¹¹ Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn) (PB L 333 van 27.12.2022, blz. 80, ELI: <http://data.europa.eu/eli/dir/2022/2555/oj>).

aan haar monitorings- en handhavingsbevoegdheden ten volle in te zetten; verzoekt de lidstaten om weerbaarheid als ontwerpprincipie als standaardvereiste op te nemen in alle nieuwe en herziene wetgeving;

42. is bezorgd over buitenlandse — met name Russische en Chinese — eigendom van kritieke infrastructuur in de EU, welke het risico op spionage en inmenging en strategische afhankelijkheid aanzienlijk vergroot; is ingenomen met het politieke akkoord dat het Parlement en de Raad hebben bereikt over een versterkt EU-screeningmechanisme voor directe buitenlandse investeringen; verzoekt de lidstaten spoedig uitvoering te geven aan deze verordening, waar mogelijk aangevuld met een “koop Europees”-benadering voor kritieke infrastructuur en defensiematerieel, teneinde de strategische autonomie van de EU te versterken;
43. erkent dat een aanzienlijk deel van de kritieke infrastructuur die verband houdt met essentiële openbare diensten en militaire capaciteiten in particulier bezit is of door particulieren wordt geëxploiteerd; dringt aan op permanente en gestructureerde kaders voor publiek-private samenwerking, onder meer voor informatie-uitwisseling, noodplanning en gecoördineerde crisisrespons; benadrukt dat, wanneer essentiële diensten en gevoelige gegevens worden ondersteund door particuliere infrastructuur, overheidsinstanties moeten zorgen voor doeltreffende regelgevende en operationele controle; dringt erop aan dat defensievereisten systematisch worden geïntegreerd in de planning, het ontwerp en de financiering van civiele infrastructuur; benadrukt dat door de EU gefinancierde infrastructuur aan voor defensie relevante weerbaarheidsnormen moet voldoen als voorwaarde voor EU-steun; dringt er bovendien op aan ontwikkelaars van defensietechnologie en aanbieders van beveiligingsdiensten systematisch te betrekken bij de vroege fasen van de dreigingsanalyse en de noodplanning voor kritieke infrastructuur, en ervoor te zorgen dat de beschikbare technologische vermogens worden meegenomen in de weerbaarheidskaders op nationaal en EU-niveau; erkent de bijdrage van kmo's, start-ups en aanbieders van innovatieve technologie aan de weerbaarheid en bescherming van kritieke infrastructuur, en roept ertoe op hen nauwer te betrekken bij desbetreffende programma's, aanbestedingsregelingen en publiek-private partnerschappen van de EU;
44. verzoekt de lidstaten om regelmatig paraatheids- en weerbaarheidsoefeningen voor kritieke infrastructuur uit te voeren, ook in de vorm van gezamenlijke oefeningen, en met spoed de in het witboek voor de Europese defensie genoemde prioritaire vermogens te realiseren, met name lucht- en raketverdediging, drones en antidronesystemen, militaire mobiliteit, cyber- en elektronische oorlogvoering en maritieme capaciteiten;
45. is bezorgd over het feit dat de EU structureel afhankelijk is van niet-EU-landen met een hoog risico, met name China, voor de levering van netwerkhardware en -software, zoals omvormers voor zonne-energie, windturbines, verbonden voertuigen en digitale consumentenapparaten, die op afstand toegang hebben tot systemen, systemen kunnen aansturen en er gegevens mee kunnen uitwisselen, en daardoor een aanzienlijk veiligheidsrisico vormen; verzoekt de Commissie voorts de beoordelingen van de beveiliging van de toeleveringsketen systematisch uit te breiden tot alle kritieke infrastructuursectoren, en meer vaart te zetten achter de inspanningen om strategische afhankelijkheden te verminderen; verzoekt de lidstaten gevolg te geven aan deze beoordelingen, toeleveringsketens te diversifiëren en bij voorkeur te werken met gelijkgestemde leveranciers in strategische sectoren wanneer dat uit

veiligheidsoverwegingen nodig is; is verheugd over het feit dat de voorgestelde herziening van de cyberbeveiligingsverordening tot doel heeft een kader te bieden voor het verbieden van op netwerken aangesloten componenten van risicovolle leveranciers, en dat de strategische routekaart voor digitalisering en AI in de energiesector — als onderdeel van het pakket voor technologische soevereiniteit — voorziet in een herziening van het kader voor de energievoorzieningszekerheid; dringt erop aan dat deze maatregelen snel worden vastgesteld;

46. benadrukt dat het belangrijk is de aanvoerroutes te diversifiëren door middel van veilige en weerbare vervoersnetwerken met betrouwbare partners om strategische afhankelijkheden te verminderen en de economische veiligheid en weerbaarheid van de toeleveringsketens van de EU te versterken;
47. benadrukt dat kritieke en opkomende technologieën, met inbegrip van AI, cloudinfrastructuur, geavanceerde halfgeleiders, kwantumtechnologieën, cyber, ruimte, autonome systemen en beveiligde communicatie, behoren tot de kritieke veiligheidsinfrastructuur van de EU, gelet op hun essentiële rol in defensiegereedheid, economische weerbaarheid en operationele continuïteit; beschouwt een weerbare, concurrerende digitale infrastructuur van de EU — met inbegrip van veilige lokale datacentra, een soevereine EU-cloud, edgecomputing en gigabitnetwerken — als een belangrijke pijler van de Europese veiligheid; benadrukt dat het vermogen van de EU om hybride campagnes op te sporen, te weerstaan en erop te reageren afhankelijk is van haar vermogen om deze technologieën te ontwikkelen, te bemachtigen en op te schalen binnen een weerbare Europese industriële en technologische basis die wordt gesteund met voldoende EU-investeringen, met inbegrip van investeringen in veilige, interoperabele en weerbare systemen voor informatie-uitwisseling en lokale datacentra die niet onder extraterritoriale wetgeving vallen;

Situationeel bewustzijn

48. benadrukt dat een doeltreffende bestrijding van hybride dreigingen preventie, vroegtijdige dreigingsanticipatie en voortdurende monitoring van strategische kwetsbaarheden vereist om vijandige acties te neutraliseren voordat zij systemische effecten hebben, alsook een gedeeld dreigingsbeeld, aangezien sectoren die worden aangevallen niet doeltreffend kunnen reageren op basis van verslagen van losstaande incidenten; wijst in dit verzoek op de, in potentie, unieke toegevoegde waarde van de EU bij het verzamelen van grensoverschrijdende gegevens om patronen van gecoördineerde hybride campagnes op te sporen die geen enkele lidstaat alleen zou kunnen identificeren, alsook bij het coördineren van de ontwikkeling van procedures voor gezamenlijk situationeel bewustzijn en gezamenlijke toerekening, gemeenschappelijke kaders, methodologieën, taxonomieën, interoperabiliteitsprotocollen tussen de EU en relevante nationale organen, en structuren ter ondersteuning van de operationele samenwerking tussen de lidstaten; dringt erop aan dat deze functies formeel worden erkend als coördinatie- en ondersteuningsbevoegdheden van de EU;
49. merkt op dat de EU-Fusiecel voor analyse van hybride dreigingen binnen de gezamenlijke capaciteit op het gebied van inlichtingenanalyse (SIAC) het centrale orgaan van de EU is met exclusieve expertise inzake de analyse van hybride dreigingen op basis van alle informatiebronnen, dat door inlichtingen gevoed situationeel

bewustzijn biedt; herhaalt dat de SIAC het enige knooppunt voor inlichtingen in de EU-instellingen moet zijn en onderstreept de bijzondere status ervan binnen de veiligheidsarchitectuur van de EU; beschouwt “Hybrid Trend Analysis” als een essentieel instrument voor de analyse van hybride dreigingen en het opsporen van patronen, en pleit ervoor dit instrument echt in te zetten in de beleidsvormingsprocessen;

50. herinnert aan de gebrekkige voortgang bij de verwezenlijking van de doelstelling van het strategisch kompas en het gezamenlijke document van de hoge vertegenwoordiger en de lidstaten over de versterking van de gezamenlijke EU-capaciteit op het gebied van inlichtingenanalyse (EEAS(2024) 2014) om SIAC te versterken door aanvullende middelen toe te wijzen voor het opstellen, analyseren en integreren van relevante informatie met het oog op de verschaffing en facilitering van een efficiënt inlichtingenaanbod met betrekking tot cyber- en hybride dreigingen waarmee de EU geconfronteerd wordt; verzoekt de Commissie, de hoge vertegenwoordiger en de lidstaten zich er stellig toe te verbinden om de gezamenlijke EU-capaciteit op het gebied van inlichtingenanalyse echt te versterken;
51. dringt er bij de lidstaten op aan meer inlichtingen uit te wisselen, onder meer met EU-Intcen en het directoraat Inlichtingen van de Militaire Staf van de Europese Unie (EUMS), met inachtneming van de soevereiniteit van de lidstaten, het “need-to-know”-beginsel en de bescherming van nationale gerubriceerde informatie; benadrukt dat gegevensgestuurde, op inlichtingen gebaseerde beoordelingen systematisch moeten worden opgenomen in de planning, het crisisbeheer en de beleidsontwikkeling van de EU;
52. verzoekt de EU-instellingen om samen met de lidstaten en de EDEO onderzoek te doen naar een veilig systeem voor informatie-uitwisseling op “need-to-know”- en “need-to-share”-basis, waarbij de EU zou fungeren als facilitator die overheidsinstanties, betrokken EU-, nationale en internationale organen, exploitanten van kritieke infrastructuur, particuliere bedrijven en betrouwbare bronnen van dreigingsinformatie met elkaar verbindt, teneinde het collectieve situationele bewustzijn te versterken en tegelijkertijd gevoelige informatie optimaal te beschermen; is van mening dat een dergelijk systeem de deelnemende instanties zou stimuleren om informatie te delen, doordat zij daarmee kunnen profiteren van een volledig dreigingsbeeld en van hoogwaardiger inlichtingenproducten, terwijl tegelijkertijd geleidelijk het vertrouwen wordt opgebouwd dat nodig is voor betekenisvolle informatie-uitwisseling;
53. dringt aan op de creatie van een zwartboek van hybride agressie door Rusland, China en anderen, waarin elke hybride operatie tegen de EU en haar lidstaten van de afgelopen tien jaar openbaar wordt gedocumenteerd; dringt aan op bespreking van het zwartboek in de Raad en een jaarlijkse presentatie ervan in het Parlement met als doel de betrokken staten verdere kosten op te leggen;

Van fragmentatie tot een gecoördineerde en doortastende Europese respons

54. onderstreept dat de EU alleen doeltreffend kan reageren op escalerende hybride en conventionele dreigingen door middel van diepere integratie, coördinatie, grotere Europese defensiegereedheid en defensievermogens, onder meer door de Europese technologische en industriële defensiebasis verder te ontwikkelen;

55. is van mening dat de EU moet overgaan van een reactieve naar een proactieve strategie, wat onder meer inhoudt dat zij haar vermogens inzet om hybride dreigingen te verstoren, te ontmoedigen en erop te reageren, en om de kosten van vijandig optreden op geloofwaardige wijze te verhogen; benadrukt dat elke schending van de soevereiniteit van de lidstaten met doeltreffende, evenredige en gecoördineerde vergeldingsmaatregelen moet worden beantwoord;
56. benadrukt dat voor een doeltreffende bestrijding en afschrikking van hybride dreigingen een gedeeld en alomvattend dreigingsbeeld nodig is, dat afhankelijk is van gemeenschappelijke kaders, methoden, taxonomieën en operationele normen; benadrukt dat diplomatieke, juridische, economische en beperkende maatregelen moeten worden gecombineerd om hybride operaties te voorkomen, op te sporen, te identificeren, toe te rekenen en erop te reageren, onder meer door middel van asymmetrische maatregelen op alle relevante gebieden; verzoekt de Commissie, de hoge vertegenwoordiger en de Raad een domeinoverschrijdend actieplan tegen hybride oorlogvoering te ontwikkelen, met inbegrip van versterkte civiel-militaire samenwerking, operationele draaiboeken, collaboratieve en efficiënte responsprotocollen, waaronder gekalibreerde vergeldingsopties voor de EU die in verhouding staan tot de ernst van vijandige activiteiten en duidelijke responsketens die interoperabel zijn met en een aanvulling vormen op die van de NAVO, met behoud van het vermogen van de EU en de lidstaten om indien nodig onafhankelijk op te treden; dringt aan op de aanwijzing van één enkel coördinatiepunt tussen de Commissie en de EDEO met het oog op de totstandbrenging van een daadwerkelijke EU-brede aanpak van hybride dreigingen;
57. is ingenomen met de lopende initiatieven om de operationele capaciteit te versterken, waaronder de EU-snellereactieteams bij hybride dreigingen en de lancering van de oostflankwacht van de EU en het Europees initiatief voor droneafweer; dringt erop aan vaart te zetten achter de uitrol ervan; benadrukt het strategische belang van regionale defensie- en veiligheidsclusters en dringt aan op specifieke EU-financieringslijnen om hun expertise en vermogens te integreren in grensoverschrijdende projecten die de Europese weerbaarheid versterken;
58. is ingenomen met de aankondiging van de Commissie en de hoge vertegenwoordiger van een nieuwe mondiale veiligheidsstrategie van de EU en dringt erop aan dat deze strategie het volledige spectrum van hybride dreigingen volledig adresseert;
59. benadrukt dat dringend vooruitgang moet worden geboekt in de richting van een echte Europese defensie-unie, als zijnde een sterkere Europese pijler van de NAVO, die afscheidbaar maar niet afgescheiden is, zodat de EU en haar lidstaten indien nodig onafhankelijk kunnen optreden; dringt erop aan dat de clausule inzake wederzijdse defensie (artikel 42, lid 7, VEU) verder operationeel wordt gemaakt in het scenario van een gewapende aanvallen en ernstige hybride scenario's; dringt voorts aan op een draaiboek inzake artikel 42, lid 7 — een beknopte maar alomvattende operationele gids voor nationale regeringen en EU-instellingen, waarin wordt uitgelegd wat er gebeurt vóór, tijdens en nadat een lidstaat zich op het artikel beroept; stelt voor dat het draaiboek regelmatig wordt getest in scenario's van ernstige hybride crisis en door middel van uitgebreide sectoroverschrijdende oefeningen;
60. benadrukt dat sommige van de hybride aanvallen van Rusland tegen de EU en haar lidstaten mogelijk kunnen worden aangemerkt als door de staat gesteund terrorisme;

moedigt de lidstaten aan gebruik te maken van alle beschikbare juridische instrumenten om die aanvallen tegen te gaan, met inbegrip van de solidariteitsclausule (artikel 222 VWEU), en ten volle gebruik te maken van de samenwerkings- en coördinatiemechanismen die beschikbaar zijn wanneer de clausule wordt geactiveerd;

61. is ingenomen met het werk dat is verricht in het kader van bestaande sanctieregelingen en dat zich richt op hybride activiteiten, met name de in oktober 2024 ingestelde sanctieregeling met betrekking tot de destabiliserende activiteiten van Rusland en de in 2019 ingestelde horizontale cybersanctieregeling; betreurt het feit dat het EU-sanctiekader complex is en gefragmenteerd is over verschillende hybride dreigingsvectoren; dringt aan op een verdere verzwaring van de beperkende maatregelen van de EU in antwoord op hybride dreigingen, waaronder de onmiddellijke vaststelling van een horizontaal EU-sanctiekader, dat specifiek is ontworpen voor hybride dreigingen teneinde de gaten in de bestaande regelingen op te vullen en het afschrikkingseffect te vergroten, en dat naast de sanctieregeling voor Russische hybride operaties zou bestaan om de actieve betrokkenheid van Rusland bij hybride operaties wereldwijd te onderstrepen en tegelijkertijd sneller en systematischer sancties te kunnen opleggen aan entiteiten die verantwoordelijk zijn voor hybride campagnes; dringt erop aan de EU-instrumentaria tegen hybride operaties en FIMI en voor cyberdiplomatie verder te versterken en effectiever in te zetten;
62. herhaalt dat de verantwoordelijken voor hybride operaties ter verantwoording moeten worden geroepen, met inbegrip van tussenpartijen die namens statelijke actoren optreden, door bestaande en specifieke instrumenten ten volle te benutten; verzoekt de EU en de lidstaten dringend maatregelen te nemen om de geldstromen waarmee aanvallen op de democratie worden gefinancierd, stop te zetten en te verstoren, onder meer door banktoezichthouders, opsporingsambtenaren en sanctieautoriteiten in te schakelen om illegale financieringsbronnen, met inbegrip van cryptovaluta, op te sporen en te onderzoeken; verzoekt de EU en de lidstaten de financiële en algoritmische prikkels die desinformatie aanwakkeren, weg te nemen, onder meer door de verbanden aan te pakken tussen illegale financiering, advertentie-inkomsten, de op aandacht gerichte bedrijfsmodellen van platforms en manipulatieve inhoud;
63. is van mening dat alle strafrechtelijke instrumenten die op het niveau van de lidstaten en de EU beschikbaar zijn, moeten worden toegepast en, in voorkomend geval, verder moeten worden ontwikkeld om illegaal gedrag dat gericht is op het ondermijnen van democratische instellingen en processen te voorkomen en tegen te gaan; benadrukt dat de bevoegde nationale autoriteiten moeten beschikken over passende instrumenten en samenwerkingskanalen om strafbare feiten in verband met buitenlandse inmenging te voorkomen, te onderzoeken, op te sporen en te vervolgen; is van mening dat corruptie en de intimidatie van gekozen functionarissen en ambtenaren door criminele netwerken moeten worden aangepakt in het kader van de respons van de EU op hybride dreigingen, via versterkte samenwerking tussen gespecialiseerde corruptiebestrijdingsinstanties, rechtshandhavingsautoriteiten en betrokken organen van de EU; verzoekt de Commissie te beoordelen wat de toegevoegde waarde zou zijn van Europeesrechtelijke minimumregels inzake de definitie van en sancties voor het strafbare feit van het willens en wetens deelnemen aan georganiseerde inmengingsactiviteiten namens buitenlandse mogendheden; merkt op dat de aanstaande herziening van de mandaten van de agentschappen van de EU op het gebied van justitie en binnenlandse zaken de kans biedt om de operationele responscapaciteit van de EU te

versterken; verzoekt de Commissie onderzoek te doen naar de mogelijkheid om een platform of taskforce in het leven te roepen waarin de lidstaten op vrijwillige basis hun nationale wetgevende respons kunnen coördineren en beste praktijken kunnen uitwisselen;

Geografische overwegingen

64. veroordeelt met klem de instrumentalisering van migratie door derde landen of vijandige niet-statelijke actoren met als doel een lidstaat te destabiliseren of de EU onder druk te zetten; neemt kennis van de specifieke bepalingen inzake de instrumentalisering van migratie die onlangs in belangrijke EU-wetten zijn opgenomen; neemt kennis van de door de Commissie aangekondigde herziening van het mandaat voor Frontex; onderstreept dat deze herziening moet voorzien in de rechtsgrondslag, analytische capaciteiten en toereikende personele, financiële en technische middelen die nodig zijn, wat ook zou helpen om de respons van de EU op hybride dreigingen te versterken;
65. veroordeelt de systematische drone-invasies en grensoverschrijdende provocaties door Rusland gericht tegen de lidstaten die langs de oostflank van de EU zijn gelegen, als weloverwogen intimidatiecampagne tegen de burgerbevolking; is ingenomen met de mededeling van de Commissie over de oostelijke regio's van de EU die grenzen aan Rusland, Belarus en Oekraïne, en de expliciete erkenning daarin dat de oostelijke grensregio's van de EU te maken hebben met structurele en aanhoudende dreigingen van Rusland en Belarus; verzoekt de Commissie deze erkenning om te zetten in specifieke financieringsstromen in het kader van het meerjarig financieel kader 2028-2034, met inbegrip van specifieke financiering om de capaciteit voor geïntegreerde grensbescherming te versterken en de fysieke en digitale grensbewakingsinfrastructuur — in overeenstemming met de NAVO-normen — aan de landbuitengrenzen van de EU te moderniseren; onderstreept dat de nadruk moet worden gelegd op geavanceerde opsporings-, monitoring- en tegenmaatregelen tegen onbemande luchtvaartuigen om kritieke infrastructuur zoals luchthavens, energiefaciliteiten en vervoersknooppunten te beschermen en de lidstaten te ondersteunen bij de uitrol van interoperabele systemen voor luchtruimbewustzijn, elektronische beschermingsmaatregelen en snellereactiecapaciteit bij incidenten; benadrukt dat dergelijke maatregelen evenredig, defensief en op de bescherming van de burgerbevolking gericht moeten zijn, waarbij de continuïteit van essentiële diensten en het vrije verkeer binnen het Schengengebied worden gewaarborgd;
66. benadrukt dat hybride dreigingen in toenemende mate de hele EU treffen, maar in de verschillende regio's verschillende vormen aannemen; onderstreept in dit verband de blootstelling van de Baltische, de Noords-Baltische en de Zwarte Zee-regio's aan bedreigingen voor de maritieme veiligheid en de veiligheid van het luchtruim, alsook aan geïnstrumentaliseerde migratie, de kwetsbaarheid van de mediterrane en zuidelijke grensregio's voor bedreigingen die gericht zijn op maritieme infrastructuur, energienetwerken, logistieke corridors, strategische vervoersroutes, desinformatiecampagnes en de instrumentalisering van migratiestromen, de blootstelling van Zuidoost-Europa aan economische dwang, energieafhankelijkheid en gecoördineerde informatiemanipulatie in verband met naburige gebieden, de specifieke kwetsbaarheid van grote stedelijke en digitale informatieruimten in de hele EU voor cognitieve oorlogvoering, polarisatie en buitenlandse inmenging; onderstreept het

toenemende strategische belang van het noordpoolgebied voor de veiligheid van Europa, met inbegrip van de bescherming van kritieke infrastructuur, vrije scheepvaart, satellietcommunicatie en opkomende vervoerscorridors; verzoekt de EU en de NAVO de geografie van hybride dreigingen tot uiting te laten komen in hun strategieën, met inbegrip van de aankomende veiligheidsstrategie van de EU, en tegelijkertijd een 360°-veiligheidsbenadering van weerbaarheid, paraatheid en respons te handhaven; benadrukt dat de financiering voor de bestrijding van hybride dreigingen gebaseerd moet zijn op strategische kwetsbaarheid, operationele behoeften en aangetoonde kwetsbaarheden, en er tevens voor te zorgen dat alle regio's die met hybride dreigingen te maken hebben steun ontvangen;

Coördinatie en samenwerking tussen de EU en de NAVO

67. bevestigt nogmaals dat de NAVO voor haar leden de hoeksteen van de collectieve defensie blijft; dringt aan op meer samenwerking tussen de EU en de NAVO om de Europese paraatheid, weerbaarheid en afschrikking te versterken; benadrukt in dit verband het belang van het beschermen van kritieke infrastructuur, militaire mobiliteit, cyberweerbaarheid en paraatheid; benadrukt dat de lessen die op hybride gebied zijn getrokken uit de oorlog in Oekraïne systematischer moeten worden uitgewisseld;
68. benadrukt dat het optreden van de EU en de NAVO op hybride gebied complementair, wederzijds versterkend en operationeel gecoördineerd moet zijn, waarbij de EU in staat moet blijven in te grijpen wanneer dat nodig is, ermee rekening houdend dat de minimumparaatheidsvereisten van de EU moeten aansluiten bij de basisvereisten van de NAVO;
69. merkt op dat de herziene hybride strategie van de NAVO van 2025 een verschuiving markeert van weerbaarheid naar actieve afschrikking; is ingenomen met de vooraf overeengekomen militaire responsopties en de uitgebreide bevoegdheden van de Geallieerde Opperbevelhebber Europa (SACEUR) om sneller te kunnen optreden aan het begin van een hybride aanval, waardoor vertragingen tussen de detectie van een dreiging en de respons daarop worden verminderd, terwijl het politieke toezicht behouden blijft;
70. is ingenomen met het traceringsmechanisme voor hybride dreigingen van de NAVO, een instrument voor het verzamelen van inlichtingen via de gezamenlijke inlichtingen- en veiligheidsafdeling van de NAVO dat bondgenoten een geconsolideerd dreigingsbeeld biedt, waarbij gebruik wordt gemaakt van nationale inlichtingendiensten; erkent de doorlopende samenwerking tussen de NAVO en de EU op inlichtingengebied, en verzoekt de Commissie en de EDEO om binnen de Fusiecel voor analyse van hybride dreigingen een gestructureerde interface met dit mechanisme tot stand te brengen, zodat het situationeel bewustzijn van de EU en het NAVO-beeld van hybride dreigingen regelmatig en systematisch op elkaar worden afgestemd;
71. wijst op de belangrijke rol van de “Arctic Sentry”, de “Baltic Sentry” en de “Eastern Sentry” van de NAVO als zijnde wendbare instrumenten voor het reageren op hybride dreigingen binnen operationeel relevante tijdspannes, met name bij de bescherming van kritieke maritieme infrastructuur en toeleveringsroutes, en bij de monitoring van hybride activiteiten in die gebieden; merkt op dat de doeltreffendheid ervan wordt beperkt door de hoge kosten van het onderscheppen van drones, lacunes in het

situationeel bewustzijn en fragmentatie van de regelgevingskaders inzake droneafweer in de lidstaten; dringt erop aan de uitvoering van het EU-actieplan inzake beveiliging van en tegen drones te versnellen, onder meer door te voorzien in specifieke financiering voor gelaagde defensievermogens waarmee lidstaten in de frontlinie meteorologische ballonnen en drones kinetisch en elektronisch kunnen bestrijden, en het actieplan systematisch af te stemmen op de operationele vereisten van de NAVO, om te zorgen voor geharmoniseerde, van voldoende middelen voorziene droneafweervermogens in alle lidstaten; is tevens voorstander van meer samenwerking bij de ontwikkeling en uitrol van kosteneffectieve droneafweertechologieën in de hele EU;

72. is ingenomen met het kader voor parallelle en gecoördineerde oefeningen tussen de EU en de NAVO (PACE) als een waardevol instrument om de capaciteit, schaal en reikwijdte van de gezamenlijke respons te testen en te verbeteren, en voor de systematische integratie van de geleerde lessen in het beleid, de planning en de institutionele regelingen van de EU; dringt aan op regelmatige EU- en NAVO-oefeningen waarin hybride aanvalsscenario's worden gesimuleerd, met inbegrip van sabotage van militaire mobiliteitsinfrastructuur, gecoördineerde cyberaanvallen, grootschalige FIMI-campagnes, luchtruimschendingen en aanvallen op kritieke infrastructuur;
73. verzoekt de Commissie en de EDEO om, in nauwe samenwerking met de NAVO en de lidstaten, een gemeenschappelijke visie op hybride dreigingen te ontwikkelen en een coherent responsmechanisme voor de EU en de NAVO op te zetten;
74. erkent de waardevolle rol die gespecialiseerde expertisecentra spelen, waaronder het Europees Kenniscentrum voor de bestrijding van hybride dreigingen in Helsinki en het Cooperative Cyber Defence Centre of Excellence van de NAVO in Tallinn, bij het versterken van de paraatheid, weerbaarheid, cyberdefensie en de capaciteiten ter bestrijding van hybride dreigingen in heel Europa; is voorts ingenomen met het werk van de EU-NAVO-taskforce voor de veerkracht van kritieke infrastructuur, met name wat betreft het versterken van de samenwerking inzake energie, vervoer, digitale infrastructuur en onderzeese connectiviteit;
75. verzoekt de lidstaten hun wetgeving te harmoniseren om de juridische tekortkomingen weg te werken die verhinderen dat geallieerd personeel kan deelnemen aan hybride responsoperaties onder de militaire geweldsdrempel; is ingenomen met de onlangs door Estland aangenomen wijzigingen van zijn wet inzake de organisatie van de strijdkrachten als een concrete stap in deze richting;

Partnerlanden: samenwerking en steun

76. onderstreept dat Russische hybride operaties buiten de EU erop gericht zijn het buitenlands beleid van derde landen op een lijn te brengen met de belangen van Moskou, de betrekkingen van de EU met haar partners te ondermijnen en de internationale steun voor Oekraïne te verzwakken; herhaalt daarom het belang van nauwe samenwerking met internationale partners en organisaties om het situationeel bewustzijn te vergroten en hybride dreigingen doeltreffender te voorkomen, te ontmoedigen en erop te reageren; erkent hoe waardevol het is bilaterale sectorale

dialogen en raadplegingen met gelijkgestemde partners over hybride dreigingen te verdiepen, met name in het kader van veiligheids- en defensiepartnerschappen;

77. benadrukt dat nauwere samenwerking met Oekraïne, Moldavië, Armenië en partners in de Westelijke Balkan een strategische noodzaak is, aangezien zij te maken hebben met voortdurende aanvallen van Rusland en belangrijke proeftuinen vormen voor de hybride tactieken van Rusland, waarbij FIMI, cyberoperaties, geheime beïnvloedingsnetwerken, energiedwang en corrupte beïnvloeding worden gecombineerd om democratische instellingen, maatschappelijke cohesie en de vooruitzichten voor toetreding tot de EU en tot de NAVO te ondermijnen; verzoekt de lidstaten lering te trekken uit de ervaringen van deze landen en gestructureerde mechanismen in te voeren voor de systematische uitwisseling van beste praktijken en operationele ervaring, onder meer inzake het vermogen van Oekraïne om essentiële diensten, de continuïteit van regeringsactiviteiten, de bescherming van kritieke infrastructuur, strategische communicatie en het maatschappelijk functioneren in stand te houden onder aanhoudende aanvallen; herhaalt zijn krachtige steun voor de geleidelijke toetreding van Oekraïne tot de EU en voor toetreding tot de NAVO zodra de nodige voorwaarden zijn vervuld;
78. wijst op het strategische belang van voortzetting en verdieping van de steun inzake weerbaarheid tegen hybride dreigingen aan kandidaat-, potentiële kandidaat- en partnerlanden, die vaak hoofddoelwit zijn van Russische hybride activiteiten en wier weerbaarheid rechtstreeks bijdraagt tot de veiligheid van de EU; is ingenomen met de actieve bijdrage die de EU en de lidstaten aan de versterking van de weerbaarheid van deze landen levert via het instrument voor buitenlands beleid, strategische communicatie, snellereactieteams bij hybride dreigingen, de analyse van hybride risico's en GVDB-missies in partnerlanden, met inbegrip van Oekraïne, Moldavië, Armenië en Montenegro; dringt aan op de organisatie van regelmatige gezamenlijke oefeningen, simulatiescenario's en opleidingsprogramma's ter vergroting van de paraatheid, ter verbetering van de snellereactievermogens en ter bevordering van een interoperabele aanpak van hybride dreigingen; neemt met waardering kennis van de gecoördineerde respons van de EU en de NAVO in Moldavië, met inbegrip van de gelijktijdige inzet van een snellereactieteam bij hybride dreigingen van de EU en een NAVO-team ter bestrijding van hybride dreigingen met aanvullende mandaten; spoort kandidaat-lidstaten en potentiële kandidaat-lidstaten aan zich volledig aan te sluiten bij het gemeenschappelijk buitenlands en veiligheidsbeleid (GBVB) van de EU, met inbegrip van beperkende maatregelen, als zijnde een belangrijk aspect van het EU-integratieproces;
79. prijst de pro-Europese krachten van Moldavië en Armenië voor hun democratische veerkracht tijdens en in de aanloop naar hun parlementsverkiezingen in 2025 en 2026, waarbij zij lieten zien stevige weerstand te bieden tegen de jarenlange FIMI-campagnes van Rusland; onderstreept de effectiviteit van de overheidsbrede aanpak als operationeel model, met inbegrip van het gebruik van rechtshandavingsmaatregelen tegen netwerken die hybride operaties uitvoeren namens Rusland; verzoekt de lidstaten en de Commissie om in samenwerking met de EDEO kaders op EU-niveau te ontwikkelen die vergelijkbare handavingsreacties mogelijk maken; wijst op de belangrijke rol die de EU-instellingen, overheidsinstellingen, het maatschappelijk middenveld en onafhankelijke media spelen bij de bestrijding van FIMI, met inbegrip van door AI

gesteunde grootschalige gecoördineerde informatiemanipulatiecampagnes, door bij te dragen tot het bijzonder grote publieke bewustzijn van hybride dreigingen;

80. pleit voor versterkte samenwerking op het gebied van hybride dreigingen met gelijkgestemde niet-EU-partners, in het bijzonder het Verenigd Koninkrijk en Noorwegen, als zijnde belangrijke Europese veiligheidspartners, alsook Canada, Japan, de Republiek Korea, Australië, Nieuw-Zeeland, Taiwan en andere gelijkgestemde partners, indien mogelijk ook via veiligheids- en defensiepartnerschappen, informatie-uitwisseling, en samenwerking op het gebied van cyberzaken, maritieme veiligheid, ruimtevaart en weerbaarheid; benadrukt dat de EER/EVA-landen en hun defensie-industrieën volledig moeten worden betrokken bij de hybride weerbaarheidskaders en capaciteitsontwikkelingsprogramma's van de EU, aangezien zij rechtstreeks bijdragen tot de Europese veiligheid en blootstaan aan dezelfde hybride dreigingen;
81. betreurt dat de recente verschuiving in het beleid van de VS het gemeenschappelijke front van democratieën heeft verzwakt in een tijd van toenemende hybride dreigingen; benadrukt dat trans-Atlantische eenheid van essentieel belang blijft om deze dreigingen te bestrijden;
82. benadrukt dat Russische beïnvloedingsoperaties in Afrika, Latijns-Amerika en het Caribisch gebied niet van ondergeschikt belang zijn voor de Europese veiligheid, aangezien zij tot doel hebben de partnerschappen van de EU te ondermijnen, de steun voor Oekraïne te verzwakken en de Europese diplomatie, veiligheidsbijstand en ontwikkelingssamenwerking te ondermijnen; merkt op dat deze operaties in Afrika voornamelijk steunen op staatsmedia en culturele en religieuze dekmantels, terwijl Rusland in Latijns-Amerika en het Caribisch gebied een Spaanstalig ecosysteem voor beïnvloeding heeft opgebouwd in aanvulling op zijn anti-Europese boodschappen elders; verzoekt de EU en de lidstaten de strategische communicatie te versterken, onafhankelijke en betrouwbare lokale media te ondersteunen, geloofwaardige lokale stemmen te betrekken en de samenwerking met partners in beide regio's te versterken om vijandige informatiecampagnes aan het licht te brengen en te bestrijden;
83. onderstreept dat de Golfstaten, Jordanië en andere relevante partners belangrijke ervaring hebben opgedaan met de bestrijding van aan de Moslimbroederschap gelieerde hybride beïnvloedingsnetwerken, onder meer via benaderingen op het gebied van bestuur, regelgeving en maatschappelijke weerbaarheid, en roept op tot een gestructureerde uitwisseling van beste praktijken met deze partners om het inzicht van de EU in hybride dreigingen te vergroten, de beleidsrespons te verbeteren en de samenwerking bij het tegengaan van buitenlandse inmenging op te schroeven, met inachtneming van de grondrechten en de diversiteit van rechtsstelsels en politieke stelsels;
84. wijst op de uitgebreide ervaring van Taiwan op het gebied van verdediging tegen hybride aanvallen en FIMI afkomstig van China; prijst het alomvattende weerbaarheidsmodel van Taiwan, met inbegrip van de oprichting van een comité voor de weerbaarheid van de gehele samenleving op defensiegebied, grootschalige civiele defensieopleidingen, samenwerking met maatschappelijke organisaties, digitale weerbaarheidsnetwerken en initiatieven voor de paraatheid van burgers; benadrukt dat de ervaringen van Taiwan aantonen dat maatschappelijke weerbaarheid geen ondergeschikt aspect van defensie is, maar een centrale pijler van de nationale

veiligheid, met name wanneer hybride druk gericht is tegen kritieke infrastructuur, het publieke vertrouwen en de sociale cohesie; dringt in dit verband aan op regelmatige uitwisselingen tussen de EU en haar Taiwanese tegenhangers over relevante veiligheidskwesties, en op nauwere samenwerking bij de bestrijding van FIMI en cognitieve oorlogvoering, de bescherming van kritieke infrastructuur en onderzeese kabels, en de versterking van de weerbaarheid van de hele samenleving in de EU en Taiwan; verzoekt de EU de samenwerking met Taiwan op handels- en industrieel gebied uit te bouwen, met name op het gebied van hightechcomponenten en strategische technologieën die cruciaal zijn voor de weerbaarheid en veiligheid van essentiële infrastructuur en toeleveringsketens, met inbegrip van halfgeleiders, 5G/6G-telecommunicatieapparatuur, drones en goederen voor tweërlei gebruik; benadrukt ook de noodzaak om IRIS2 (Infrastructure for Resilience, Interconnectivity and Security by Satellite — infrastructuur voor veerkracht, interconnectiviteit en beveiliging per satelliet) aan Taiwan en Oekraïne te verstrekken;

◦

◦ ◦

85. verzoekt zijn Voorzitter deze resolutie te doen toekomen aan de Raad, de hoge vertegenwoordiger en de Commissie.

TOELICHTING

Een oorlog die niet op oorlog lijkt

De Europese Unie bevindt zich momenteel noch in een situatie van vrede, noch in een openlijk gewapend conflict. Tegenstanders opereren opzettelijk in een grijs gebied waarbij de drempel van een gewapende aanval niet wordt overschreden. Hybride operaties zijn geen losstaande incidenten. Het gaat om gecombineerde, door inlichtingen gevoede en gecoördineerde handelingen die worden uitgevoerd door staten — ook via gelieerde actoren, tussenpartijen en niet-overheidsactoren — en waarmee beoogd wordt de indruk te wekken dat er sprake is van losstaande incidenten, terwijl de effecten van deze handelingen vergelijkbaar zijn met die van conventionele agressie. Deze handelingen zijn met opzet dubbelzinnig, zodat het moeilijker is verantwoordelijkheid aan een dader toe te schrijven en zodat onze respons wordt vertraagd. Dit verslag gaat uit van een eenvoudige doch zwaarwegende premisse: hybride handelingen kunnen een vorm van oorlogsvoering zijn, ongeacht of er conventioneel geweld wordt gebruikt. De veiligheidsomgeving waarin wij ons bevinden, wordt niet gekenmerkt door vrede maar door een soort voorstadium (“zero-stage”) van oorlogvoering waarbij tegenstanders gebruik weten te maken van de discrepantie tussen onze bestuursstructuren voor vreedstijd en de snelheid die vereist is voor een werkelijke respons.

Wie zit erachter?

De ernstigste hybride dreiging waarmee de Unie en haar lidstaten worden geconfronteerd is Rusland, dat ofwel direct ofwel middels Belarus en andere gelieerde actoren opereert. Ook China, Iran en Noord-Korea ontwikkelen hybride campagnes. Ook niet-overheidsactoren — georganiseerde misdaad, kleptocratische netwerken, particuliere militaire bedrijven, geloofsnetwerken en actoren die tegen betaling aan beïnvloeding doen — kunnen hybride campagnes uitvoeren of faciliteren. In het verslag wordt daarom opgeroepen tot een alomvattende aanpak gericht op Russische en Belarussische activiteiten, zonder daarbij de toenemende rol van China, Iran en Noord-Korea uit het oog te verliezen.

De belangrijkste slagvelden

Informatie en cognitieve oorlogvoering. Buitenlandse informatiemaniipulatie en inmenging (FIMI) is een kernelement van hybride oorlogvoering dat tot doel heeft het vertrouwen in democratische instellingen uit te hollen, polarisatie te vergroten en de steun voor de Europese defensie — met inbegrip van steun aan Oekraïne — te ondermijnen. Deze campagnes maken steeds vaker gebruik van geavanceerde cognitief-psychologische methoden en het bereik ervan wordt uitgebreid met behulp van door AI gegenereerde inhoud, deepfakes en geautomatiseerde netwerken. Onze respons blijft steken in het reactieve, en in het verslag wordt er daarom op aangedrongen dat FIMI wordt behandeld als een ernstige bedreiging voor de veiligheid, met realtime opsporing, toerekening en proactieve respons, en dat maatschappelijke weerbaarheid — mediageletterdheid, onafhankelijke journalistiek, burgerparaatheid — niet als een secundair punt van zorg wordt behandeld, maar als een centrale pijler van veiligheid.

Cyberbeveiliging. Cyberspace is nu het vijfde militaire domein en een centrale facilitator van hybride campagnes. In het verslag wordt benadrukt dat volledige cyberbescherming onmogelijk is en dat Europa zijn mentaliteit moet verleggen naar weerbaarheid — hetgeen aangeleerd moet worden door middel van frequente, realistische oefeningen in alle lagen van

de economie. Het is echter evenzeer duidelijk dat weerbaarheid en defensie alleen niet voldoende zijn om vijandige actoren af te schrikken. In het verslag wordt daarom opgeroepen tot soevereine cybercapaciteiten — voor opsporing, toerekening en respons, inclusief offensieve capaciteiten — en, in samenwerking met de NAVO, tot werken aan de voorwaarden voor evenredige, rechtmatige tegenmaatregelen op cyberniveau om een geloofwaardige afschrikking te waarborgen. De rapporteur wil waarschuwen dat AI nu zowel een wapen als een doelwit is.

Kritieke infrastructuur. Energie, vervoer en communicatie zijn zowel kritieke facilitators als strategische goederen voor de defensie, weerbaarheid en civiele bescherming van de Unie, en zij zijn steeds vaker het doelwit van hybride aanvallen. Deze infrastructuur vormt een systeem met vele onderlinge verbindingen, dat niet afzonderlijk kan worden beschermd, en hoe meer verbindingen er zijn des te groter de kwetsbaarheid van het systeem. In het verslag worden de hybride aanvallen op infrastructuur veroordeeld en wordt opgeroepen minder afhankelijk te zijn van leveranciers met een hoog risico, een strengere screening van investeringen uit te voeren en de bestaande wetgeving inzake weerbaarheid (CER-richtlijn, NIS 2) volledig uit te voeren, en het ruimtedomein te beschermen. Tevens worden de lidstaten opgeroepen om weerbaarheid als ontwerpprincipe in alle nieuwe en herziene wetgeving op te nemen als een standaardvereiste.

Van fragmentatie naar een doortastende respons

Het centrale argument van dit verslag is dat de Unie moet bewegen van een reactieve naar een proactieve houding, om niet alleen hybride aanvallen te kunnen weerstaan, maar deze ook te kunnen ontmoedigen en een respons klaar te hebben. Dat begint met een gedeeld dreigingsbeeld, want geen enkele lidstaat is in staat gecoördineerde campagnes zelfstandig op te sporen. Daarom wordt er in het verslag bij de lidstaten op aangedrongen de uitwisseling van inlichtingen te vergroten via de gezamenlijke capaciteit op het gebied van inlichtingenanalyse van de EU (SIAC), en wordt erop aangedrongen dat de rol van de EU bij het bundelen van gegevens uit meerdere landen en het coördineren van gemeenschappelijke procedures voor situationeel bewustzijn en toerekening formeel wordt erkend als zijnde coördinerende en ondersteunende bevoegdheden van de EU. Op basis hiervan wordt in het verslag opgeroepen tot een horizontaal actieplan tegen hybride oorlogvoering en tot één coördinatiepunt tussen de Commissie en de EDEO — en wordt erop aangedrongen dat elke schending van de soevereiniteit van een lidstaat wordt beantwoord met een doeltreffende, evenredige en gecoördineerde respons, met inbegrip van gekalibreerde vergeldingsopties. In verband met verantwoording wordt er in het verslag op aangedrongen dat elk beschikbaar instrument wordt gebruikt, met inbegrip van een specifiek horizontaal sanctiekader voor hybride dreigingen en maatregelen tegen de illegale geldstromen die aanvallen op onze democratieën financieren. Ook wordt erop gewezen dat we voortgang moeten maken in de richting van een echte Europese defensie-unie teneinde de Europese pijler van de NAVO te versterken, en dat de clausule inzake wederzijdse defensie (artikel 42, lid 7, VEU) operationeel moet worden gemaakt voor ernstige hybride scenario's. Het verslag is evenzeer duidelijk over de begrenzing van het optreden van de EU. Nationale veiligheid blijft in de eerste plaats een verantwoordelijkheid van de lidstaten, en wanneer de EU een grotere rol gaat innemen moet zij exclusieve bevoegdheden en de bescherming van gerubriceerde informatie eerbiedigen.

Geografische overwegingen

Hybride dreigingen hebben gevolgen voor de hele Unie, maar nemen in de verschillende regio's verschillende vormen aan. In het verslag worden de Russische drone-invallen en provocaties langs de oostelijke flank veroordeeld en wordt opgeroepen tot specifieke financiering om de buitengrenzen van de EU te beschermen, met behoud van een 360-gradenaanpak waarin de specifieke kwetsbaarheden van het Oostzeegebied, de Noords-Baltische regio, het Zwarte Zeegebied, het Middellandse Zeegebied, de zuidoostelijke regio en het noordpoolgebied worden erkend. Het verslag veroordeelt met klem de instrumentalisering van migratie door derde landen en vijandige niet-overheidsactoren met als doel een lidstaat te destabiliseren of druk uit te oefenen op de Unie, en neemt nota van de aangekondigde herziening van het mandaat van Frontex als zijnde een kans om de respons van de EU op hybride dreigingen te versterken. Er wordt benadrukt dat financiering afhankelijk moet worden gesteld van strategische blootstelling en aantoonbare behoefte, rekening houdend met het feit dat alle regio's die met hybride dreigingen worden geconfronteerd, steun moeten ontvangen.

Samenwerken met bondgenoten en partners

De NAVO blijft de hoeksteen van de collectieve defensie voor haar leden, en in het verslag wordt opgeroepen tot een aanvullend, wederzijds versterkend en operationeel gecoördineerd optreden van de EU en de NAVO. In het verslag wordt steun uitgesproken voor nauwere samenwerking met Oekraïne, Moldavië, Armenië en de Westelijke Balkan — landen in de frontlinie waar Rusland zijn tactiek uitprobeert, en waarvan Europa kan leren — en met gelijkgestemde partners zoals het Verenigd Koninkrijk, Noorwegen, Canada, Japan, Korea, Australië en Taiwan. Er wordt met name gewezen op het Taiwanese weerbaarheidsmodel dat de gehele samenleving omvat, waarvan de EU kan leren.

Waarom dit nu belangrijk is

De geloofwaardigheid van afschrikking berust niet alleen op vermogens, maar ook op politieke wil, cohesie en een gedeeld begrip van de dreiging, en dit zijn nu juist de kwaliteiten die Rusland poogt te verzwakken met zijn hybride strategie, nog voordat er sprake is van een militair conflict. Voorlichting van burgers over de nabijheid en realiteit van deze dreiging, is op zichzelf een kwestie van paraatheid en afschrikking. Met dit verslag wordt beoogd dichter in de buurt van die duidelijkheid te komen — en te bewegen in de richting van een Unie die niet alleen haar grondgebied kan verdedigen, maar ook de democratische grondslagen waarvan haar veiligheid afhankelijk is.

BIJLAGE: BEKENDMAKING VAN INPUT

Overeenkomstig artikel 8 van bijlage I bij het Reglement verklaart de rapporteur in het verslag input te hebben opgenomen over aangelegenheden in verband met het onderwerp van het dossier die in het kader van de opstelling van het verslag door haar is ontvangen van de volgende belangenvertegenwoordigers die binnen het toepassingsgebied van het Interinstitutioneel Akkoord over een verplicht transparantieregister¹ vallen, of van de volgende vertegenwoordigers van overheidsinstanties van derde landen, met inbegrip van hun diplomatieke vertegenwoordigingen en ambassades:

1. Belangenvertegenwoordigers die binnen het toepassingsgebied van het Interinstitutioneel Akkoord over een verplicht transparantieregister vallen
Vestas Wind Systems A/S
Kongsberg Group
2. Vertegenwoordigers van overheidsinstanties van derde landen, met inbegrip van hun diplomatieke vertegenwoordigingen en ambassades

De bovenstaande lijst is opgesteld onder de exclusieve verantwoordelijkheid van de rapporteur.

De rapporteur verklaart dat aan natuurlijke personen die met hun naam en/of functie in de lijst worden vermeld privacyverklaring nr. 484 van het Europees Parlement (<https://www.europarl.europa.eu/data-protect/index.do>) is verstrekt, waarin de voorwaarden voor de verwerking van hun persoonsgegevens en de rechten in verband met die verwerking worden toegelicht.

¹ Interinstitutioneel Akkoord van 20 mei 2021 tussen het Europees Parlement, de Raad van de Europese Unie en de Europese Commissie over een verplicht transparantieregister (PB L 207 van 11.6.2021, blz. 1, ELI: http://data.europa.eu/eli/agree_interinstit/2021/611/oj).

INFORMATIE OVER DE GOEDKEURING IN DE BEVOEGDE COMMISSIE

Datum goedkeuring	15.7.2026		
Uitslag eindstemming	+	:	28
	-	:	8
	0	:	0

HOOFDELIJKE EINDSTEMMING IN DE BEVOEGDE COMMISSIE

28	+
ECR	Alberico Gambino, Reinis Poznaks, Cristian Terhes, Alexandr Vondra
PPE	Georgios Aftias, Salvatore De Meo, Michael Gahler, Niclas Herbst, Rasa Juknevičienė, Andrey Novakov, Liesbet Sommen, Helder Sousa Silva, Pekka Toveri, Marta Wcisło
Renew	Petras Austrevičius, Marjan Sarec, Marie-Agnes Strack-Zimmermann, Lucia Yar
S&D	José Cepeda, Tobias Cremer, Vasile Dîncu, François Kalfon, Costas Mavrides, Sven Mikser
The Left	Merja Kyllönen
Vers/ALE	Hannah Neumann, Villy Søvndal, Reinier Van Lanschot

8	-
ECR	Marion Maréchal
NI	Michael von der Schulenburg
PPE	Christophe Gomart
PfE	Jaroslava Pokorná Jermanová, Petra Steger, Pierre-Romain Thionnet
The Left	Marc Botenga, Lynn Boylan

0	0
---	---

Verklaring van de gebruikte tekens:

+ : voor

- : tegen

0 : onthouding(en)