**Europäisches Parlament**
2024-2029

**ANGENOMMENE TEXTE**

# P10_TA(2026)0303

## Hybride Kriegsführung und Schutz der territorialen Unversehrtheit und der kritischen Sicherheits- und Verteidigungsinfrastruktur der EU

### Entschließung des Europäischen Parlaments vom 16. September 2026 zu hybrider Kriegsführung und den Schutz der territorialen Unversehrtheit und der kritischen Sicherheits- und Verteidigungsinfrastruktur der EU (2026/2024(INI))

*Das Europäische Parlament*,

– unter Hinweis auf die Charta der Vereinten Nationen und die Grundprinzipien des Völkerrechts,

– gestützt auf Titel V des Vertrags über die Europäische Union (EUV), insbesondere auf Kapitel 2, Abschnitt 2 betreffend Bestimmungen über die Gemeinsame Sicherheits- und Verteidigungspolitik,

– gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union (AEUV),

– gestützt auf Artikel 42 Absatz 7 und Artikel 222 AEUV,

– unter Hinweis auf seine früheren Entschließungen zur Ukraine, zu Russland und zu Belarus, insbesondere die Entschließungen, die seit der Annexion der Halbinsel Krim durch Russland im Februar 2014 und der groß angelegten Invasion der Ukraine durch Russland im Februar 2022 angenommen wurden,

– unter Hinweis auf den internationalen Rechtsrahmen zur Verhütung und Bekämpfung von Terrorismus, einschließlich der vom Sicherheitsrat der Vereinten Nationen am 13. Februar 2017 verabschiedeten Resolution 2341 zum Schutz kritischer Infrastruktur vor terroristischen Handlungen,

– unter Hinweis auf die Verordnung (EU) 2019/452 des Europäischen Parlaments und des Rates vom 19. März 2019 zur Schaffung eines Rahmens für die Überprüfung ausländischer Direktinvestitionen in

der Union[1],

– unter Hinweis auf den „Strategischen Kompass für Sicherheit und Verteidigung – Für eine Europäische Union, die ihre Bürgerinnen und Bürger, Werte und Interessen schützt und zu Weltfrieden und internationaler Sicherheit beiträgt“, der am 21. März 2022 vom Rat und am 25. März 2022 vom Europäischen Rat gebilligt wurde,

– unter Hinweis auf die Schlussfolgerungen des Rates vom 21. Juni 2022 über einen Rahmen für eine koordinierte Reaktion der EU auf hybride Kampagnen,

– unter Hinweis auf die Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates[2],

– unter Hinweis auf den abschließenden Bewertungsbericht der EU-NATO-Taskforce für die Resilienz kritischer Infrastrukturen vom 29. Juni 2023,

– unter Hinweis auf den Bericht von Sauli Niinistö vom 30. Oktober 2024 mit dem Titel „Safer Together: Strengthening Europe’s Civilian and Military Preparedness and Readiness“ (Gemeinsam für mehr Sicherheit: Stärkung der zivilen und militärischen Vorsorge und Bereitschaft Europas) (Niinistö-Bericht),

– unter Hinweis auf die Mitteilung der Kommission vom 11. Dezember 2024 über die Abwehr hybrider Bedrohungen infolge des Einsatzes von Migration als Waffe und die Stärkung der Sicherheit an den EU-Außengrenzen (COM(2024)0570),

– unter Hinweis auf die Verordnung (EU) 2025/37 des Europäischen Parlaments und des Rates vom 19. Dezember 2024 zur Änderung der Verordnung (EU) 2019/881 im Hinblick auf verwaltete Sicherheitsdienste[3],

– unter Hinweis auf die Verordnung (EU) 2025/38 des Europäischen Parlaments und des Rates vom 19. Dezember 2024 über Maßnahmen zur Stärkung der Solidarität und der Kapazitäten in der Union für die Erkennung von, Vorsorge für und Bewältigung von Cyberbedrohungen und Sicherheitsvorfällen und zur Änderung der

---

1 ABl. L 79I vom 21.3.2019, S. 1, ELI: http://data.europa.eu/eli/reg/2019/452/oj.
2 ABl. L 333 vom 27.12.2022, S. 164, ELI: http://data.europa.eu/eli/dir/2022/2557/oj.
3 ABl. L, 2025/37, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/37/oj.

Verordnung (EU) 2021/694 (Cybersolidaritätsgesetz)[4],

– unter Hinweis auf die Gemeinsame Mitteilung der Kommission und der Hohen Vertreterin der Union für Außen- und Sicherheitspolitik vom 21. Februar 2025 mit dem Titel „EU-Aktionsplan für Kabelsicherheit“ (JOIN(2025)0009),

– unter Hinweis auf seine Entschließung vom 12. März 2025 zu dem Weißbuch zur Zukunft der europäischen Verteidigung[5],

– unter Hinweis auf das Gemeinsame Weißbuch der Kommission und der Hohen Vertreterin der Union für Außen- und Sicherheitspolitik vom 19. März 2025 mit dem Titel „Gemeinsames Weißbuch zur europäischen Verteidigung – Bereitschaft 2030“ (JOIN(2025)0120),

– unter Hinweis auf die Gemeinsame Mitteilung der Kommission und der Hohen Vertreterin der Union für Außen- und Sicherheitspolitik vom 26. März 2025 über eine europäische Strategie für eine Union der Krisenvorsorge (JOIN(2025)0130),

– unter Hinweis auf die Mitteilung der Kommission vom 1. April 2025 an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen mit dem Titel „ProtectEU – eine Europäische Strategie für die innere Sicherheit“ (COM(2025)0148),

– unter Hinweis auf die Erklärung im Rahmen des Gipfeltreffens des Nordatlantikrats in Den Haag, die von den Staats- und Regierungschefs, die an dem Treffen des Nordatlantikrats am 25. Juni 2025 teilgenommen haben, angenommen wurde,

– unter Hinweis auf seine Entschließung vom 9. Oktober 2025 zu einer geeinten Reaktion auf die jüngsten Verletzungen des Luftraums und die jüngsten Bedrohungen der kritischen Infrastruktur der EU-Mitgliedstaaten durch Russland[6],

– unter Hinweis auf das Non-Paper des italienischen Verteidigungsministers vom November 2025 mit dem Titel „Countering hybrid Warfare: an active strategy“ (Abwehr hybrider Kriegsführung: eine aktive Strategie),

– unter Hinweis auf den Vorschlag der Kommission vom 10. Dezember 2025 zu Leitlinien für die transeuropäische Energieinfrastruktur

---

4 ABl. L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj.
5 ABl. C, C/2025/3151, 20.6.2025, ELI: http://data.europa.eu/eli/C/2025/3151/oj.
6 ABl. C, C/2026/1530, 15.4.2026, ELI: http://data.europa.eu/eli/C/2026/1530/oj.

(COM(2025)0006),

– unter Hinweis auf seine Entschließung vom 18. Dezember 2025 zu den anhaltenden hybriden Angriffen auf Litauen seitens Belarus[7],

– unter Hinweis auf die Mitteilung der Kommission vom 18. Februar 2026 zu den östlichen Regionen der EU an der Grenze zu Russland, Belarus und der Ukraine (COM(2026)0082),

– unter Hinweis auf seine Entschließung vom 21. Januar 2026 zur Umsetzung der Gemeinsamen Sicherheits- und Verteidigungspolitik – Jahresbericht 2025[8],

– unter Hinweis auf die Schlussfolgerungen des Rates vom 16. März 2026 zur Stärkung der Fähigkeit der Europäischen Union zur Abwehr hybrider Bedrohungen,

– gestützt auf Artikel 55 seiner Geschäftsordnung,

– unter Hinweis auf den Bericht des Ausschusses für Sicherheit und Verteidigung (A10-0212/2026),

– unter Hinweis auf die Erklärung im Rahmen des Gipfeltreffens des Nordatlantikrats, die von den Staats- und Regierungschefs, die an dem Treffen des Nordatlantikrats am 8. Juli 2026 in Ankara teilgenommen haben, angenommen wurde,

A. in der Erwägung, dass die Intensität und das Ausmaß hybrider Angriffe auf die EU seit Beginn des Angriffskriegs Russlands gegen die Ukraine erheblich zugenommen haben, wobei Vorfälle wiederholt mit autoritären Staaten, vor allem Russland, Belarus, China, Iran und Nordkorea, in Zusammenhang gebracht wurden;

B. in der Erwägung, dass Russland die größte und bedeutsamste Sicherheitsbedrohung für die EU und ihre Mitgliedstaaten darstellt; in der Erwägung, dass Russland kontinuierlich gegen den in Artikel 2 Absatz 4 der Charta der Vereinten Nationen verankerten Grundsatz der territorialen Integrität und der politischen Unabhängigkeit verstoßen hat; in der Erwägung, dass hybride Angriffe eine Bedrohung für die Demokratie in der EU und ihren Mitgliedstaaten darstellen;

C. in der Erwägung, dass die Schwere dieser Angriffe drastisch zugenommen hat und dass diese Angriffe eine eklatante Verletzung der Souveränität der Mitgliedstaaten, der territorialen Unversehrtheit der EU und des Völkerrechts darstellen; in der Erwägung, dass hybride Kriegsführung zu einem strukturellen

---

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

8 Angenommene Texte, P10_TA(2026)0013.

Merkmal des derzeitigen geopolitischen Umfelds geworden ist;

D. in der Erwägung, dass die jüngsten hybriden Angriffe unerlaubte Drohnenüberflüge, „Schmuggelballone“, Verletzungen des Luftraums, geheime Tunnel für Infiltration und Schmuggel, Sabotage und Spionage kritischer Sicherheits- und Verteidigungsinfrastruktur, die Sabotage von Unterseekabeln und Energieinfrastruktur, GPS-Störungen und Datenmanipulation bei der Navigation, Cyberangriffe, Brandstiftungen und Attentate, die Instrumentalisierung von Migration und organisierter Kriminalität, die Vereinnahmung von Eliten, verdeckte ausländische Investitionen, wirtschaftlicher Zwang, Datenexfiltration und sonstige subversive politische Aktivitäten sowie wirtschaftliche Durchdringung, Informationsmanipulation und Einflussnahme aus dem Ausland und die Einmischung in politische Prozesse und Wahlprozesse umfassen können;

E. in der Erwägung, dass die EU im Sommer 2026 eine Intensivierung physischer hybrider Aktivitäten und Angriffe im gesamten Gebiet der EU erlebt hat; in der Erwägung, dass dazu ein versuchter Drohnenangriff auf ukrainische Frachtflugzeuge am Flughafen Leipzig/Halle in Deutschland, ein versuchter Angriff einer mit Sprengstoff beladenen Seedrohne auf ein rumänisches Offshore-Gasprojekt, ein vereiteltes von Russland gesteuertes Sabotage- und Spionageprojekt gegen militärische Infrastruktur und ukrainische Frachtflugzeuge in Rumänien, ein Brandanschlag auf einen Verteidigungsauftragnehmer in Estland, gezielte Sabotage- und Brandangriffe auf Verteidigungs- und Drohnenherstellungsanlagen in Polen, ein russischer Marschflugkörper, der den polnischen Luftraum verletzt und in der Region Lublin abgestürzt ist, und ein vereitelter Brandanschlag in der Slowakei gegen einen ukrainischen Drohnenhersteller gehörten; in der Erwägung, dass der Anschlag auf den Flughafen Leipzig/Halle, das Vorgehen gegen das rumänische Offshore-Gasprojekt und die Sabotage gegen militärische Infrastruktur und ukrainische Frachtflugzeuge in Rumänien von den jeweiligen nationalen Behörden öffentlich Russland zugeschrieben wurden; in der Erwägung, dass die deutschen Behörden nach dem Angriff auf den Flughafen Leipzig/Halle das russische Konsulat in Bonn und das Russische Haus in Berlin geschlossen haben;

F. in der Erwägung, dass die Souveränität und territoriale Unversehrtheit aller Mitgliedstaaten Gründungsprinzipien der EU sind; in der Erwägung, dass feindselige staatliche Akteure, insbesondere Russland, die territoriale Integrität der EU an zwei Fronten ins Visier nehmen: durch direkte physische Angriffe auf Mitgliedstaaten und durch Beeinflussungsoperationen, die darauf abzielen, die Einheit der EU zu untergraben, indem auf den Austritt von Mitgliedstaaten aus der EU hingewirkt wird;

G. in der Erwägung, dass die EU als Ganzes, auch überseeische Länder und Gebiete wie Grönland, zunehmend von hybriden Bedrohungen

betroffen sind, dass die Regionen an den EU-Außengrenzen und die Meeresgebiete der EU jedoch besonders anfällig für Angriffe sind; in der Erwägung, dass diese Angriffe auch gegen Bewerberländer und Nachbarländer der EU, insbesondere die Ukraine, Moldau, Armenien, Georgien und den Westbalkan, gerichtet sind; in der Erwägung, dass die territoriale Unversehrtheit der Nachbarschaft der EU von entscheidender Bedeutung ist, um Frieden, Stabilität und Sicherheit in Europa und darüber hinaus sicherzustellen;

H. in der Erwägung, dass die Einmischung durch Nicht-EU-Staaten in Grönland, insbesondere über aufwieglerische Narrative und die Durchführung hybrider Maßnahmen auf grönländischem Hoheitsgebiet, sowie Äußerungen der US-Regierung, die für die Souveränität Grönlands eine ausdrückliche Bedrohung darstellen, Bedenken hinsichtlich der Souveränität und der territorialen Unversehrtheit Grönlands aufkommen ließen;

I. in der Erwägung, dass Georgien als Beispiel für eine erfolgreiche hybride Einflussnahme Russlands gelten kann, in deren Folge die staatlichen Stellen der mit dem Kreml verbündeten Partei „Georgischer Traum“ das russische Handbuch hybrider Operationen gegen die Zivilgesellschaft und die demokratischen Institutionen des Landes reproduzieren;

J. in der Erwägung, dass Sabotageaktionen durch russische Nachrichtendienste immer häufiger von Mittelsleuten, anfälligen sozialen Gruppen, darunter von Minderjährigen, sowie von Proxy-Akteuren und sogenannten Einweg-Agenten durchgeführt werden, wodurch die Zuordnung und Reaktion erschwert werden; in der Erwägung, dass religiöse Einrichtungen, darunter die Russisch-Orthodoxe Kirche und Netzwerke, die mit der Muslimbruderschaft in Verbindung stehen, herangezogen wurden, um Beeinflussungsoperationen in der EU durchzuführen, durch die demokratische Werte, Rechtsstaatlichkeit und die Fähigkeit der EU, sich zu verteidigen, untergraben werden;

K. in der Erwägung, dass diese Angriffe nicht nur darauf ausgerichtet sind, Chaos zu stiften und die EU-Mitgliedstaaten zu destabilisieren, sondern auch darauf, die demokratische Integrität zu unterwandern, Entscheidungsprozesse zu manipulieren, politische Gräben noch zu vertiefen, den sozialen Zusammenhalt zu schwächen, Angst und öffentliches Misstrauen unter den EU-Bürgern zu säen, die Verteidigungsbereitschaft und die Unterstützung der EU für die Ukraine zu schwächen und auf diese Weise EU-weit Kaskadeneffekte auszulösen;

L. in der Erwägung, dass die Berufung auf Artikel 5 der NATO nach den Terroranschlägen vom 11. September 2001 gezeigt hat, dass die kollektive Verteidigung nach Angriffen nicht nur durch die Handlungen eines staatlichen Akteurs ausgelöst werden kann,

sondern auch durch Angriffe, an denen nichtstaatliche Akteure und komplexe Netze beteiligt sind, die über nationale Grenzen hinweg tätig sind; in der Erwägung, dass dieser Präzedenzfall den sich wandelnden Charakter von Sicherheitsbedrohungen und die Notwendigkeit einer entsprechenden Anpassung der kollektiven Reaktionsmechanismen deutlich macht, auch über verbesserte gemeinsame Standards und Verfahren für die Zuordnung;

M. in der Erwägung, dass kognitive Kriegsführung einhergehend mit Informationsmanipulation und Einflussnahme aus dem Ausland drastisch zugenommen haben; in der Erwägung, dass dem 4. Jahresbericht des Europäischen Auswärtigen Dienstes (EAD) über Bedrohungen in Bezug auf Informationsmanipulation und Einflussnahme aus dem Ausland zufolge die Aktivitäten Russlands im Bereich der Informationsmanipulation und Einflussnahme aus dem Ausland im Jahr 2026 voraussichtlich zunehmen werden, wobei sich die Haushaltsmittel für staatlich kontrollierte Medien Prognosen zufolge auf etwa 1,56 Mrd. EUR belaufen werden, was einem Anstieg um 7 % gegenüber 2025 entspricht, und die Ostsee- und die Arktisregion als vorrangige Ziele gelten dürften;

N. in der Erwägung, dass bei Operationen der Informationsmanipulation und Einflussnahme aus dem Ausland ausgefeilte kognitive und psychologische Methoden eingesetzt werden, darunter die Methode der „reflexiven Kontrolle“, einer in der sowjetischen Militärtheorie verwurzelten Technik, bei der spezifische Informationen ins Spiel gebracht werden, um die wahrgenommenen Entscheidungen eines Zieles einzuengen und Entscheidungen auf die strategischen Ziele des Einflussnehmers auszurichten;

O. in der Erwägung, dass in den Nationalen Sicherheitsstrategien Russlands aus den Jahren 2015 und 2021 die Förderung sogenannter traditioneller Werte und der „Russischen Welt“ als Instrumente seiner umfassenderen Strategie der hybriden Kriegsführung und seines geopolitischen Einflusses fungieren; in der Erwägung, dass Russland im Rahmen seiner Strategie der hybriden Kriegsführung historische, religiöse, kulturelle und wertebasierte Narrative mit Berechnung eingesetzt hat, um den öffentlichen Diskurs und kirchliche Dynamiken zu beeinflussen, den sozialen Zusammenhalt zu schwächen und die demokratische Resilienz und transatlantische Integration zu untergraben;

P. in der Erwägung, dass der Querschnittcharakter des kognitiven Bereichs es erfordert, dass kognitive Indikatoren vollständig in das gemeinsame Lagebild integriert werden, das von Strukturen in den Bereichen Cyberraum, Nachrichtendienste, Strafverfolgung, Militär und kritische Infrastrukturen genutzt wird;

Q. in der Erwägung, dass der Erfolg moderner Militäroperationen und

die Wirksamkeit öffentlicher Einrichtungen zunehmend von der Kontrolle des Cyberraums und der strategischen Nutzung von digitalen Ressourcen und Informationssystemen abhängen;

R. in der Erwägung, dass die innere Sicherheit nach wie vor in die Zuständigkeit der Mitgliedstaaten fällt, dass der grenzüberschreitende, vernetzte und mehrdimensionale Charakter dieser hybriden Angriffe jedoch eine verstärkte Zusammenarbeit, einen systematischen Informationsaustausch und koordinierte Maßnahmen auf EU-Ebene erfordert, die durch eine angemessene Finanzierung zu unterstützen und durch langfristige Strategien zu ergänzen sind, damit die Resilienz von Gesellschaften gestärkt und die institutionelle Integrität geschützt wird;

S. in der Erwägung, dass den EU-Agenturen im Bereich Justiz und Inneres (JI) in Zusammenarbeit mit den nationalen Behörden eine Schlüsselrolle bei der Schaffung und Aufrechterhaltung eines gemeinsamen Lagebewusstseins für die mit solchen Bedrohungen verbundenen Risiken und bei der Unterstützung der Mitgliedstaaten an den Außengrenzen in Krisensituationen zukommt; in der Erwägung, dass die Kommission die Stärkung der Europäischen Agentur für die Grenz- und Küstenwache (Frontex) sowie eine Überarbeitung der Mandate der Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) und der Agentur der Europäischen Union für justizielle Zusammenarbeit in Strafsachen (Eurojust) in ihre Leitinitiativen für die Wahlperiode 2024-2029 aufgenommen hat; in der Erwägung, dass weitere Initiativen wie der sogenannte Schutzschild für die Ostflanke dazu beitragen können, den Schutz der Außengrenzen zu stärken und die Resilienz gegenüber hybriden Bedrohungen zu erhöhen;

T. in der Erwägung, dass das Aufkommen fortschrittlicher KI-Systeme eine strukturelle Störung der bestehenden Cybersicherheitsarchitekturen darstellt, wodurch Bedrohungsmodelle und defensive Annahmen, die in den vorangegangenen Jahrzehnten entwickelt wurden, hinfällig werden; in der Erwägung, dass feindselige staatliche und nichtstaatliche Akteure bereits KI-Fähigkeiten nutzen, um die Geschwindigkeit, den Umfang und die Präzision hybrider Operationen, darunter Cyberangriffe, Manipulation von für KI bestimmten Daten („AI poisoning“), Desinformationskampagnen und Angriffe auf kritische Infrastrukturen, zu verbessern; in der Erwägung, dass die gemeinsamen Rahmen der EU für die Cyberresilienz angepasst werden müssen, um diesen neuen Schwachstellen zu begegnen;

U. in der Erwägung, dass die Reaktion der EU auf hybride Angriffe trotz erheblicher Anstrengungen der Mitgliedstaaten und der Entwicklung von Instrumenten und Mechanismen zur Abwehr hybrider Bedrohungen nach wie vor durch Gesetzeslücken, das Fehlen einer

harmonisierten Herangehensweise zwischen den Mitgliedstaaten, einen unterschiedlichen Grad der Sensibilisierung und das Fehlen einer spezifischen Struktur oder Einrichtung zur Überwachung solcher Angriffe beeinträchtigt wird; in der Erwägung, dass die EU-Mitgliedstaaten trotz der Dringlichkeit eine vollständig koordinierte und kohärente Reaktion auf hybride Kriegsführung noch entwickeln müssen, und zwar sowohl auf einzelstaatlicher Ebene als auch auf EU-Ebene und gegebenenfalls gemeinsam mit der NATO;

V. in der Erwägung, dass die nationalen Verteidigungsausgaben von einer verstärkten Koordinierung und Bündelung zwischen den Mitgliedstaaten oder weiteren Investitionen in europäische Kooperationsprojekte profitieren würden; in der Erwägung, dass im Zuge der erheblichen Aufstockungen der Verteidigungsausgaben der Mitgliedstaaten in Verbindung mit den Verteidigungsinitiativen der EU wie SAFE und weiteren Maßnahmen im Einklang mit dem Rahmen für die Verteidigungsbereitschaft 2030 damit begonnen wird, seit Langem bestehende Defizite bei den Fähigkeiten zu beheben, dass jedoch eine schnellere Umsetzung in konkrete operative Fähigkeiten erforderlich ist, um die EU, ihre Mitgliedstaaten und ihre Bürger besser vor hybriden Bedrohungen zu schützen; in der Erwägung, dass in diesem Bereich nach wie vor Potenzial für Technologien mit doppeltem Verwendungszweck besteht; in der Erwägung, dass auch im Bereich der inneren Sicherheit weitere Maßnahmen erforderlich sind;

W. in der Erwägung, dass die Verantwortung für die nationale Sicherheit nach wie vor in erster Linie bei den Mitgliedstaaten liegt und dass sämtliche auf EU-Ebene koordinierten oder vorgeschlagenen Maßnahmen und Initiativen unter uneingeschränkter Achtung der ausschließlichen Zuständigkeiten der Mitgliedstaaten konzipiert und umgesetzt und mit den EU-Instrumentarien für hybride Bedrohungen, Informationsmanipulation und Einflussnahme aus dem Ausland und Cyberdiplomatie in Einklang gebracht werden müssen;

X. in der Erwägung, dass die Abhängigkeit der EU von ausländischen Akteuren und aus dem Ausland hergestellten Technologien in kritischen Infrastrukturen und Lieferketten, einschließlich der Beschaffung von Rohstoffen aus Drittländern, eine der größten Schwachstellen der EU und eine zentrale Herausforderung für die Sicherheit und strategische Autonomie Europas darstellt;

Y. in der Erwägung, dass das aktuelle Sicherheitsumfeld der EU weder durch Frieden noch durch einen offenen bewaffneten Konflikt charakterisiert wird, sondern durch eine „Grauzonen-Kriegsführung“, bei der Gegner hybride Instrumente einsetzen, um die Lücke zwischen den friedenszeitlichen Governance-Strukturen der EU und der für Abschreckung und Reaktion erforderlichen Entschlossenheit auszunutzen; in der Erwägung, dass die

bestehenden außen- und sicherheitspolitischen Rahmen der EU, die auf konsensorientierte Beratungen ausgerichtet sind, zu strukturellen Schwachstellen führen, die von Gegnern aktiv ausgenutzt werden; in der Erwägung, dass diese Zwischensituation eine grundlegende Neubewertung der Beschlussfassungsarchitektur der EU im Bereich Sicherheit und Verteidigung erfordert;

Z. in der Erwägung, dass die Glaubwürdigkeit der Abschreckung nicht nur auf den materiellen Fähigkeiten und dem technologischen Vorsprung der europäischen und verbündeten Streitkräfte beruht, sondern entscheidend auf dem politischen Willen, dem strategischen Zusammenhalt und einem gemeinsamen Verständnis der Bedrohung; in der Erwägung, dass die hybride Strategie Russlands darauf ausgerichtet ist, genau diese Eigenschaften auszuhöhlen – durch Mehrdeutigkeit, Spaltung und Druck unterhalb der Eskalationsschwelle –, um die Glaubwürdigkeit kollektiver Verteidigungsverpflichtungen zu schwächen, noch bevor eine kinetische Schwelle erreicht wird;

***Hybride Kriegsführung: zwischen Krieg und Frieden***

1. betont, dass es sich bei hybriden Operationen um vorsätzliche, kombinierte, erkenntnisgestützte und koordinierte Handlungen von Staaten – auch vonseiten nichtstaatlicher Akteure, Vermittler und Proxy-Akteure – handelt, die sich gleichzeitig über mehrere Bereiche erstrecken; betont, dass diese so konzipiert sind, dass sie wie isolierte Vorfälle erscheinen und unterhalb der Schwelle eines bewaffneten Konflikts angesiedelt werden, allerdings zugleich Auswirkungen nach sich ziehen können, die mit denen einer herkömmlichen Aggression vergleichbar sind, was eine Zurechnung und wirksame Reaktion erheblich erschwert; fordert die EU und die Mitgliedstaaten daher auf, anzuerkennen, dass hybride Handlungen eine Form von Kriegsführung darstellen können, unabhängig davon, ob konventionelle Gewalt im Spiel ist;

2. betont, dass das vorrangige Ziel der hybriden Kriegsführung darin besteht, die EU und ihre Mitgliedstaaten zu destabilisieren, zu spalten und auszuhöhlen, indem systemische Schwachstellen ausgenutzt und deren Sicherheit, Resilienz und demokratische Grundlagen geschwächt werden, und deren Verteidigungsbereitschaft zu unterminieren, indem die industrielle Basis und die kritische Infrastruktur der EU im Verteidigungsbereich gestört werden und die öffentliche und politische Unterstützung für die Verteidigung der EU untergraben wird, und politische Kräfte zu stärken, die den Urhebern wohlgesonnen sind, indem systematisch auf demokratische Prozesse Einfluss genommen wird;

3. bekräftigt, dass Russland, das direkt oder über mehrere Proxy-Akteure wie Belarus handelt, der staatliche Akteur ist, von dem sehr schwerwiegende hybride Bedrohungen ausgehen und der die EU und

ihre Mitgliedstaaten ins Visier nimmt; stellt fest, dass China, Iran, Nordkorea und andere hybride Kampagnen durchführen, die darauf abzielen, die europäischen Demokratien auszuhöhlen und die Sicherheitsinteressen der EU zu untergraben; betont, dass die EU einen umfassenden Ansatz in Bezug auf hybride Bedrohungen verfolgen muss, der nicht nur auf russische und belarussische Aktivitäten ausgerichtet ist, sondern auch der wachsenden strategischen Rolle Chinas, Irans und Nordkoreas bei der Ermöglichung und Verstärkung feindseliger Handlungen gegen europäische Interessen und die europäische Sicherheit Rechnung trägt; stellt mit Besorgnis fest, dass nichtstaatliche Akteure – darunter terroristische Gruppen, Netzwerke der organisierten Kriminalität, oligarchische und kleptokratische Netzwerke, religiöse Einrichtungen und religiöse Netzwerke, private Militärunternehmen, extremistische Bewegungen und bezahlte Einflussnehmer – ebenfalls hybride Kampagnen gegen europäische Demokratien durchführen oder ermöglichen können;

4. fordert die Kommission und den Rat auf, die Angemessenheit der bestehenden EU-Rechtsrahmen für die Bewältigung hybrider Bedrohungen zu bewerten, ermittelte Lücken zu schließen und hybride Operationen unterhalb der Schwelle, die nicht allein durch Strafverfolgungsmaßnahmen bewältigt werden können, als Angelegenheiten der kollektiven Sicherheit zu behandeln, die eine kombinierte zivil-militärische Reaktion erfordern;

***Informationskriegsführung, kognitive Sicherheit und Resilienz von Gesellschaften***

5. betont, dass Informationskriegsführung als eines der Kernelemente der hybriden Kriegsführung gilt; ist besorgt über das zunehmende Ausmaß der kognitiven Kriegsführung einhergehend mit Informationsmanipulation und Einflussnahme aus dem Ausland, die darauf abzielen, das Vertrauen von Gesellschaften in demokratische Institutionen zu untergraben, die Polarisierung zu verstärken und die demokratische Entscheidungsfindung und die öffentliche Unterstützung für die europäische Sicherheit und Verteidigung, einschließlich der Unterstützung für die Ukraine, auszuhöhlen;

6. betont, dass die vorstehend genannten Ziele (siehe Ziffer 5) überwiegend im Rahmen von ausgeklügelten und koordinierten Operationen verfolgt werden, sich über mehrere Bereiche des sozialen Lebens erstrecken und dabei strategisch-kognitive und psychologische Techniken zum Einsatz kommen, die darauf ausgerichtet sind, Entscheidungsprozesse, individuelle und kollektive Wahrnehmungen, die Identitätsbildung, kulturelle Normen, das historische Gedächtnis, moralische Rahmenbedingungen und religiöse Glaubenssysteme zu beeinflussen, wobei die technologische Infrastruktur, Medienökosysteme und wirtschaftliche und politische

Schwachstellen ausgenutzt werden; stellt mit Besorgnis fest, dass bei Operationen der Informationsmanipulation und Einflussnahme aus dem Ausland ausgefeilte kognitive und psychologische Methoden, einschließlich reflexiver Kontrolle, zum Einsatz kommen, die durch konventionelle Reaktionen schwer zu erkennen, zuzuordnen oder zu bekämpfen sind; betont daher, dass das Instrumentarium der EU im Bereich der Informationsmanipulation und Einflussnahme aus dem Ausland ausdrücklich Gegenmaßnahmen gegen solche fortschrittlichen Einflusstechniken umfassen muss, um die Integrität der Beschlussfassungsverfahren der EU zu wahren;

7. warnt davor, dass einzelne kinetische Vorfälle entweder Auslöser für sofortige, synchronisierte und koordinierte Operationen der Informationsmanipulation und Einflussnahme aus dem Ausland sein oder aber bewusst inszeniert werden können, um diese zu verschleiern, wobei feindliche Akteure die zeitliche Lücke vor der Veröffentlichung offizieller Stellungnahmen ausnutzen, um die öffentliche Wahrnehmung zu beeinflussen; fordert, dass diese Informationslücke im Wege einer verstärkten europäischen Koordinierung ordnungsgemäß angegangen wird, insbesondere durch die Verbesserung der öffentlich-privaten Koordinierung im Informationsbereich; betont, dass gemeinsame Instrumente wie Handbücher für die Kommunikation ausgearbeitet werden müssen, die eine schnellere, koordinierte und genaue Kommunikation ermöglichen, bevor feindselige Narrative den Informationsraum übersättigen;

8. ist besorgt darüber, dass sich Russland auf Geschichtsrevisionismus beruft, insbesondere wenn es um den Zweiten Weltkrieg und das sowjetische Erbe, Informationsmanipulation und Einflussnahme aus dem Ausland sowie um die selektive Neuinterpretation historischer Ereignisse als Instrumente der hybriden Kriegsführung geht, die darauf abzielt, die öffentliche Meinung zu polarisieren, den gesellschaftlichen Zusammenhalt und die demokratische Resilienz zu untergraben und die territoriale Integrität souveräner Staaten zu delegitimieren;

9. betont, dass sich Informationsmanipulation und Einflussnahme aus dem Ausland über die traditionellen Medien hinaus auf Bildungs-, Kultur- und Religionsbereiche erstrecken; hebt den strategischen Einsatz religiöser Einrichtungen und religiöser Netzwerke hervor, einschließlich der Instrumentalisierung der Russisch-Orthodoxen Kirche, um moralische Autorität zu vermitteln, staatlich geförderte Narrative zu verbreiten und die gesellschaftliche Resilienz und den demokratischen Zusammenhalt schrittweise zu entkräften; fordert die EU ferner auf, hybride Bedrohungen aufzudecken, bei denen religiöse Kanäle ausgenutzt werden, und EU-Beamte in interreligiösem Engagement und religiöser Kompetenz sowie in der Erkennung von finanzieller Einflussnahme, der Vereinnahmung von Organisationen und der Manipulation von Informationen, durch die

demokratische Werte und der soziale Zusammenhalt untergraben werden, zu schulen;

10. verurteilt den Einsatz von Online-Plattformen durch feindselige Akteure für hybride Aktivitäten; fordert, dass die geltenden EU-Rechtsvorschriften über die Transparenz von Empfehlungssystemen, politische Werbung, koordiniertes unauthentisches Verhalten und die rasche Verbreitung manipulierter oder KI-generierter Inhalte im Zusammenhang mit feindseliger ausländischer Einflussnahme stärker durchgesetzt werden;

11. betont, dass feindselige Akteure immer anspruchsvollere und anpassungsfähigere hybride Techniken einsetzen; betont, dass KI-Instrumente – Deepfakes, algorithmische Verstärkung und automatisierte Kontennetze – solche Beeinflussungsoperationen schneller, kostengünstiger und schwerer erkennbar werden lassen; ist der Ansicht, dass bei der Reaktion der EU auf KI-gestützte Informationsmanipulation und Einflussnahme aus dem Ausland KI sowohl als Bedrohungsvektor als auch als entscheidende Fähigkeit im Bereich der Verteidigung angesehen werden muss;

12. stellt fest, dass die Antwort der EU auf Informationsmanipulation und Einflussnahme aus dem Ausland aufgrund des Mangels an Echtzeit-Fähigkeiten in den Bereichen Überwachung, Zuordnung und proaktive Reaktion nach wie vor defensiv ausfällt; besteht darauf, dass Informationsmanipulation und Einflussnahme aus dem Ausland als ernsthafte Sicherheitsbedrohung behandelt werden müssen, die einen operativen Ansatz, eine bessere Koordinierung und die Zusammenarbeit zwischen den Mitgliedstaaten auf allen Ebenen erfordern, darunter eine frühzeitige Aufdeckung, geeignete Reaktionsoptionen und einen besseren Schutz demokratischer Prozesse, insbesondere in Wahlkampfzeiten;

13. begrüßt die Arbeit des EAD bei der Überwachung, Aufdeckung und Reaktion auf Informationsmanipulation und Einflussnahme aus dem Ausland und betont, wie relevant das Schnellwarnsystem der EU für koordinierte gemeinsame Reaktionen auf Desinformation ist; legt der Kommission und den Mitgliedstaaten nahe, die Empfehlungen des Sonderausschusses für den Europäischen Schutzschild für die Demokratie (EUDS) zu bewerten und darauf aufzubauen; fordert, dass das Schnellwarnsystem weiter gestärkt wird, um gegen die Manipulation von Informationen in Echtzeit vorzugehen, wobei es mit klaren operativen Zuständigkeiten zu versehen ist; fordert standardisierte Prebunking- und Krisenreaktionsmechanismen in der gesamten EU und den Partnerländern, einschließlich strukturierter Frühwarn-Kommunikationskanäle; spricht sich für die Entwicklung proaktiver strategischer Kommunikationsinstrumente aus, mit denen die Bevölkerung im Voraus vor voraussichtlichen Taktiken der Desinformation, Narrativmustern und erfundenen Inhalten vor

kritischen Ereignissen wie Wahlen, Energieverhandlungen oder Sicherheitskrisen gewarnt werden kann;

14. fordert die Kommission, die Hohe Vertreterin und die Mitgliedstaaten überdies auf, das Instrumentarium gegen Informationsmanipulation und Einflussnahme aus dem Ausland vollständig einsatzbereit werden zu lassen und konsequent und koordiniert zu nutzen und den Leitfaden zur Abschreckung von Informationsmanipulation und Einflussnahme aus dem Ausland anzuwenden, was auch eine koordinierte öffentliche Zuordnung der Verantwortung und gegebenenfalls den Einsatz restriktiver Maßnahmen beinhaltet, die nicht nur auf einzelne Vorfälle ausgerichtet sind, sondern auch auf illegale Finanzströme, die technische Infrastruktur und die Vermittlungs- und Stellvertreternetze, die Operationen zur Informationsmanipulation und Einflussnahme aus dem Ausland unterstützen;

15. betont, dass die öffentliche Meinung in Europa nach wie vor ein vorrangiges Ziel russischer hybrider Operationen ist; weist darauf hin, dass Jahrzehnte des Friedens die Bedingungen für strategische Nachlässigkeit geschaffen haben, die durch Operationen der gegnerischen Einflussnahme ausgenutzt und vertieft werden; ist der Ansicht, dass die Regierungen und die EU-Organe gemeinsam dafür verantwortlich sind, dass die Öffentlichkeit ein Verständnis dafür entwickelt, wie eine hybride Bedrohung beschaffen ist und ob sie unmittelbar bevorsteht, und dass durch ein Versäumnis, dies zu tun, die Vorsorge und Abschreckung vereitelt werden;

16. fordert die Mitgliedstaaten auf, ressortübergreifende und gesamtgesellschaftliche Ansätze zu verfolgen und dabei der Resilienz und Vorsorge Vorrang einzuräumen, wie dies auch im Niinistö-Bericht hervorgehoben wird; weist darauf hin, dass hybride Bedrohungen die Gesellschaft als Ganzes ins Visier nehmen, da feindselige Akteure Schwachstellen in miteinander verbundenen Bereichen, Diensten, Gemeinschaften und Informationsräumen ausnutzen; ist davon überzeugt, dass Vertrauen und sozialer Zusammenhalt für die Resilienz von Gesellschaften von grundlegender Bedeutung sind; betont daher, dass die Resilienz gegenüber hybriden Bedrohungen über militärische, technische und institutionelle Maßnahmen hinausgehen muss, indem staatliche Stellen, der Privatsektor, die Zivilgesellschaft – einschließlich lokaler Gemeinschaften und schwer erreichbarer Wahlkreise –, Hochschulen und unabhängige Medien zusammengebracht werden, um das demokratische Vertrauen, das öffentliche Bewusstsein und die gesellschaftliche Vorsorge zu stärken und auf diese Weise eine neue europäische Sicherheitskultur zu fördern;

17. betont, dass die Resilienz der Öffentlichkeit gegenüber Informationsmanipulation und Einflussnahme aus dem Ausland durch politische Bildung, Medienkompetenz, strategische

Kommunikation, Unterstützung für unabhängige Medien, darunter für investigativen Journalismus, Netze zur Faktenprüfung wie die Europäische Beobachtungsstelle für digitale Medien und KI-gestützte Instrumente zur Erkennung und Analyse von Desinformationskampagnen in großem Maßstab gestärkt werden muss; fordert eine engere Zusammenarbeit mit Medien und audiovisuellen Akteuren, wenn es darum geht, Informationsmanipulation und Einflussnahme aus dem Ausland aufzudecken, die Verantwortung dafür zuzuordnen und darauf zu reagieren; fordert Anreize, unter anderem durch öffentlich-private Initiativen, für die Aufdeckung, Analyse und Zuweisung der Verantwortung bei Informationsmanipulation und Einflussnahme aus dem Ausland, sichere Mechanismen für den Datenaustausch und interoperable Frühwarnsysteme;

18. ist besorgt über anhaltende Berichte über Einflussnahme aus dem Ausland auf Wahlen in Europa, unter anderem durch Cyberangriffe und KI-gestützte Desinformation; erinnert daran, dass die Integrität und Resilienz von Wahlprozessen ausschlaggebend für die demokratischen Grundlagen der EU und ein zentrales Ziel hybrider Operationen sind; betont, dass Informationsmanipulation und Einflussnahme aus dem Ausland im Vorfeld von Wahlen tendenziell zunehmen und dass kontinuierliche Wachsamkeit und Koordinierung daher von wesentlicher Bedeutung sind, um die Integrität von Wahlen und die demokratische Stabilität in der gesamten EU und in Partnerländern, darunter in Kandidatenländern und potenziellen Kandidatenländern, zu wahren; begrüßt die Gemeinsame Mitteilung mit dem Titel „Europäischer Schutzschild für die Demokratie: Förderung starker und widerstandsfähiger Demokratien“ und die Einrichtung eines Europäischen Zentrums für demokratische Resilienz und fordert eine klare Definition seiner Aufgaben, um Überschneidungen mit bestehenden Initiativen zu vermeiden;

19. fordert, dass kognitive Verwundbarkeiten im Zusammenhang mit hybrider Kriegsführung in der künftigen Sicherheitsstrategie der EU anerkannt und angegangen werden und dass die Kommission weitere Schritte unternimmt, indem sie eine Kartierung kognitiver Verwundbarkeiten und Referenzwerte für die Resilienz bereitstellt;

***Cybersicherheit***

20. betont, dass Cyberangriffe zu einem zentralen Element hybrider Kampagnen geworden sind, wobei die zunehmende Digitalisierung kritischer Bereiche wie Gesundheitsversorgung, Finanzen und Energie ausgenutzt wird, um durch Kettenreaktionen fortsetzende Ausfälle auszulösen, die schwerwiegende wirtschaftliche und gesellschaftliche Folgen haben können;

21. stellt fest, dass sich der Cyberraum als fünfter militärischer Bereich und als zentraler Wegbereiter hybrider Bedrohungen etabliert hat;

betont, dass die Cybersicherheit angesichts der zunehmenden Abhängigkeit militärischer Plattformen, kritischer Infrastrukturen und der Befehls-, Kontroll-, Kommunikations- und Nachrichtensysteme von digitalen Technologien für die operative Überlegenheit und Resilienz in allen Bereichen nunmehr von wesentlicher Bedeutung ist; betont daher, dass souveräne Cyberfähigkeiten zur Erkennung, Zuordnung der Verantwortung, Reaktion und Aufklärung erforderlich sind, zu denen auch Offensivfähigkeiten gehören, um Bedrohungen zu neutralisieren und für eine überzeugende Abschreckung zu sorgen;

22. hebt hervor dass Informationsmanipulation und Einflussnahme aus dem Ausland unmittelbar den Bereich der Cybersicherheit betreffen und stellt fest, dass Cyberangriffe häufig in den frühen Phasen von Kampagnen zur Informationsmanipulation und Einflussnahme aus dem Ausland stattfinden; fordert, dass Mechanismen zur Bekämpfung von Informationsmanipulation und Einflussnahme aus dem Ausland systematisch mit Cybersicherheitskapazitäten verknüpft werden, um koordinierte Manipulationsinfrastrukturen frühzeitig zu erkennen, zuzuordnen und auszuschalten;

23. warnt vor den Risiken, die von konvergenten Cyberoperationen ausgehen, bei denen staatsnahe Akteure aktiv die operativen Profile, Methoden und Persönlichkeitsprofile unabhängiger Hacktivisten oder kommerziell motivierter Cyberkriminelle übernehmen, um die Zuordnung zu verschleiern und Cyberaktivitäten mit geopolitischen Ereignissen, Wahlen oder kinetischen Operationen in Verbindung zu bringen; betont, dass bei der Reaktion auf hybride Cyberbedrohungen klar zwischen legitimen Formen politischer Meinungsäußerung oder abweichender Meinung in der Bevölkerung sowie zwischen finanziell motivierter Cyberkriminalität und staatlich geförderten Operationen unterschieden werden muss, damit die Grundfreiheiten geschützt und gleichzeitig die Zuordnung, Rechenschaftspflicht und Abschreckung verbessert werden;

24. warnt davor, dass durch die Ausweitung des Internets der Dinge das Risiko erhöht wird, dass Cyberangriffe physische Auswirkungen auf kritische Infrastrukturen und grundlegende Dienste nach sich ziehen, und fordert Verpflichtungen zur eingebauten Sicherheit, um dafür zu sorgen, dass vernetzte Geräte nicht zu einem Einfallstor für hybride Operationen mit konkreten Folgen werden;

25. warnt davor, dass es keinen vollständigen Cyberschutz gibt und dass ein Umdenken im Hinblick auf Cyberresilienz erforderlich ist; betont, dass die Cyberresilienz Europas durch häufige und realistische Cyberübungen aufgebaut werden muss; betont, dass die Cyberresilienz nicht nur Systeme betrifft, sondern auch den Schutz von Daten, die sowohl das Angriffsziel als auch das Einfallstor für hybride Bedrohungen darstellen können; betont ferner, dass die Cyberresilienz im gesamten europäischen Wirtschaftsgefüge, zu dem

auch kleine und mittlere Unternehmen (KMU) und Anbieter wesentlicher digitaler Dienste gehören, gestärkt werden muss;

26. hebt den Mehrwert der EU bei der Unterstützung der Mitgliedstaaten hervor, wenn es darum geht, nationale Fähigkeiten miteinander zu verknüpfen, ein gemeinsames Lagebewusstsein aufzubauen und schnellere und kohärentere Reaktionen auf hybride Bedrohungen zu ermöglichen; empfiehlt der Kommission, Vorschläge für einen einheitlicheren Rahmen zur Unterstützung der Mitgliedstaaten bei der Planung, operativen Koordinierung und Durchführung von Cyberoperationen zu prüfen; begrüßt den Abschluss des im Rahmen der Ständigen Strukturierten Zusammenarbeit (SSZ) betriebenen Projekts zum Koordinierungszentrum für den Cyber- und Informationsraum (CIDCC) und die Fortschritte bei seiner Umgestaltung in ein ständiges EU-Koordinierungszentrum für die Cyberabwehr (EUCDCC);

27. fordert eine stärkere Harmonisierung der Verpflichtungen zur Meldung von Sicherheitsvorfällen und der wichtigsten Rechtskonzepte im EU-Rahmen für Cybersicherheit und Resilienz, um die Fragmentierung zu verringern, die Interoperabilität zu verbessern und sicherzustellen, dass die rasche Wiederherstellung wesentlicher Dienste in hybriden Krisenszenarien eine zentrale Priorität bleibt;

28. nimmt die von der Agentur der Europäischen Union für Cybersicherheit (ENISA) im Rahmen des Cybersolidaritätsgesetzes verwaltete EU-Cybersicherheitsreserve als strategische Fähigkeit der EU zur raschen Reaktion auf Cybervorfälle zur Kenntnis; fordert, dass ihre Finanzierung an die operative Nachfrage angepasst wird, und hebt ihren ersten Einsatz in Moldau als wichtigen Schritt zur Stärkung der operativen Cyberresilienz der EU und als Unterstützung der Partnerländer hervor; fordert die für Cybersicherheit zuständigen Behörden der Mitgliedstaaten auf, die strukturierte Zusammenarbeit mit vertrauenswürdigen Anbietern, die sich an der Reserve beteiligen, zu fördern, um die verfügbaren Kapazitäten für die Reaktion auf Vorfälle in vollem Umfang zu nutzen, wenn hybride Bedrohungen durch schwerwiegende Cybervorfälle oder Cybervorfälle großen Ausmaßes auftreten;

29. bekräftigt die Bedeutung des als ständige Cyberabwehrfähigkeit fungierenden SSZ-Teams für die rasche Reaktion auf Cybervorfälle, das auf Ersuchen von Mitgliedstaaten, Partnerländern und Missionen im Rahmen der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP), die mit Cyberangriffen mit Auswirkungen auf Sicherheit und Verteidigung konfrontiert sind, eingesetzt werden kann, und fordert eine angemessene Ressourcenausstattung durch die EU;

30. bekräftigt, wie wichtig es ist, das Instrumentarium für die Cyberdiplomatie in vollem Umfang zu nutzen, um Cyberbedrohungen und böswillige Cyberaktivitäten zu verhindern, davon abzuschrecken und darauf zu reagieren; nimmt zur Kenntnis, dass im März 2026 der erste ständige globale Mechanismus der Vereinten Nationen für Cybersicherheit ins Leben gerufen wurde, und ist der Ansicht, dass sich die EU dabei auf Bereiche konzentrieren sollte, in denen ein eindeutiger europäischer Mehrwert besteht, während die europäische Cyberdiplomatie gleichzeitig weiter gestärkt wird;

31. betont, dass Cyberresilienz und Abwehrmaßnahmen nicht ausreichen, um eine glaubwürdige Abschreckung vor hybriden Bedrohungen sicherzustellen, wie dies auch im Gemeinsamen Weißbuch zur europäischen Verteidigung – Bereitschaft 2030 hervorgehoben wird; fordert die Kommission und die Mitgliedstaaten auf, in Zusammenarbeit mit der NATO die rechtlichen, verfahrenstechnischen und operativen Voraussetzungen für verhältnismäßige und rechtskonforme Cyberabwehrmaßnahmen zu prüfen; begrüßt die Fortschritte bei der Einrichtung des CDCC der EU und fordert dessen rasche Operationalisierung und die Umsetzung eines Mandats im Einklang mit den Schlussfolgerungen des Rates zur Cyberabwehrpolitik der EU, um eine glaubwürdigere und leistungsfähigere Cyberabwehr der EU zu erreichen;

32. weist in diesem Zusammenhang warnend darauf hin, dass KI nicht nur ein Instrument ist, das bei hybriden Cyberaktivitäten eingesetzt wird, sondern auch eine kritische Technologie, die durch Manipulation mittels bestimmter Eingaben („Prompt Injection“), die Beeinflussung von Trainingsdaten („Training Data Poisoning“) und Angriffe auf die Lieferkette selbst zum Ziel, manipuliert oder beeinträchtigt werden kann; betont, dass die EU angesichts der zunehmenden Abhängigkeit von kommerziellen KI-Systemen und KI-Systemen mit doppeltem Verwendungszweck im zivilen, sicherheits- und verteidigungsbezogenen Kontext einen klaren Standpunkt zur Cybersicherheit, Widerstandsfähigkeit und Governance von KI mit doppeltem Verwendungszweck entwickeln muss, darunter Schutzvorkehrungen für die Modellintegrität, vertrauenswürdige Lieferketten und Aufsicht an der Grenze zwischen zivilen Anwendungen, verteidigungsbezogenen Anwendungen und Anwendungen im Bereich der nationalen Sicherheit;

33. betont, dass kritische öffentliche digitale Infrastrukturen und sensible staatlich verwaltete Datenregister, einschließlich der Wahlinfrastruktur, besser geschützt werden müssen, da sie angesichts ihrer Rolle in den Bereichen digitale Identität, öffentliche Verwaltung, Daten-Governance, sichere Kommunikation, Zugang zu wesentlichen Dienstleistungen und Integrität demokratischer Prozesse potenzielle Ziele hybrider Bedrohungen bilden könnten;

***Kritische Infrastruktur***

34. verurteilt die hybriden Angriffe auf die kritische Infrastruktur der EU, insbesondere auf die Energie-, Verkehrs-, Kommunikations- und Satelliteninfrastruktur, einschließlich der Infrastruktur für die militärische Mobilität, zumal diese Infrastrukturen sowohl als entscheidende Voraussetzungen als auch als strategische Vermögenswerte für die kollektive Verteidigung der EU, die Resilienz und den Schutz der Zivilbevölkerung fungieren; betont, dass diese kritische Infrastruktur als vernetztes System funktioniert, das nicht isoliert geschützt werden kann, und dass durch eine größere digitale Konnektivität die Anfälligkeit erhöht wird; begrüßt, dass im Vorschlag der Kommission für eine Verordnung über die militärische Mobilität (COM(2025)0847) und im Vorschlag der Kommission für Leitlinien für die transeuropäische Energieinfrastruktur (COM(2025)1006) der Schwerpunkt auf den Schutz und die Resilienz der Infrastruktur für Energie und militärische Mobilität gelegt wird; fordert die Kommission und die Mitgliedstaaten auf, alle erforderlichen Maßnahmen zu ergreifen, damit diese Infrastruktur geschützt wird;

35. betont, dass der Weltraumbereich zu einem immer wichtigeren Schauplatz für hybride Kriegsführung geworden ist, wobei feindliche Akteure mit Cyberoperationen, physischen Angriffen, Jamming und Spoofing satellitengestützte Kommunikations-, Navigations- und Beobachtungssysteme ins Visier nehmen oder strategische Abhängigkeiten ausnutzen; betont, dass sich die Störung von Weltraumressourcen in erheblicher Weise auf die zivile Sicherheit, die kritische Infrastruktur, die militärische Mobilität und die Krisenreaktionsfähigkeiten der EU auswirken kann; fordert daher eine Stärkung der Resilienz der Raumfahrtsysteme der EU, auch durch eine bessere Weltraumlageerfassung, den Schutz der Bodeninfrastruktur, Cybersicherheitsanforderungen, die Sicherheit der Lieferketten, regelmäßige Übungen sowie alternative oder Backup-Kapazitäten in den Bereichen Ortung, Navigation und Zeitgebung; fordert die weitere Integration des Bereichs Weltraum in den umfassenderen Rahmen der EU für die Abwehr hybrider Bedrohungen;

36. stellt fest, dass feindselige Akteure, vor allem Russland, Energieinfrastruktur, Energiemärkte und Energieabhängigkeiten zunehmend als Waffe einsetzen, um politischen Druck auszuüben; betont die strategische Bedeutung kritischer Energieinfrastrukturen sowohl für die Verteidigung als auch für den zivilen Bedarf; fordert die Kommission und die EU-Mitgliedstaaten nachdrücklich auf, beim nächsten Mehrjährigen Finanzrahmen 2028-2034 einen rechtlichen und finanziellen Rahmen der EU festzulegen, mit dem ein ausreichender Schutz und eine ausreichende Resilienz kritischer Energieinfrastruktur sichergestellt werden, indem den Vorschlägen der Kommission für Leitlinien für die transeuropäische Energieinfrastruktur (COM(2025)1006) und zur Schaffung der

Fazilität „Connecting Europe“ (COM(2025)0547) Vorrang eingeräumt wird;

37. verurteilt die Aktivitäten der Schattenflotte Russlands, durch die das Risiko von Seeunfällen erhöht, staatliche Sabotage verschleiert und kritische Infrastruktur wie Unterseekabel, Offshore-Energieanlagen und Hafenanlagen gefährdet wird; verlangt bessere Überwachungs-, Inspektions- und Durchsetzungsmaßnahmen in europäischen Gewässern und fordert die EU auf, ihre Reaktion auf hybride Bedrohungen in Meeresgebieten zu verstärken; legt der Kommission nahe, ausgehend von der Sicherheitsinitiative zur Unterbindung der Verbreitung von Massenvernichtungswaffen als Vorbild rechtliche und operative Rahmenbedingungen zu prüfen, um das Anbordgehen auf Schiffen zu ermöglichen, die mit Schattenflotten in Verbindung stehen, und fordert die Arbeitsgruppe „Bekämpfung der Geldwäsche und Terrorismusfinanzierung“ auf, die Rolle undurchsichtiger Eigentumsstrukturen, Flaggenregister und damit verbundener Finanznetzwerke bei der Erleichterung der Umgehung von Sanktionen und bei illegalen Finanzströmen weiter zu untersuchen;

38. betont, dass Unterseekabel aufgrund ihrer physischen Exposition und möglicher systemischer Störungen eine zentrale strategische Schwachstelle und Ziel hybrider Sabotage-, Spionage- und Einflussoperationen darstellen, zumal sie den überwiegenden Teil des interkontinentalen Internetverkehrs übertragen; würdigt die Empfehlung der Kommission von 2024 über sichere und resiliente Seekabelinfrastrukturen[9] und die gemeinsame Mitteilung von 2025 über den EU-Aktionsplan für Kabelsicherheit (JOIN(2025)0009) als wichtige erste Schritte hin zur Stärkung der Sicherheit und Resilienz von Seekabelinfrastrukturen; fordert ferner, dass Fähigkeiten zur maritimen Lageerfassung eingesetzt werden, die Satelliten-, Oberflächen- und Unterwassersensordaten umfassen, damit physische Bedrohungen für Seekabel- und Offshore-Energieinfrastrukturen in strategischen Meeresgebieten, darunter in den Gebieten der Ostsee, der Nordsee, des Schwarzen Meeres, der Arktis und des Mittelmeers, erkannt, überwacht und zugeordnet werden können; empfiehlt strenge Bestimmungen über die strafrechtliche Haftung, um von solchen Angriffen abzuschrecken, sowie redundante Systeme, um die Resilienz sicherzustellen; betont überdies, dass es einen umfassenden, mehrschichtigen Ansatzes bedarf, um technologische Innovationen, eine vermehrte Einbindung der Nachrichtendienste, verbesserte Zuordnungsfähigkeiten und eine verstärkte Zusammenarbeit zwischen der NATO, den EU-Mitgliedstaaten und einschlägigen Akteuren der Privatwirtschaft zu

---

9 Empfehlung (EU) 2024/779 der Kommission vom 26. Februar 2024 über sichere und resiliente Seekabelinfrastrukturen (ABl. L, 2024/779, 8.3.2024, ELI: http://data.europa.eu/eli/reco/2024/779/oj).

bündeln, damit ein kohärenter Schutz der Unterseeinfrastruktur gegeben ist;

39. fordert die Kommission und die Mitgliedstaaten auf, für eine koordinierte, EU-weite Auslegung des Seerechtsübereinkommens der Vereinten Nationen (SRÜ) zu sorgen, um ein kohärentes Vorgehen gegen hybride Aktivitäten, Sabotageakte und Verletzungen der Hoheitsrechte in den Meeresgebieten der EU, insbesondere in der Ostsee, sicherzustellen und wirksam davor abzuschrecken und solche Aktivitäten zu einem Straftatbestand zu erklären, und weist gleichzeitig auf den Zweck des SRÜ hin, die friedliche Nutzung der Meere sicherzustellen; fordert die Kommission und die Mitgliedstaaten auf, das Beispiel Australiens heranzuziehen, das „Kabelschutzzonen“ eingerichtet, rechtliche Schutzmaßnahmen ergriffen und die Beschädigung von Seekabeln außerhalb der Hoheitsgewässergrenze von 12 Seemeilen unter Strafe gestellt hat, was von einer aktiven Beobachtung, Überwachung und Reaktion in Zusammenarbeit mit den relevanten Partnern aus Drittländern flankiert wurde;

40. fordert die Mitgliedstaaten und die Europäische Verteidigungsagentur (EDA) auf, die SSZ-Projekte „Schutz kritischer Infrastruktur im Meer“ (CSIP), „Hafen- und Meeresüberwachung und -schutz“ (HARMSPRO), „Integriertes mehrschichtiges Luftverteidigungs- und Raketenabwehrsystem“ (IMLAMD) und „Abwehrsystem für unbemannte Flugsysteme“ (C-UAS) voranzubringen, um die Überwachungs-, Erkennungs- und Verteidigungsfähigkeiten gegenüber Bedrohungen aus der Luft und maritimen Bedrohungen zu fördern; fordert die Kommission auf, in Zusammenarbeit mit der Hohen Vertreterin und in Absprache mit den Mitgliedstaaten ein europäisches Verteidigungsvorhaben von gemeinsamem Interesse vorzuschlagen, das für die integrierte Verteidigung der Meeresumwelt und der Tiefsee bestimmt ist;

41. begrüßt, dass die Richtlinie über die Resilienz kritischer Einrichtungen[10] und die NIS-2-Richtlinie[11] verabschiedet wurden, da es sich hierbei um wichtige Schritte zur Stärkung der Widerstandsfähigkeit gegenüber hybriden Angriffen handelt, betont

---

10 Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates (ABl. L 333 vom 27.12.2022, S. 164, ELI: http://data.europa.eu/eli/dir/2022/2557/oj).

11 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (ABl. L 333 vom 27.12.2022, S. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

jedoch, dass Verzögerungen bei der Umsetzung in den Mitgliedstaaten eine gemeinsame, dringend zu behebende Schwachstelle darstellen, und fordert die vollständige und rechtzeitige Umsetzung; fordert die Kommission nachdrücklich auf, ihre Überwachungs- und Durchsetzungsbefugnisse in vollem Umfang zu nutzen; fordert die Mitgliedstaaten auf, die konzeptionelle Resilienz als Standardanforderung in alle neuen und überarbeiteten Rechtsvorschriften aufzunehmen;

42. ist besorgt über ausländisches Eigentum, insbesondere Russlands und Chinas, an kritischer Infrastruktur in der EU, das das Risiko von Spionage, Einflussnahme und strategischer Abhängigkeit erheblich erhöht; begrüßt die zwischen dem Parlament und dem Rat erzielte politische Einigung über einen verstärkten Überprüfungsmechanismus der EU für ausländische Direktinvestitionen (ADI); fordert die Mitgliedstaaten auf, diese Verordnung rasch durchzuführen und sie, wenn möglich, durch einen Ansatz der bevorzugten Beschaffung europäischer Güter („Buy European“) in den Bereichen kritische Infrastruktur und Verteidigungsgüter zu ergänzen, um die strategische Autonomie der EU zu stärken;

43. stellt fest, dass sich ein erheblicher Teil der kritischen Infrastruktur, die mit grundlegenden öffentlichen Diensten und militärischen Fähigkeiten verbunden ist, in privatem Eigentum befindet oder privat betrieben wird; fordert ständige und strukturierte Rahmen für die öffentlich-private Zusammenarbeit, auch für den Informationsaustausch, die Notfallplanung und eine koordinierte Krisenreaktion; betont, dass die staatlichen Stellen in Fällen, in denen durch private Infrastruktur wesentliche Dienste und sensitive Daten unterstützt werden, für eine wirksame regulatorische und operative Kontrolle sorgen müssen; fordert, dass Erfordernisse im Bereich Verteidigung bei der Planung, Gestaltung und Finanzierung ziviler Infrastruktur systematisch berücksichtigt werden; beharrt darauf, dass von der EU finanzierte Infrastruktur als Voraussetzung für die Unterstützung durch die EU verteidigungsrelevante Resilienzstandards erfüllen muss; fordert darüber hinaus, dass Entwickler von Verteidigungstechnologien und Bereitsteller von Sicherheit systematisch in die frühen Phasen der Bewertung der Bedrohungslage und der Notfallplanung für kritische Infrastrukturen einbezogen werden, damit die verfügbaren technologischen Fähigkeiten in den Resilienzrahmen der Mitgliedstaaten und der EU berücksichtigt werden; nimmt den Beitrag von KMU, Start-up-Unternehmen und Anbietern innovativer Technologien zur Resilienz und zum Schutz kritischer Infrastruktur zur Kenntnis und fordert ihre stärkere Beteiligung an einschlägigen Programmen, Beschaffungsprogrammen und öffentlich-privaten Partnerschaften der EU;

44. fordert die Mitgliedstaaten auf, regelmäßige Vorsorge- und Resilienzübungen im Bereich kritische Infrastruktur durchzuführen, einschließlich gemeinsamer Übungen, und dringend die im Weißbuch zur europäischen Verteidigung genannten vorrangigen Fähigkeiten bereitzustellen, insbesondere Luft- und Raketenabwehr, Drohnen und Drohnenabwehrsysteme, militärische Mobilität, Cyberkriegsführung und elektronische Kriegsführung sowie maritime Fähigkeiten;

45. ist besorgt über die strukturelle Abhängigkeit der EU von Drittländern mit hohem Risiko – insbesondere von China –, was die Bereitstellung von vernetzter Hard- und Software betrifft, darunter Solar-Wechselrichter, Windturbinen, vernetzte Fahrzeuge und digitale Geräte für Verbraucher, mit denen aus der Ferne auf Systeme zugegriffen werden kann, Informationen gesendet und Systeme kontrolliert werden können und die daher eine erhebliche Schwachstelle darstellen; fordert die Kommission auf, die Bewertungen der Sicherheit der Lieferketten systematisch auf alle Sektoren mit kritischer Infrastruktur auszuweiten und die Bemühungen um die Verringerung strategischer Abhängigkeiten zu beschleunigen; fordert die Mitgliedstaaten auf, Folgemaßnahmen zu diesen Bewertungen zu ergreifen, die Lieferketten zu diversifizieren und europäischen und gleich gesinnten Lieferanten in strategischen Bereichen Vorrang einzuräumen, wann immer dies aus Sicherheitsgründen erforderlich ist; begrüßt, dass die vorgeschlagene Überarbeitung des Rechtsakts zur Cybersicherheit darauf abzielt, einen Rahmen für das Verbot vernetzter Komponenten von Hochrisikoanbietern zu schaffen, und dass der Strategische Fahrplan für Digitalisierung und KI im Energiebereich als Teil des Pakets zur technologischen Souveränität Europas eine Überprüfung des Rahmens für die Energieversorgungssicherheit vorsieht; fordert, dass diese Maßnahmen rasch angenommen werden;

46. erachtet es als dringend geboten, dass die Versorgungswege durch sichere und widerstandsfähige Verkehrsnetze mit vertrauenswürdigen Partnern diversifiziert werden, um strategische Abhängigkeiten zu verringern und die wirtschaftliche Sicherheit und die Widerstandsfähigkeit der Lieferketten in der EU zu stärken;

47. betont, dass kritische und neu entstehende Technologien, einschließlich KI, Cloud-Infrastruktur, fortgeschrittener Halbleiter, Quantentechnologien, Cyber- und Weltraumtechnologien, autonomer Systeme und sicherer Kommunikation, angesichts ihrer wesentlichen Funktion für die Verteidigungsbereitschaft, wirtschaftliche Widerstandsfähigkeit und Betriebskontinuität Teil der kritischen Sicherheitsinfrastruktur der EU sind; hält eine widerstandsfähige, wettbewerbsfähige digitale Infrastruktur der EU – einschließlich sicherer lokaler Rechenzentren, einer souveränen EU-Cloud, Edge-Computing und Gigabit-Netzen – für eine wichtige Säule der

Sicherheit in Europa; betont, dass die Fähigkeit der EU, hybride Kampagnen zu erkennen, ihnen standzuhalten und darauf zu reagieren, von ihrer Fähigkeit abhängt, diese Technologien innerhalb einer widerstandsfähigen industriellen und technologischen Basis Europas zu entwickeln, zu sichern und zu skalieren, was durch ausreichende Investitionen der EU unterstützt werden muss, einschließlich Investitionen in sichere, interoperable und widerstandsfähige Systeme für den Informationsaustausch und lokale Rechenzentren, die keinen extraterritorialen Rechtsvorschriften unterliegen;

***Lagebewusstsein***

48. betont, dass eine wirksame Abwehr hybrider Bedrohungen die Prävention, frühzeitige Antizipation von Bedrohungen und die kontinuierliche Überwachung strategischer Schwachstellen, um feindselige Handlungen zu neutralisieren, bevor sie systemische Auswirkungen haben, und ein gemeinsames Bedrohungsbild erfordert, da die betroffenen Bereiche auf der Grundlage isolierter Berichte über Vorfälle nicht wirksam reagieren können; hebt in diesem Zusammenhang den potenziellen einzigartigen Mehrwert der EU hervor, wenn es darum geht, grenzüberschreitende Daten zusammenzuführen, um bei koordinierten hybriden Kampagnen Muster aufzudecken, die kein Mitgliedstaat im Alleingang erkennen könnte, sowie die Entwicklung von Verfahren für ein gemeinsames Lagebewusstsein und die Zuordnung, gemeinsame Rahmen, Methoden, Taxonomien und Interoperabilitätsprotokolle zwischen den einschlägigen Stellen und Strukturen der EU und der Mitgliedstaaten zu koordinieren, die die operative Zusammenarbeit zwischen den Mitgliedstaaten begünstigen würden; fordert, dass diese Aufgaben formell als Koordinierungs- und Unterstützungsbefugnisse der EU anerkannt werden;

49. stellt fest, dass die EU-Analyseeinheit für hybride Bedrohungen im Rahmen des Einheitlichen Analyseverfahrens (SIAC) nach wie vor die zentrale Stelle der EU ist, die über exklusive Fachkompetenz im Bereich der Analyse hybrider Bedrohungen aus allen Informationsquellen verfügt und für ein erkenntnisgestütztes Lagebewusstsein sorgt; bekräftigt, dass das SIAC in den EU-Organen das gemeinsame Zentrum für nachrichtendienstliche Erkenntnisse sein sollte, und hebt seinen besonderen Status innerhalb der Sicherheitsarchitektur der EU hervor; unterstützt die Analyse von Trends bei hybriden Bedrohungen als wichtiges Instrument zur Analyse hybrider Bedrohungen sowie zur Erkennung von Mustern und spricht sich für ihre angemessene Einbeziehung in die politischen Entscheidungsprozesse aus;

50. weist darauf hin, dass bei der Verwirklichung des im Strategischen Kompass und im Gemeinsamen Papier der Hohen Vertreterin und der Mitgliedstaaten zur Stärkung des Einheitlichen

Analyseverfahrens der EU (EAD(2024)2014) vorgesehenen Ziels, das SIAC durch die Bereitstellung zusätzlicher Ressourcen zu stärken, um relevante Informationen zusammenzutragen, zu analysieren und einzuordnen und so eine effiziente Bereitstellung von Erkenntnissen in den Bereichen Cyberbedrohungen und hybride Bedrohungen für die EU zu ermöglichen, keine Fortschritte erzielt wurden; fordert die Kommission, die Hohe Vertreterin und die Mitgliedstaaten auf, sich nachdrücklich für eine wirksame Stärkung des SIAC einzusetzen;

51. fordert die Mitgliedstaaten nachdrücklich auf, den Austausch von Erkenntnissen, auch mit dem EU INTCEN und der Direktion „Aufklärung“ des Militärstabs der Europäischen Union (EUMS), zu verstärken und dabei die Souveränität der Mitgliedstaaten, den Grundsatz „Kenntnis nur, wenn nötig“ und den Schutz von Verschlusssachen der Mitgliedstaaten zu achten; betont, dass daten- und erkenntnisgestützte Bewertungen systematisch in die Planung, das Krisenmanagement und die Politikgestaltung der EU einbezogen werden müssen;

52. fordert die EU-Organe auf, in Zusammenarbeit mit den Mitgliedstaaten und dem EAD ein sicheres System für den Informationsaustausch, das den Grundsätzen „Kenntnis nur, wenn nötig“ und „Need-to-share“ gerecht wird, zu prüfen, bei dem die EU als Vermittlerin fungieren und Behörden, einschlägige Einrichtungen der EU, nationale und internationale Stellen, Betreiber kritischer Infrastruktur, private Unternehmen und vertrauenswürdige Quellen für Bedrohungsinformationen zusammenführen würde, um das kollektive Lagebewusstsein zu stärken und gleichzeitig den größtmöglichen Schutz sensibler Informationen sicherzustellen; ist der Ansicht, dass ein solches System Anreize für die teilnehmenden Stellen schaffen würde, Informationen auszutauschen, da sie in die Lage versetzt würden, aus einem vollständigeren Bedrohungsbild und hochwertigeren nachrichtendienstlichen Ergebnissen Nutzen zu ziehen und gleichzeitig schrittweise das für einen sachgerechten Informationsaustausch erforderliche Vertrauen aufzubauen;

53. fordert die Verfassung eines „Schwarzbuchs der hybriden Aggression, unter anderem Russlands und Chinas“, um jede hybride Operation gegen die EU und ihre Mitgliedstaaten der letzten zehn Jahre öffentlich zu dokumentieren; besteht darauf, dass das „Schwarzbuch“ jährlich im Rat erörtert und dem Parlament vorgelegt wird, um den betreffenden Staaten weitere Kosten aufzuerlegen;

***Von der Fragmentierung hin zu einer koordinierten und entschlossenen Reaktion Europas***

54. betont, dass die EU nur durch eine vertiefte Integration und Koordinierung und eine größere Verteidigungsbereitschaft und umfassendere Verteidigungsfähigkeiten, unter anderem durch die

Weiterentwicklung der technologischen und industriellen Basis der europäischen Verteidigung, wirksam auf eskalierende hybride und konventionelle Bedrohungen reagieren kann;

55. ist der Ansicht, dass die EU von einer reaktiven zu einer proaktiven Strategie übergehen muss, die die Nutzung ihrer Fähigkeiten umfasst, hybride Bedrohungen zu stören, davor abzuschrecken und darauf zu reagieren und die Kosten feindseliger Handlungen glaubwürdig zu erhöhen; betont, dass jeder Verletzung der Souveränität der Mitgliedstaaten mit wirksamen, verhältnismäßigen und koordinierten Vergeltungsmaßnahmen begegnet werden muss;

56. betont, dass zur wirksamen Abwehr und Abschreckung hybrider Bedrohungen ein gemeinsames und umfassendes Bedrohungsbild erforderlich ist, dem gemeinsame Rahmen, Methoden, Taxonomien und operative Standards zugrunde liegen; betont, dass diplomatische, rechtliche, wirtschaftliche und restriktive Maßnahmen kombiniert werden müssen, um hybride Operationen zu unterbinden, aufzudecken, zu identifizieren, zuzuordnen und darauf zu reagieren, unter anderem durch asymmetrische Maßnahmen in allen relevanten Dimensionen; fordert die Kommission, die Hohe Vertreterin und den Rat auf, einen dimensionsübergreifenden Aktionsplan gegen hybride Kriegsführung auszuarbeiten, der auch eine verstärkte zivil-militärische Zusammenarbeit, operative Handbücher, kooperative und effiziente Reaktionsprotokolle, einschließlich gezielter EU-Vergeltungsoptionen, die in einem angemessenen Verhältnis zur Schwere feindseliger Aktivitäten stehen, und klare Reaktionsketten umfasst, die mit denen der NATO interoperabel sind und diese ergänzen, wobei die EU und die Mitgliedstaaten bei Bedarf weiterhin unabhängig handeln können müssen; fordert die Benennung einer zentralen Koordinierungsstelle für die Kommission und den EAD, um eine echte EU-weite Herangehensweise an hybride Bedrohungen zu etablieren;

57. begrüßt die laufenden Initiativen zur Stärkung der operativen Kapazitäten, einschließlich der EU-Teams für die rasche Reaktion auf hybride Bedrohungen und der Einführung des EU-Schutzschilds für die Ostflanke und der Europäischen Drohnenabwehrinitiative; fordert rasche Fortschritte bei ihrem Einsatz; betont, dass regionale Verteidigungs- und Sicherheitscluster von strategischer Bedeutung sind, und fordert spezielle EU-Finanzierungsoptionen, um ihr Know-how und ihre Fähigkeiten in grenzüberschreitende Projekte zur Verbesserung der Resilienz Europas zu integrieren;

58. begrüßt, dass die Kommission und die Hohe Vertreterin eine neue globale Sicherheitsstrategie der EU angekündigt haben, und fordert, dass damit umfassend gegen das gesamte Spektrum hybrider Bedrohungen vorgegangen wird;

59. besteht darauf, dass dringend Fortschritte auf dem Weg zu einer echten Europäischen Verteidigungsunion als stärkere europäische Säule der NATO erzielt werden müssen, die trennbar, jedoch nicht getrennt ist und es der EU und ihren Mitgliedstaaten ermöglicht, erforderlichenfalls unabhängig zu handeln; fordert, dass die Beistandsklausel (Artikel 42 Absatz 7 EUV) in Szenarien von bewaffneten Angriffen und schwerwiegenden hybriden Vorfällen weiter operationalisiert wird; fordert ferner ein Handbuch zu Artikel 42 Absatz 7 – einen kurz und bündigen, aber umfassenden operativen Leitfaden für die nationalen Regierungen und die EU-Organe, in dem erläutert wird, was vor, während und nach der Geltendmachung des Artikels durch einen Mitgliedstaat geschieht; ist der Ansicht, dass das Handbuch regelmäßig in Szenarien schwerer hybrider Krisen und durch umfassende bereichsübergreifende Übungen getestet werden sollte;

60. betont, dass einige hybride Angriffe Russlands gegen die EU und ihre Mitgliedstaaten staatlich gesponsertem Terrorismus gleichkommen könnten; fordert die Mitgliedstaaten auf, alle verfügbaren Rechtsinstrumente zu nutzen, um diese Angriffe abzuwehren, einschließlich der Solidaritätsklausel (Artikel 222 AEUV), und dabei die Kooperations- und Koordinierungsmechanismen, die zur Verfügung stehen, wenn die Klausel aktiviert wird, in vollem Umfang zu nutzen;

61. begrüßt die im Rahmen bestehender Sanktionsregelungen geleistete Arbeit, mit denen gegen hybride Aktivitäten vorgegangen wird, insbesondere die im Oktober 2024 eingeführte Sanktionsregelung zur Abwehr der destabilisierenden Aktivitäten Russlands und die 2019 eingeführte horizontale Sanktionsregelung zur Abwehr von Cyberaktivitäten; bedauert, dass der EU-Sanktionsrahmen komplex und auf unterschiedliche Quellen hybrider Bedrohungen verteilt ist; fordert eine weitere Stärkung der restriktiven Maßnahmen der EU als Reaktion auf hybride Bedrohungen, darunter die sofortige Einrichtung eines horizontalen EU-Sanktionsrahmens, der speziell für hybride Bedrohungen konzipiert ist, um die Lücken in den geltenden Regelungen zu schließen und die abschreckende Wirkung verstärken, und parallel zur Sanktionsregelung zur Abwehr hybrider Aktivitäten Russlands bestehen würde, um zu verdeutlichen, dass Russland weltweit aktiv hybride Operationen durchführt, und gleichzeitig eine schnellere und systematischere Verhängung von Sanktionen gegen Akteure zu ermöglichen, die für hybride Kampagnen verantwortlich sind; fordert, dass die EU-Instrumentarien gegen hybride Bedrohungen und gegen ausländische Informationsmanipulation und Einmischung sowie für die Cyberdiplomatie weiter gestärkt und wirksamer eingesetzt werden;

62. bekräftigt, dass die Rechenschaftspflicht für hybride Operationen und der Verantwortlichen, einschließlich der Stellvertreter, die im

Namen staatlicher Akteure handeln, sichergestellt werden muss, indem bestehende und spezielle Instrumente in vollem Umfang genutzt werden; fordert die EU und die Mitgliedstaaten auf, dringend Maßnahmen zu ergreifen, um die Finanzströme, mit denen Angriffe auf die Demokratie finanziert werden, zu stoppen und zu unterbinden, unter anderem durch die Mobilisierung von Bankenregulierungsbehörden, strafrechtlichen Ermittlern und Sanktionsbehörden, damit illegale Finanzierungsquellen, einschließlich Kryptowährungen, aufgespürt und untersucht werden; fordert die EU und die Mitgliedstaaten auf, die finanziellen und algorithmischen Anreize zu brechen, die es ermöglichen, dass Desinformation um sich greift, unter anderem durch die Beseitigung der Verbindungen zwischen illegaler Finanzierung, Werbeeinnahmen, auf Aufmerksamkeit ausgerichteten Geschäftsmodellen von Internetplattformen und manipulativen Inhalten;

63. ist der Ansicht, dass alle auf Ebene der Mitgliedstaaten und der EU verfügbaren strafrechtlichen Instrumente angewandt und nötigenfalls weiterentwickelt werden sollten, um rechtswidriges Verhalten, das die Aushöhlung demokratischer Institutionen und Prozesse zum Ziel hat, zu verhindern und zu bekämpfen; betont, dass die zuständigen nationalen Behörden mit angemessenen Instrumenten und Kooperationskanälen ausgestattet werden müssen, um Straftaten im Zusammenhang mit ausländischer Einflussnahme zu verhindern, zu untersuchen, aufzudecken und strafrechtlich zu verfolgen; ist der Ansicht, dass gegen Korruption und Einschüchterung gewählter und öffentlicher Amtsträger im Rahmen krimineller Netzwerke durch eine verstärkte Zusammenarbeit zwischen spezialisierten Antikorruptionsbehörden, Strafverfolgungsbehörden und relevanten Einrichtungen der EU als Teil der Reaktion der EU auf hybride Bedrohungen vorgegangen werden sollte; fordert die Kommission auf, zu beurteilen, ob es einen Mehrwert bringt, Mindestvorschriften im Unionsrecht für die Definition des Straftatbestands der wissentlichen Beteiligung an organisierten Aktivitäten zur Einflussnahme im Auftrag ausländischer Mächte und für diesbezügliche Sanktionen festzulegen; stellt fest, dass die bevorstehende Überarbeitung der Mandate der Agenturen der EU im Bereich Justiz und Inneres eine Gelegenheit bietet, die operative Reaktionsfähigkeit der EU zu stärken; fordert die Kommission auf, die Idee zu prüfen, eine Plattform oder Taskforce für die Mitgliedstaaten einzurichten, die es ihnen ermöglicht, die nationalen legislativen Maßnahmen freiwillig zu koordinieren und bewährte Verfahren austauschen;

***Geografische Erwägungen***

64. verurteilt aufs Schärfste die Instrumentalisierung der Migration durch Drittländer oder feindselige nichtstaatliche Akteure mit dem Ziel, einen Mitgliedstaat zu destabilisieren oder die EU unter Druck

zu setzen; nimmt die spezifischen Bestimmungen über die Instrumentalisierung der Migration zur Kenntnis, die kürzlich in wichtige EU-Rechtsvorschriften aufgenommen wurden; nimmt die von der Kommission angekündigte Überarbeitung des Mandats von Frontex zur Kenntnis; betont, dass diese Überarbeitung die Rechtsgrundlage, die Analysefähigkeiten und angemessene personelle, finanzielle und technische Ressourcen vorsehen sollte, die erforderlich sind, wodurch auch zur Stärkung der Reaktion der EU auf hybride Bedrohungen beigetragen würde;

65. verurteilt aufs Schärfste den Ansturm auf die südliche Grenze der EU in der Stadt Ceuta vom 30. und 31. Juli 2026 sowie die anschließende Invasion Ceutas, die einen Angriff auf die territoriale Unversehrtheit und Souveränität eines Mitgliedstaats darstellen; bedauert, dass irreguläre Migrationsströme als Instrument der hybriden Kriegsführung gegen die Stabilität und Sicherheit eines Mitgliedstaats eingesetzt werden, und fordert daher eine unabhängige und umfassende Untersuchung, um die Verantwortung für die Planung und Durchführung dieses Angriffs zu klären und die verfolgten Ziele zu ermitteln;

66. verurteilt Russlands systematische Drohnenüberflüge und grenzüberschreitende Provokationen gegen EU-Mitgliedstaaten entlang der Ostflanke der EU als gezielte Einschüchterungskampagne gegen die Zivilbevölkerung; begrüßt die Mitteilung der Kommission zu den östlichen Regionen der EU an der Grenze zu Russland, Belarus und der Ukraine und den Umstand, dass die Kommission ausdrücklich anerkennt, dass die östlichen Grenzregionen der EU mit strukturellen und anhaltenden Bedrohungen durch Russland und Belarus konfrontiert sind; fordert die Kommission auf, diese Anerkennung in spezielle Finanzierungsströme innerhalb des Mehrjährigen Finanzrahmens 2028-2034 zu überführen, einschließlich zweckgebundener Mittel für die Verbesserung der Fähigkeiten für den integrierten Grenzschutz, die Modernisierung der physischen und digitalen Grenzüberwachungsinfrastruktur – im Einklang mit den NATO-Standards – an den Landaußengrenzen der EU; betont, dass der Schwerpunkt auf fortschrittliche Detektions-, Überwachungs- und Gegenmaßnahmensysteme gegen unbemannte Luftfahrtsysteme gelegt werden sollte, um kritische Infrastruktur wie Flughäfen, Energieanlagen und Verkehrsknotenpunkte zu schützen und die Mitgliedstaaten beim Einsatz interoperabler Systeme zur Luftraumerfassung, elektronischer Schutzmaßnahmen und von Kapazitäten für die rasche Reaktion auf Vorfälle zu unterstützen; betont, dass Maßnahmen verhältnismäßig, defensiv und auf den Schutz der Zivilbevölkerung ausgerichtet sein müssen, um die Kontinuität wesentlicher Dienste und die Freizügigkeit innerhalb des Schengen-Raums sicherzustellen;

67. betont, dass hybride Bedrohungen zunehmend die gesamte EU betreffen, in den einzelnen Regionen jedoch unterschiedliche Formen annehmen; betont in diesem Zusammenhang, dass der Ostseeraum, der nordisch-baltische Raum und der Schwarzmeerraum Bedrohungen der maritimen Sicherheit und der Sicherheit im Luftraum ausgesetzt sind, hebt die instrumentalisierte Migration, die Anfälligkeit der Mittelmeer- und südlichen Grenzregionen für Bedrohungen der Seeverkehrsinfrastruktur, Energienetze, Logistikkorridore und Routen für den strategischen Transport, Desinformationskampagnen und die Instrumentalisierung von Migrationsströmen hervor, betont, dass Südosteuropa wirtschaftlichem Zwang, Energieabhängigkeit und koordinierter Informationsmanipulation im Zusammenhang mit benachbarten Einsatzgebieten ausgesetzt ist, und weist auf die besondere Anfälligkeit großer städtischer und digitaler Informationsräume in der gesamten EU für kognitive Kriegsführung, Polarisierung und ausländische Einflussnahme hin; betont, dass der Arktis eine zunehmende strategische Bedeutung für die europäische Sicherheit zukommt, einschließlich des Schutzes kritischer Infrastruktur, der Freiheit der Schifffahrt, der Satellitenkommunikation und neu entstehender Verkehrskorridore; fordert die EU und die NATO auf, die Geografie hybrider Bedrohungen in ihren Strategien, einschließlich der künftigen Sicherheitsstrategie der EU, zu berücksichtigen und gleichzeitig einen 360-Grad-Sicherheitsansatz für Resilienz, Vorsorge und Reaktion beizubehalten; betont, dass sich die Finanzierung zur Abwehr hybrider Bedrohungen der strategischen Exposition, dem operativen Bedarf und nachgewiesenen Schwachstellen zuwenden sollte, wobei die Unterstützung sämtlicher Regionen, die hybriden Bedrohungen ausgesetzt sind, sichergestellt werden sollte;

***Koordinierung und Zusammenarbeit zwischen EU und NATO***

68. bekräftigt, dass die NATO für ihre Mitglieder nach wie vor der Eckpfeiler der kollektiven Verteidigung ist; fordert eine intensivere Zusammenarbeit zwischen der EU und der NATO, um die europäische Abwehrbereitschaft, Widerstandsfähigkeit und Abschreckung gegen hybride Bedrohungen zu stärken; betont in diesem Zusammenhang, dass dem Schutz kritischer Infrastruktur, der militärischen Mobilität, der Cyberresilienz und der Abwehrbereitschaft große Bedeutung zukommt; betont, dass ein systematischerer Austausch von Erkenntnissen aus dem Krieg in der Ukraine im hybriden Bereich erforderlich ist;

69. betont, dass die Maßnahmen der EU und der NATO im hybriden Bereich einander ergänzen, sich gegenseitig verstärken und operativ koordiniert werden müssen, wobei sicherzustellen ist, dass die EU vor dem Hintergrund der Angleichung der Mindestanforderungen der EU an die Krisenvorsorge an die Grundanforderungen der NATO bei Bedarf handlungsfähig ist;

70. stellt fest, dass die überarbeitete Strategie der NATO zur Bekämpfung hybrider Bedrohungen von 2025 einen Übergang von Resilienz zu aktiver Abschreckung markiert; begrüßt die vorab vereinbarten Optionen für die militärische Reaktion und die erweiterten Befugnisse des Obersten Alliierten Befehlshabers Europa (SACEUR), durch die ein schnelleres Handeln zu Beginn eines hybriden Angriffs ermöglicht wird, die Verzögerungen zwischen der Erkennung von Bedrohungen und der Reaktion darauf verringert werden und gleichzeitig die politische Aufsicht gewahrt bleibt;

71. begrüßt den Mechanismus der NATO zur Nachverfolgung hybrider Bedrohungen – ein Instrument zur Zusammenführung nachrichtendienstlicher Erkenntnisse über die Gemeinsame Abteilung für Nachrichtendienste und Sicherheit der NATO, über das den Verbündeten ein konsolidiertes Bedrohungsbild zur Verfügung gestellt wird, das sich auf nationale Nachrichtendienste stützt; nimmt die laufende Zusammenarbeit zwischen der NATO und der EU im Bereich der nachrichtendienstlichen Erkenntnisse zur Kenntnis und fordert die Kommission und den EAD auf, innerhalb der EU-Analyseeinheit für hybride Bedrohungen eine strukturierte Schnittstelle mit diesem Mechanismus einzurichten, damit das Lagebewusstsein der EU und das Lagebild der NATO zu hybriden Bedrohungen regelmäßig und systematisch aufeinander abgestimmt werden;

72. betont die wichtige Rolle der Missionen „Artic Sentry“ (Wächter der Arktis), „Baltic Sentry“ (Wächter der Ostsee) und „Eastern Sentry“ (Wächter des Ostens) der NATO als flexible Instrumente bei der Reaktion auf hybride Bedrohungen innerhalb operativ relevanter Zeitrahmen, insbesondere beim Schutz kritischer maritimer Infrastruktur und von Versorgungswegen und bei der Überwachung hybrider Aktivitäten in diesen Räumen; stellt fest, dass deren Wirksamkeit durch die hohen Kosten für das Abfangen von Drohnen, Lücken im Lagebewusstsein und die Fragmentierung der Regelungsrahmen für die Drohnenabwehr in den Mitgliedstaaten eingeschränkt wird; fordert, dass die Umsetzung des EU-Aktionsplans zur Drohnen- und Drohnenabwehrsicherheit, einschließlich der Bereitstellung gezielter Finanzmittel für Fähigkeiten der gestaffelten Verteidigung in den an vorderster Front liegenden Mitgliedstaaten zur kinetischen und elektronischen Bekämpfung von Wetterballons und Drohnen, beschleunigt und dieser Aktionsplan systematisch an die operativen Anforderungen der NATO angepasst wird, um harmonisierte und angemessen ausgestattete Fähigkeiten zur Drohnenabwehr in allen Mitgliedstaaten sicherzustellen; unterstützt zudem eine stärkere Zusammenarbeit bei der Entwicklung und Einführung kosteneffizienter Technologien zur Drohnenabwehr in der gesamten EU;

73. begrüßt den Rahmen für parallele und koordinierte Übungen (PACE) zwischen der EU und der NATO als wertvolles Instrument für die Erprobung und Verbesserung der gemeinsamen Reaktionsfähigkeit, des Umfangs und des Anwendungsbereichs sowie für die systematische Einbeziehung der gewonnenen Erkenntnisse in die Politik, die Planung und die institutionellen Vorkehrungen der EU; fordert regelmäßige Übungen der EU und der NATO, bei denen Szenarien hybrider Angriffe simuliert werden, darunter Sabotage der Infrastruktur für militärische Mobilität, koordinierte Cyberangriffe, groß angelegte Kampagnen der ausländischen Informationsmanipulation und Einmischung, Verletzungen des Luftraums und Angriffe auf kritische Infrastruktur;

74. fordert die Kommission und den EAD auf, in enger Abstimmung mit der NATO und den Mitgliedstaaten ein gemeinsames Verständnis hybrider Bedrohungen zu entwickeln und einen kohärenten Reaktionsmechanismus für die EU und die NATO einzurichten;

75. würdigt die wertvolle Rolle, die spezialisierte Exzellenzzentren, einschließlich des Europäischen Kompetenzzentrums für die Abwehr hybrider Bedrohungen in Helsinki und des Exzellenzzentrums der NATO für kooperativen Schutz vor Computerangriffen in Tallinn, bei der Stärkung der Abwehrbereitschaft, Resilienz, Cyberabwehr und Abwehrfähigkeiten gegen hybride Bedrohungen in ganz Europa spielen; begrüßt ferner die Arbeit der EU-NATO-Taskforce für die Resilienz kritischer Infrastruktur, insbesondere bei der Stärkung der Zusammenarbeit in den Bereichen Energie, Verkehr, digitale Infrastruktur und Untersee-Konnektivität;

76. fordert die Mitgliedstaaten auf, ihre Rechtsvorschriften zu harmonisieren, um die Rechtslücken zu schließen, durch die Personal von Verbündeten daran gehindert wird, sich an Einsätzen zur Reaktion auf hybride Bedrohungen unterhalb der entsprechenden Schwelle zu beteiligen; begrüßt, dass Estland kürzlich Änderungen an seinem Gesetz über die Organisation der Streitkräfte angenommen hat, was einen konkreten Schritt in diese Richtung darstellt;

***Partnerländer: Zusammenarbeit und Unterstützung***

77. betont, dass hybride Operationen Russlands außerhalb der EU darauf abzielen, die Außenpolitik von Drittländern im Sinne der Interessen Moskaus zu verändern, die Beziehungen der EU zu ihren Partnern zu untergraben und die internationale Unterstützung für die Ukraine zu schwächen; bekräftigt daher, dass eine enge Zusammenarbeit mit internationalen Partnern und Organisationen wichtig ist, um das Lagebewusstsein verbessern und hybride Bedrohungen verhindern, davon abschrecken und wirksamer darauf reagieren zu können; nimmt zur Kenntnis, wie wichtig es ist, die bilateralen sektoralen Dialoge und Konsultationen über hybride

Bedrohungen mit gleich gesinnten Partnern, insbesondere im Rahmen der Sicherheits- und Verteidigungspartnerschaften, zu vertiefen;

78. betont, dass eine verstärkte Zusammenarbeit mit der Ukraine, Moldau, Armenien und den Partnern auf dem Westbalkan eine strategische Notwendigkeit ist, da sie ständigen Angriffen Russlands ausgesetzt sind und als wichtige Testgelände für die hybriden Taktiken Russlands fungieren, die eine Kombination aus ausländischer Informationsmanipulation und Einmischung, Cyberoperationen, Netzen der verdeckten Einflussnahme, Zwangsmaßnahmen im Zusammenhang mit Energielieferungen und Druck durch Korruption zur Schwächung demokratischer Institutionen, des gesellschaftlichen Zusammenhalts und der Aussichten auf eine Integration der EU und der NATO sind; fordert die Mitgliedstaaten auf, die aus diesen Ländern gewonnenen Erkenntnisse zu übernehmen und strukturierte Mechanismen für den systematischen Austausch bewährter Verfahren und operativer Erfahrungen einzurichten, auch zur Fähigkeit der Ukraine, grundlegende Dienste, die Kontinuität der Regierung, den Schutz kritischer Infrastruktur, die strategische Kommunikation und das Funktionieren und die Resilienz der Gesellschaft unter anhaltenden Angriffen aufrechtzuerhalten; bekräftigt seine nachdrückliche Unterstützung für den allmählichen Beitritt der Ukraine zur EU und ihren Beitritt zur NATO, sobald die entsprechenden Bedingungen erfüllt sind;

79. betont, dass es von strategischer Bedeutung ist, die Unterstützung der hybriden Resilienz für Bewerberländer, mögliche Bewerberländer und Partnerländer, die häufig Hauptziele der hybriden Aktivitäten Russlands sind und deren Widerstandsfähigkeit unmittelbar zur Sicherheit der EU beiträgt, fortzusetzen und zu vertiefen; begrüßt den aktiven Beitrag der EU und ihrer Mitgliedstaaten zur Stärkung der Widerstandsfähigkeit dieser Länder durch das außenpolitische Instrument, strategische Kommunikation, Teams für die rasche Reaktion auf hybride Bedrohungen, die Untersuchung über hybride Bedrohungen und GSVP-Missionen in Partnerländern wie der Ukraine, Moldau, Armenien und Montenegro; fordert die Organisation regelmäßiger gemeinsamer Übungen, Simulationsszenarien und Schulungsprogramme, die darauf abzielen, die Abwehrbereitschaft zu optimieren, die Krisenreaktionskapazitäten zu verbessern und die Interoperabilität bei der Bewältigung hybrider Bedrohungen zu fördern; nimmt anerkennend die koordinierte Reaktion der EU und der NATO in Moldau zur Kenntnis, einschließlich des parallelen Einsatzes eines EU-Teams für die Reaktion auf hybride Bedrohungen und eines NATO-Teams zur Unterstützung bei der Abwehr hybrider Bedrohungen mit einander ergänzenden Mandaten; bestärkt die Bewerberländer und möglichen Bewerberländer darin, eine vollständige Angleichung an die Gemeinsame Außen- und

Sicherheitspolitik (GASP) der EU, einschließlich der restriktiven Maßnahmen, als einen zentralen Aspekt des EU-Integrationsprozesses vorzunehmen;

80. würdigt die demokratische Resilienz der proeuropäischen Kräfte Moldaus und Armeniens während und im Vorfeld ihrer Parlamentswahlen 2025 und 2026, was der Beleg für einen starken Widerstand gegen die seit Jahren anhaltenden Kampagnen Russlands zur Informationsmanipulation und Einmischung ist; hebt die Wirksamkeit des ressortübergreifenden Ansatzes als operatives Modell hervor, einschließlich des Einsatzes von Strafverfolgungsmaßnahmen gegen Netzwerke, die hybride Operationen im Auftrag Russlands durchführen; fordert die Mitgliedstaaten und die Kommission auf, in Zusammenarbeit mit dem EAD Rahmen auf EU-Ebene zu entwickeln, die vergleichbare Reaktionen der Strafverfolgungsbehörden ermöglichen; weist auf die wichtige Rolle hin, die den Organen der EU, staatlichen Institutionen, der Zivilgesellschaft und unabhängigen Medien bei der Bekämpfung von ausländischer Informationsmanipulation und Einmischung zukommt, einschließlich KI-gestützter groß angelegter koordinierter Kampagnen zur Informationsmanipulation, und die zu dem besonders hohen Grad der Sensibilisierung der Öffentlichkeit für hybride Bedrohungen beiträgt;

81. fordert eine verstärkte Zusammenarbeit bei hybriden Bedrohungen mit gleich gesinnten Partnern außerhalb der EU, insbesondere mit dem Vereinigten Königreich und Norwegen als wichtigen europäischen Sicherheitspartnern, sowie mit Kanada, Japan, der Republik Korea, Australien, Neuseeland, Taiwan und anderen gleich gesinnten Partnern, unter anderem, wenn möglich, durch Sicherheits- und Verteidigungspartnerschaften, Informationsaustausch, Zusammenarbeit im Cyberbereich und in den Bereichen maritime Sicherheit, Weltraum und Resilienz; betont, dass die dem EWR angehörende EFTA-Staaten und ihre Verteidigungsindustrien vollständig in die EU-Rahmen für hybride Resilienz und die EU-Programme zur Fähigkeitenentwicklung einbezogen werden sollten, wobei ihr direkter Beitrag zur europäischen Sicherheit und ihre gemeinsame Exposition gegenüber hybriden Bedrohungen anerkannt werden sollten;

82. bedauert, dass der jüngste Wandel in der US-Politik die gemeinsame Front der Demokratien in einer Zeit zunehmender hybrider Bedrohungen geschwächt hat; betont, dass die transatlantische Einheit für die Bekämpfung dieser Bedrohungen nach wie vor von entscheidender Bedeutung ist;

83. betont, dass die Beeinflussungsoperationen Russlands in Afrika, Lateinamerika und der Karibik für die europäische Sicherheit nicht von untergeordneter Bedeutung sind, da sie darauf abzielen, die Partnerschaften der EU zu beeinträchtigen, die Unterstützung für

die Ukraine zu schwächen und die europäische Diplomatie, Sicherheitshilfe und Entwicklungszusammenarbeit zu untergraben; stellt fest, dass sich diese Operationen in Afrika hauptsächlich auf staatliche Medien sowie kulturelle und religiöse Fronten stützen, während Russland in Lateinamerika und der Karibik ein spanischsprachiges Einflusssystem aufgebaut hat, das seine antieuropäischen Botschaften andernorts ergänzt; fordert die EU und die Mitgliedstaaten auf, die strategische Kommunikation zu stärken, unabhängige und vertrauenswürdige lokale Medien zu unterstützen, glaubwürdige lokale Stimmen einzubeziehen und die Zusammenarbeit mit Partnern in beiden Regionen zu verstärken, um feindselige Informationskampagnen aufzudecken und zu bekämpfen;

84. betont, wie wichtig die Erfahrungen der Golfstaaten, Jordaniens und anderer einschlägiger Partner bei der Bekämpfung hybrider Einflussnetzwerke sind, die mit der Muslimbruderschaft in Verbindung stehen, unter anderem durch Ansätze in den Bereichen Regierungsführung, Regulierung und gesellschaftliche Resilienz, und fordert einen strukturierten Austausch bewährter Verfahren mit diesen Partnern, um das Verständnis der EU für hybride Bedrohungen zu stärken, die politischen Reaktionen und die Zusammenarbeit bei der Bekämpfung ausländischer Einflussnahme zu verstärken und gleichzeitig die Grundrechte und die Vielfalt der rechtlichen und politischen Systeme zu achten;

85. nimmt die umfassende Erfahrung Taiwans bei der eigenen Verteidigung gegen die hybriden Angriffe Chinas und die Informationsmanipulation und Einmischung von dort zur Kenntnis; würdigt das umfassende Resilienzmodell Taiwans, einschließlich der Einrichtung eines gesamtgesellschaftlichen Ausschusses für Resilienz im Verteidigungsbereich, groß angelegter Schulungen im Bereich des Katastrophenschutzes, der Zusammenarbeit mit Organisationen der Zivilgesellschaft, digitaler Resilienznetze und öffentlicher Wappnungsinitiativen; betont, dass die Erfahrungen Taiwans zeigen, dass die Resilienz der Gesellschaft kein sekundärer Aspekt der Verteidigung, sondern eine zentrale Säule der nationalen Sicherheit ist, insbesondere wenn hybrider Druck auf kritische Infrastrukturen, das Vertrauen der Öffentlichkeit und den sozialen Zusammenhalt abzielt; fordert einen regelmäßigen Austausch zwischen der EU und ihren taiwanesischen Amtskollegen über relevante Sicherheitsfragen und eine engere diesbezügliche Zusammenarbeit zwischen der EU und Taiwan bei der Bekämpfung von ausländischer Informationsmanipulation und Einflussnahme und der kognitiven Kriegsführung sowie beim Schutz von kritischer Infrastruktur und Unterseekabeln und bei der Stärkung der gesamtgesellschaftlichen Resilienz; fordert die EU auf, den Handel und die industrielle Zusammenarbeit mit Taiwan auszuweiten, insbesondere bei Hochtechnologiekomponenten und strategischen Technologien, die für die Widerstandsfähigkeit und Sicherheit von wesentlicher Infrastruktur und Lieferketten von entscheidender

Bedeutung sind, darunter Halbleiter, 5G- bzw. 6G-Telekommunikationsausrüstung, Drohnen und Güter mit doppeltem Verwendungszweck; betont ferner, dass Taiwan und der Ukraine IRIS² (Infrastruktur für Resilienz, Interkonnektivität und Sicherheit durch Satelliten) zur Verfügung gestellt werden muss;

°

° °

86. beauftragt seine Präsidentin, diese Entschließung dem Rat, der Hohen Vertreterin und der Kommission zu übermitteln.