Rat der
Europäischen Union

Brüssel, den 10. Dezember 2019
(OR. en)

14972/19

HYBRID 56	**EDUC 478**
DISINFO 18	**AUDIO 118**
AG 68	**DIGIT 179**
PE 257	**INF 332**
DATAPROTECT 300	**COSI 252**
JAI 1307	**CSDP/PSDC 575**
CYBER 328	**COPS 360**
JAIEX 177	**POLMIL 129**
FREMP 176	**IPCR 23**
RELEX 1147	**PROCIV 100**
CULT 141	**CSC 294**

BERATUNGSERGEBNISSE

Absender:	Generalsekretariat des Rates
Empfänger:	Delegationen
Betr.:	Zusätzliche Anstrengungen zur Stärkung der Resilienz und zur Abwehr hybrider Bedrohungen - Schlussfolgerungen des Rates (10. Dezember 2019)

Die Delegationen erhalten anbei die Schlussfolgerungen des Rates zu zusätzlichen Anstrengungen zur Stärkung der Resilienz und zur Abwehr hybrider Bedrohungen, die der Rat auf seiner 3739. Tagung vom 10. Dezember 2019 angenommen hat.

ANLAGE

Schlussfolgerungen des Rates zu zusätzlichen Anstrengungen zur Stärkung der Resilienz und zur Abwehr hybrider Bedrohungen

1. Unter Hinweis auf die relevanten Schlussfolgerungen des Europäischen Rates[1] und des Rates[2] bekräftigt der Rat, dass er sich kontinuierlich dafür einsetzt, die Resilienz der Union und der Mitgliedstaaten gegenüber den vielschichtigen und sich ständig wandelnden hybriden Bedrohungen zu stärken und die Zusammenarbeit hinsichtlich der Aufdeckung, Prävention und Abwehr dieser Bedrohungen zu verbessern.

2. Der Rat würdigt die Fortschritte, die im Einklang mit den einschlägigen Schlussfolgerungen des Rates bei der Umsetzung des Gemeinsamen Rahmens für die Bekämpfung hybrider Bedrohungen (2016), der Gemeinsamen Mitteilung mit dem Titel „Stärkung der Resilienz und Ausbau der Kapazitäten zur Abwehr hybrider Bedrohungen“ (2018) und dem Aktionsplan gegen Desinformation (2018) erzielt wurden.

3. Die Verantwortung für die Abwehr hybrider Bedrohungen liegt in erster Linie bei den Mitgliedstaaten. Die auf EU-Ebene unternommenen Anstrengungen sind ergänzender Natur und berühren nicht die alleinige Verantwortung der Mitgliedstaaten in Fragen der nationalen Sicherheit. Zur Bewältigung hybrider Bedrohungen ist ein umfassender, resssortübergreifender und gesamtgesellschaftlicher Sicherheitsansatz erforderlich, bei dem in allen einschlägigen Politikbereichen auf eine stärker strategische, koordinierte und kohärente Art und Weise gearbeitet wird. Es ist wichtig, dass auch auf EU-Ebene ein ressortübergreifender Ansatz verfolgt und angewendet wird.

4. In diesen Schlussfolgerungen des Rates werden im Kontext der Umsetzung der neuen Strategischen Agenda für den Zeitraum 2019-2024 Prioritäten festgelegt, nämlich der Schutz unserer Gesellschaften, der Bürgerinnen und Bürger und der Freiheiten sowie der Sicherheit unserer Union vor hybriden Bedrohungen; erreicht werden soll dies durch die Förderung eines umfassenden Sicherheitsansatzes mit besserer Koordinierung, mehr Mitteln und besseren technischen Kapazitäten, der auf der umfangreichen Arbeit aufbaut, die in verschiedenen Politikbereichen bereits geleistet wurde, unter anderem auch im Rahmen der sicherheits- und verteidigungspolitischen Zusammenarbeit.

---

1 Insbesondere die Schlussfolgerungen des Europäischen Rates von Juni 2019, März 2019, Dezember 2018, Oktober 2018, Juni 2018, März 2018, Juni 2015 und März 2015.

2 Insbesondere die Dokumente ST 10048/19, ST 6573/1/19 REV1, ST 10255/19, ST 12836/19 und ST 7928/16.

5. Beim Schutz unserer demokratischen Institutionen vor hybriden Bedrohungen müssen stets die Grundrechte geachtet werden; hierzu zählen unter anderem der Schutz personenbezogener Daten, die Freiheit der Meinungsäußerung, die Informationsfreiheit und die Vereinigungsfreiheit, die in der Charta der Grundrechte verankert sind.

6. Die EU und ihre Mitgliedstaaten sollten weiterhin Fähigkeiten entwickeln, trainieren und ausüben, die es ihnen ermöglichen, hybride Aktivitäten zu erkennen, die Quellen dieser Aktivitäten zu analysieren und darauf zu reagieren; außerdem sollten sie weiterhin Unterstützung dabei leisten, die Resilienz der Mitgliedstaaten sowie der Organe, Agenturen und Einrichtungen der EU gegenüber hybriden Bedrohungen auf lange Sicht zu stärken und dazu bereits vorhandene geeignete Instrumente in vollem Umfang nutzen. Der Rat hebt hervor, dass das Protokoll der EU für das operative Vorgehen bei der Abwehr hybrider Bedrohungen auf der Grundlage des bei früheren Übungen festgestellten Verbesserungsbedarfs und der dabei gewonnenen Erkenntnisse aktualisiert werden muss.

7. Der Rat unterstreicht, dass auch im Kontext der Abwehr hybrider Bedrohungen weiterhin die Notwendigkeit besteht, mit internationalen Organisationen wie den Vereinten Nationen, der OSZE und dem Europarat sowie mit Formaten wie den G7 zusammenzuarbeiten, um die auf Regeln basierende Weltordnung – unter anderem durch vertrauensbildende Maßnahmen und andere relevante Maßnahmen – zu verteidigen.

8. Der Rat betont, dass die EU entschlossen ist, die enge und sich gegenseitig verstärkende Zusammenarbeit mit allen relevanten Partnerländern, insbesondere in der Nachbarschaft der EU, in Bezug auf die Stärkung der Resilienz gegenüber hybriden Bedrohungen und die Abwehr solcher Bedrohungen fortzusetzen und diese Länder diesbezüglich auch weiterhin zu unterstützen.

9. Der Rat fordert kontinuierliche und nachhaltige Anstrengungen, um weitere Fortschritte bei der Durchführung sämtlicher Maßnahmen zur Abwehr hybrider Bedrohungen, die in dem gemeinsamen Paket von Vorschlägen für die Umsetzung der Gemeinsamen Erklärungen über die Zusammenarbeit zwischen EU und NATO genannt sind, zu erzielen, auch in den Bereichen Lageerfassung, strategische Kommunikation, Krisenprävention und Krisenreaktion sowie Stärkung der Resilienz. In diesem Zusammenhang bekräftigt er, dass der politische Dialog über die Abwehr hybrider Bedrohungen weiter intensiviert werden muss, und dass regelmäßig parallele und koordinierte Übungen durchgeführt werden müssen, an denen alle Mitgliedstaaten der EU und alle NATO-Bündnispartner teilnehmen; in diesem Zusammenhang fordert er außerdem die zügige Fertigstellung des neuen Plans für die parallelen und koordinierten Übungen. Der Rat hebt hervor, dass der festgestellte Verbesserungsbedarf berücksichtigt werden muss, und betont zugleich, wie wichtig ein ungehinderter, inklusiver und diskriminierungsfreier Informationsaustausch ist.

Ferner würdigt der Rat die wertvollen Beiträge des Europäischen Kompetenzzentrums für die Abwehr hybrider Bedrohungen in Helsinki und spricht sich für eine Zusammenarbeit des Zentrums mit den relevanten NATO-Kompetenzzentren aus. Außerdem begrüßt er den regelmäßigen und strukturierten Austausch auf Mitarbeiterebene, wozu auch die Zusammenarbeit zwischen der EU-Analyseeinheit für hybride Bedrohungen des EU-Zentrums für Informationsgewinnung und Lageerfassung und der NATO-Analyseeinheit für hybride Bedrohungen gehört.

10. Der Rat würdigt die Anstrengungen, die von den Mitgliedstaaten in Zusammenarbeit mit der Kommission und dem Europäischen Auswärtigen Dienst (EAD) unternommen wurden, um die Untersuchung über hybride Risiken gemäß der Maßnahme 1 des Gemeinsamen Rahmens für die Bekämpfung hybrider Bedrohungen (2016) durchzuführen, und fordert eine Fortsetzung dieser Arbeit sowie unter Umständen eine Überarbeitung der Untersuchung über hybride Risiken, um Schwachstellen besser beseitigen zu können.

Kohärente Arbeit zur Stärkung der Resilienz und zur Abwehr hybrider Bedrohungen

11. Bei der Entwicklung und Nutzung neuer und aufstrebender Technologien, einschließlich künstlicher Intelligenz und Datenerfassungstechniken, sollten neue Möglichkeiten zur Verbesserung der Resilienz sowie mögliche Schwachstellen und Kaskadeneffekte im Zusammenhang mit der Abwehr hybrider Bedrohungen gebührend berücksichtigt werden, um das Gesamtrisiko zu verringern; dies gilt auch für das strategische Planungsverfahren des Rahmenprogramms für Forschung und Innovation.

12. Der Rat nimmt zur Kenntnis, dass böswillige Cyberaktivitäten Teil einer hybriden Bedrohung sein können, und hebt in diesem Zusammenhang die Bedeutung des Instrumentariums der EU für die Cyberdiplomatie hervor, die sogenannte Cyber Diplomacy Toolbox.

13. Der Zusammenhang zwischen hybriden Bedrohungen und wirtschaftlicher Sicherheit ist ein wichtiger Aspekt, den es zu berücksichtigen gilt, wobei dies in erster Linie nach wie vor eine Zuständigkeit der Mitgliedstaaten ist.

14. Neue Instrumente wie beispielsweise der Mechanismus gemäß der Verordnung der EU über die Überprüfung ausländischer Direktinvestitionen sollten wirksam zur Stärkung der Resilienz und zur Abwehr hybrider Bedrohungen eingesetzt werden, da sie Möglichkeiten bieten, um Direktinvestitionen, die die Sicherheit oder die öffentliche Ordnung beeinträchtigen könnten, zu ermitteln und dagegen vorzugehen.

15. Der Rat ersucht die Kommission, die Resilienz gegenüber hybriden Bedrohungen in die Folgenabschätzungen für einschlägige künftige Gesetzgebungsvorschläge, auch solcher zu künftigen Rahmenprogrammen für Forschung und Innovation, aufzunehmen.

16. Der Rat unterstreicht, wie wichtig es ist, regelmäßig Übungen zur Abwehr hybrider Bedrohungen durchzuführen und dieses Thema auf Ministerebene und anderen Ebenen auf der Grundlage konkreter Szenarien zu diskutieren; ferner hebt er hervor, wie wichtig es ist, dass hybride Elemente in weitere relevante Ausbildungsmaßnahmen und Übungen der EU auf allen Ebenen einbezogen werden, und dass hierzu die Unterstützung der Mitgliedstaaten und der relevanten Gremien, gegebenenfalls insbesondere des Europäischen Kompetenzzentrums für die Abwehr hybrider Bedrohungen, erforderlich ist.

17. Zur Gewährleistung eines kohärenten weiteren Vorgehens im Rahmen der Zusammenarbeit der EU zur Stärkung der Resilienz und zur Abwehr hybrider Bedrohungen ersucht der Rat die Kommission und den Hohen Vertreter, im Hinblick auf eventuelle neue Initiativen eine umfassende Bestandsaufnahme der bisher getroffenen Maßnahmen und der verabschiedeten relevanten Dokumente zu erstellen.

Verknüpfung von innerer und äußerer Sicherheit

18. Strafverfolgungsbehörden, Katastrophenschutzbehörden und andere zuständige Behörden sollten ihre Vorsorgemaßnahmen zur Prävention und Abwehr hybrider Bedrohungen weiter ausbauen. Die Zusammenarbeit zwischen den zuständigen nationalen Behörden sowie den Organen, Agenturen und Einrichtungen der EU auf der Grundlage ihrer jeweiligen Mandate muss im gesamten Bereich der Verknüpfung von innerer und äußerer Sicherheit kontinuierlich verbessert und durchgängig umgesetzt werden, wobei gleichzeitig für mehr Synergien gesorgt und Doppelarbeit vermieden werden muss, unter anderem durch horizontale Arbeitsmethoden, freiwilligen Informationsaustausch sowie sektorübergreifende Schulungen und Übungen. Hierfür sollten die Unterstützungsfunktion und die Beiträge der relevanten Mechanismen und Agenturen der EU auf der Grundlage ihrer jeweiligen Mandate und unter Berücksichtigung bestehender Haushaltszwänge eingehender bewertet werden.

19. Der Einsatz der relevanten Mechanismen und Instrumente der EU zur Unterstützung der Mitgliedstaaten bei der Reaktion auf sektorübergreifende und grenzüberschreitende Bedrohungen, unter anderem die Integrierte EU-Regelung für die politische Reaktion auf Krisen (IPCR), das Katastrophenschutzverfahren der Union und das Zentrum für die Koordination von Notfallmaßnahmen (ERCC), sollte von den Institutionen und Einrichtungen der EU in Zusammenarbeit mit den Mitgliedstaaten näher festgelegt werden.

20. Der Rat bestätigt, dass die Mitgliedstaaten im Hinblick auf die Bewältigung einer schweren Krise, die auf hybride Aktivitäten zurückzuführen ist, die Solidaritätsklausel (Artikel 222 AEUV) geltend machen können.

Lageerfassung und Intelligence-Auswertung und -Analyse

21. Die Zusammenarbeit der EU bei der Verbesserung der Resilienz und der Abwehr hybrider Bedrohungen muss sich an einer regelmäßig aktualisierten Einschätzung der Bedrohungslage und einer umfassenden Lageerfassung orientieren. Beide müssen vom Zentrum der Europäischen Union für Informationsgewinnung und Lageerfassung (EU-INTCEN) und der zugehörigen EU-Analyseeinheit für hybride Bedrohungen erstellt werden, um die EU und ihre Mitgliedstaaten besser in die Lage zu versetzen, hybride Aktivitäten zu erkennen, zu verhindern, zu stören und darauf zu reagieren, wobei die Zuständigkeiten der Mitgliedstaaten zu achten sind. Der Rat ist der Auffassung, dass die Tätigkeit der EU-Analyseeinheit für hybride Bedrohungen ausgeweitet werden sollte, wobei eine angemessene Ausstattung mit Ressourcen, einschließlich Fachwissen, vorzusehen ist.

22. Der Rat weist auf die Schlussfolgerungen zur Bewältigung hybrider Bedrohungen vom 19. April 2016 hin, in denen gefordert wird, die EU-Instrumente zur Prävention und Bewältigung hybrider Bedrohungen für die Union und ihre Mitgliedstaaten sowie für ihre Partner zu mobilisieren. Er unterstreicht, dass es unerlässlich ist, die bei den Mitgliedstaaten und der EU vorhandenen Funktionen zur Lageerfassung unter Berücksichtigung der Quellen von Bedrohungen weiterzuentwickeln, und dass die vom EU INTCEN und von der zugehörigen EU-Analyseeinheit für hybride Bedrohungen erstellten Intelligence-Auswertungen und -Analysen insbesondere bei den Beschlussfassungs- und Krisenbewältigungsverfahren der EU im Zusammenhang mit der Abwehr hybrider Bedrohungen besser genutzt werden müssen.

23. Dem Rat ist bewusst, dass die GSVP-Missionen und -Operationen einen wichtigen Beitrag dazu leisten können, gegebenenfalls bei Bedarf Indikatoren für mögliche hybride Aktivitäten Dritter – einschließlich Desinformation, die darauf gerichtet ist, Maßnahmen der EU und ihrer Mitgliedstaaten zu diskreditieren und zu beeinträchtigen – zu ermitteln und zu analysieren, und er weist darauf hin, dass es nützlich sein könnte die Möglichkeiten zur Weiterentwicklung dieses Beitrags zu sondieren.

Schutz kritischer Infrastrukturen

24. Der Schutz von kritischen Infrastrukturen auf nationaler und europäischer Ebene sowie der Schutz der Funktionen und Dienste, die für das ordnungsgemäße Funktionieren von Staat, Wirtschaft und Gesellschaft unerlässlich sind, sind auch im Kontext der Verbesserung der Resilienz gegenüber hybriden Bedrohungen eine wichtige Priorität und machen einen ressortübergreifenden und gesamtgesellschaftlichen Ansatz erforderlich. Dabei müssen die starken wechselseitigen Abhängigkeiten zwischen den verschiedenen kritischen Funktionen und Diensten, einschließlich Finanzdiensten, die wichtige Rolle des Privatsektors, das sich verändernde Sicherheitsumfeld sowie aufkommende physische Bedrohungen und Cyberbedrohungen berücksichtigt werden.

25. Darüber hinaus sollten ergänzend zu den rechtlichen, regulatorischen und aufsichtsrechtlichen Anforderungen, die auf EU-Ebene und auf nationaler Ebene an einen stabilen Systembetrieb und die Aufrechterhaltung des Geschäftsbetriebs gestellt werden, Vereinbarungen mit Infrastrukturbesitzern und -betreibern und Diensteanbietern des Privatsektors getroffen werden, um die Aufrechterhaltung von kritischen Diensten und den Zugang dazu auch in Fällen höherer Gewalt zu gewährleisten, indem ein angemessenes Maß an Vorsorge sichergestellt wird, um alle relevanten Bedrohungen abwehren zu können, ebenso wie die notwendige Flexibilität, um Ereignisse mit schwerwiegenden Folgen, jedoch geringer Eintrittswahrscheinlichkeit, bewältigen und eindämmen und sich davon erholen zu können.

26. Der Rat hebt hervor, dass zwar die Zuständigkeit für den Schutz kritischer Infrastrukturen in erster Linie bei den Mitgliedstaaten liegt, aufgrund des hohen Maßes an grenzüberschreitenden und sektorübergreifenden wechselseitigen Abhängigkeiten jedoch koordinierte oder erforderlichenfalls auch harmonisierte Anstrengungen auf EU-Ebene erforderlich sind, unter anderem auch im Hinblick auf ein unterbrechungsfreies Funktionieren des Binnenmarktes.

27. Im Anschluss an die im Juli 2019 erfolgte Bewertung der Umsetzung der Richtlinie 2008/114/EG des Rates über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen ersucht der Rat die Kommission, sich mit den Mitgliedstaaten über einen zu Beginn der neuen Legislaturperiode vorzulegenden etwaigen Vorschlag zur Überarbeitung der Richtlinie ins Benehmen zu setzen, der potenzielle ergänzende Maßnahmen zur Verbesserung des Schutzes und der Resilienz kritischer Infrastrukturen in der EU enthält und den bestehenden starken wechselseitigen Abhängigkeiten zwischen kritischen Funktionen und Diensten Rechnung tragen sollte.

28. Der Rat ersucht die Kommission, weiterhin mit den Mitgliedstaaten zusammenzuarbeiten und gegebenenfalls nicht bindende Kooperationsvereinbarungen zwischen Mitgliedstaaten, die vernetzte kritische Infrastrukturen gemeinsam nutzen, zu erarbeiten.

29. Der Rat ist sich der Bedeutung bewusst, die der Richtlinie zur Netz- und Informationssicherheit (NIS-Richtlinie) zum einen hinsichtlich der Entwicklung einer Risikomanagement- und Sicherheitskultur bei den Betreibern in kritischen Sektoren und zum anderen im Hinblick auf die nationalen Fähigkeiten und Strategien zur Gewährleistung eines hohen Maßes an Netz- und Informationssicherheit im eigenen Hoheitsgebiet, auch im Zusammenhang mit hybriden Bedrohungen, zukommt. Der Rat ersucht die Mitgliedstaaten, die Kommission und die Agentur der Europäischen Union für Cybersicherheit (ENISA), ihre Zusammenarbeit auf der Grundlage der Empfehlung der Kommission für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen (Blaupause) in allen relevanten Bereichen zu intensivieren.

Bekämpfung von Desinformation und Sicherstellung freier und fairer Wahlen

30. Der Rat würdigt den Bericht über die Umsetzung des Aktionsplans gegen Desinformation und weist darauf hin, dass die weitere Umsetzung dieses Aktionsplans auch weiterhin im Mittelpunkt der Anstrengungen der EU steht. Er betont, dass der Aktionsplan regelmäßig überarbeitet und erforderlichenfalls aktualisiert werden muss, um sicherzustellen, dass ein wirksamer langfristiger Ansatz verfolgt wird.

31. Der Rat hebt hervor, dass die Arbeit der Abteilung Strategische Kommunikation des EAD und insbesondere die Arbeit der drei Task Forces (Osteuropa, Westbalkan, Südeuropa) mit ausreichenden Ressourcen unterstützt werden muss, sodass eine langfristige Planung, Durchführung und Evaluierung möglich ist. Zu den Aufgaben aller drei Task Forces gehört es, Desinformationsaktivitäten ausländischer staatlicher Akteure und externer nicht-staatlicher Akteure kontinuierlich erkennen, untersuchen und gegen sie vorgehen zu können. Die Task Forces sollten außerdem weiterhin zu einer wirksamen und faktengestützten positiven Kommunikation und zur Förderung der Grundsätze, Werte und Politiken der Union in der östlichen und der südlichen Nachbarschaft der EU sowie im Westbalkan beitragen ebenso wie zur Stärkung der allgemeinen Medienlandschaft und der Zivilgesellschaft in den jeweiligen Regionen. Der Rat ersucht den EAD zu ermitteln, welcher Bedarf und welche Möglichkeiten bestehen, seine strategische Kommunikation in anderen Regionen, etwa in den afrikanischen Ländern südlich der Sahara, zu verstärken und dabei zugleich die notwendigen Fähigkeiten zur Wahrnehmung der bestehenden Aufgaben im Bereich der strategischen Kommunikation zu erhalten.

32. Der Rat ist sich dessen bewusst, dass auf allen Ebenen ein umfassender Ansatz erforderlich ist, um die Problematik der Desinformation, zu der auch Manipulationen zur Beeinträchtigung der freien und fairen Wahlen in Europa gehören, zu bewältigen und dabei alle online wie offline verfügbaren Instrumente bestmöglich zu nutzen. Zu diesen Instrumenten müssen die Überwachung und Analyse von Desinformation und Manipulation, die Durchsetzung der europäischen Datenschutzvorschriften, die Anwendung von Schutzvorkehrungen für Wahlen, Anstrengungen zur Förderung pluralistischer Medien, des professionellen Journalismus und der Medienkompetenz und die Sensibilisierung der Bürgerinnen und Bürger gehören. Der Rat empfiehlt eine weitere Konsolidierung eines aktiven, unabhängigen europaweiten Netzes von Faktenprüfern und Forschern zur Bekämpfung von Desinformation. Der Rat ist sich der Bedeutung und der Rolle bewusst, die der Zivilgesellschaft, akademischen Kreisen und dem Privatsektor bei der Bekämpfung von Desinformation und bei der Stärkung der Resilienz zukommen.

33. Der Rat ist sich dessen bewusst, über welches Potenzial das Frühwarnsystem in Bezug auf die Bekämpfung von Desinformation, und insbesondere von Wahlmanipulation, verfügt. Er fordert die Kommission und den EAD nachdrücklich auf, gemeinsam mit den Mitgliedstaaten das Frühwarnsystem dahingehend auszubauen, dass eine umfassende Plattform für die Mitgliedstaaten und die Institutionen der EU geschaffen wird mit dem Ziel, die Zusammenarbeit, die Koordination und den Austausch von Informationen, einschließlich Forschungs- und Analyseergebnissen und bewährten Verfahren, sowie die Kommunikationsprodukte zu verbessern und somit als Teil der europäischen und nationalen Anstrengungen die Abwehr von Desinformationskampagnen zu unterstützen.

34. Der Rat ist sich des Nutzens der Maßnahmen und Empfehlungen bewusst, die die Kommission am 12. September 2018 in ihrem Paket zur Gewährleistung freier und fairer Europawahlen vorgelegt hat. Der Rat bestärkt die Kommission und die Mitgliedstaaten darin zu prüfen, welche Möglichkeiten bestehen, um die Aktivitäten der europäischen Wahlkooperationsnetze fortzusetzen und so den Austausch von Informationen und bewährten Verfahren zu unterstützen. Der Rat würdigt die Anstrengungen, die die Kommission unternommen hat, um unter Berücksichtigung der nationalen Zuständigkeiten in diesem Bereich alle relevanten Akteure einzubeziehen und eine breite Palette an Maßnahmen zu unterstützen, so beispielsweise die Übung zu Cybersicherheitsvorfällen bei den Wahlen zum Europäischen Parlament (EU ELEx19).

35. Dem Rat ist bewusst, dass die Arbeit mit den Plattformen sozialer Medien weitergeführt werden muss, um bezüglich der Abwehr von Desinformation höhere Standards für Verantwortung, Transparenz und Rechenschaftspflicht durchzusetzen. Außerdem sollten die Anbieter von Plattformen sozialer Medien zu Zwecken der akademischen Forschung ungehinderten Zugang zu anonymisierte Daten gewähren, um die Erarbeitung faktengestützter Strategien zu ermöglichen. Der Rat ersucht die Kommission, Initiativen zum weiteren Vorgehen hinsichtlich der Abwehr von Desinformation auf Online-Plattformen vorzulegen. Diese Initiativen sollten auf einer Bewertung der Umsetzung des Verhaltenskodex für den Bereich der Desinformation beruhen; bei dieser Bewertung sollten die von akademischen Kreisen und zivilgesellschaftlichen Organisationen durchgeführten Analysen und vorgelegten Berichte, der von der Gruppe europäischer Regulierungsstellen für audiovisuelle Medien vorgelegte Überwachungsbericht zum Verhaltenskodex sowie die bei den Wahlen zum Europäischen Parlament im Mai 2019 gewonnenen Erkenntnisse berücksichtigt werden. In diesem Zusammenhang ersucht der Rat die Kommission zu prüfen, welche Möglichkeiten, einschließlich eines eventuellen Durchsetzungsmechanismus für Online-Plattformen, bestehen, um den Verhaltenskodex besser umzusetzen, insbesondere durch Einbeziehung einer unabhängigen Bewertung, inwieweit die Unterzeichner die eingegangenen Verpflichtungen umsetzen.

Sicherheit der Organe, Agenturen und Einrichtungen der EU

36. Es liegt im gemeinsamen Interesse der EU und ihrer Mitgliedstaaten, das Personal, die Organe, die Agenturen und die Einrichtungen der EU vor hybriden Bedrohungen und anderen böswilligen Aktivitäten zu schützen. Der Rat ersucht alle Organe, Agenturen und Einrichtungen der EU, mit der Unterstützung der Mitgliedstaaten auf der Grundlage einer umfassenden Einschätzung der Bedrohungslage dafür zu sorgen, dass die Union in der Lage ist, ihre Integrität zu schützen, und sicherzustellen, dass die Kommunikations- und Informationsnetze und die Beschlussfassungsverfahren der EU vor böswilligen Aktivitäten aller Art geschützt sind. Im Einklang mit dem vom Europäischen Rat auf seiner Tagung im Juni 2019 erteilten Mandat sollten daher die Organe, Einrichtungen und Agenturen der EU mit der Unterstützung der Mitgliedstaaten ein umfassendes Bündel von Maßnahmen ausarbeiten und umsetzen, um für ihre Sicherheit zu sorgen. Der Rat betont, wie wichtig es ist, dass die Interoperabilität der IT-Infrastruktur für den Austausch von EU-Verschlusssachen zwischen den Organen, Agenturen und Einrichtungen der EU und den Mitgliedstaaten gewährleistet ist.