



–1880022-V150–

Präsidenten des Deutschen Bundestages  
Herrn Prof. Dr. Norbert Lammert MdB  
Parlamentssekretariat  
Platz der Republik 1  
11011 Berlin

**Dr. Ralf Brauksiepe**

Parlamentarischer Staatssekretär  
Mitglied des Deutschen Bundestages

HAUSANSCHRIFT Stauffenbergstraße 18, 10785 Berlin

POSTANSCHRIFT 11055 Berlin

TEL +49 (0)30-18-24-22350

FAX +49 (0)30-18-24-22380

E-MAIL BMVgBueroParlStsDrBrauksiepe@BMVg.BUND.DE

BETREFF **Kleine Anfrage der Abgeordneten Andrej Hunko, Wolfgang Gehrcke, Jan van Aken u.a. und der Fraktion DIE LINKE. vom 22. April 2016, eingegangen beim Bundeskanzleramt am 26. April 2016**

**BT-Drucksache 18/8227 vom 22. April 2016**

**Einsatzmöglichkeiten von Militär und Geheimdiensten gegen sogenannte hybride Bedrohungen**

ANLAGE Antwort der Bundesregierung auf die oben genannte Kleine Anfrage  
Berlin, 30. Mai 2016

Sehr geehrter Herr Bundestagspräsident,

beigefügt übersende ich die Antwort der Bundesregierung auf die oben genannte Kleine Anfrage.

Auf die Einstufung von Teilen der Antwort auf die Frage 11 sowie der Antworten auf die Fragen 12 und 13 als „VS-VERTRAULICH“ erlaube ich mir hinzuweisen.

Mit freundlichen Grüßen

**Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Wolfgang Gehrcke, Jan van Aken u.a. sowie der Fraktion DIE LINKE. vom 22. April 2016**

**BT-Drucksache 18/8227 vom 22. April 2016**

**Einsatzmöglichkeiten von Militär und Geheimdiensten gegen sogenannte hybride Bedrohungen**

*Am 6. April 2016 veröffentlichten die Europäische Kommission und der Europäische Auswärtige Dienst ihre Initiative „Gemeinsamer Rahmen für die Abwehr hybrider Bedrohungen, die Stärkung der Resilienz der EU, ihrer Mitgliedstaaten und Partnerländer und den Ausbau der Zusammenarbeit mit der NATO bei der Bekämpfung solcher Bedrohungen“. Ein entsprechendes Papier enthält Vorschläge für 22 operative Maßnahmen (JOIN(2016) 18 final). Laut einer am gleichen Tag herausgegebenen Pressemitteilung seien die Europäische Union und ihre Mitgliedstaaten „in zunehmendem Maße hybriden Bedrohungen ausgesetzt“. Das Sicherheitsumfeld habe sich drastisch verändert, auch an den Außengrenzen der Europäischen Union nähmen „hybride Bedrohungen“ zu. „Hybride“ Aggressionen würden nicht nur unmittelbaren Schaden anrichten und Verwundbarkeiten ausnutzen, sondern Gesellschaften destabilisieren und „durch Verschleierungstaktik“ die Entscheidungsfindung zu einer gemeinsamen Antwort behindern. Innere und äußere Sicherheit müssten deshalb noch stärker miteinander verknüpft werden. Auch Geheimdienste sollen sich an der Abwehr von „hybriden Angriffen“ unterhalb der Schwelle militärischer Gewalt beteiligen. Das Lagezentrum Intelligence and Situation Centre (INTCEN) in Brüssel soll mit einer „Hybrid Fusion Cell“ erhalten. Die Zelle soll Frühwarnberichte erstellen und mit anderen Agenturen zusammenarbeiten. Genannt werden die bei Europol angesiedelten Zentren gegen Cyberkriminalität sowie gegen Terrorismus, die Grenzschutzagentur FRONTEX und das Computersicherheits-Ereignis- und Reaktionsteam der Europäischen Union (CERT-EU). Zur besseren Zusammenarbeit soll die „Hybrid Fusion Cell“ ein Abkommen mit der Abteilung gegen „hybride Bedrohungen“ bei der NATO schließen. Anvisiert sind unter anderem gemeinsame Übungen „auf politischer und technischer Ebene“.*

*Ein eigenes Kapitel widmet sich den Cyberbedrohungen. Zwar hat die Europäische Union bereits eine Strategie zur Cybersicherheit veröffentlicht (Ratsdokument 6225/13). Trotzdem müsse vor allem die Abwehrfähigkeit kritischer Infrastrukturen ausgebaut werden. Hierzu gehören die Bereiche Energie, Verkehr und Raumfahrt, aber auch der Schutz des Finanzsystems. Dessen Geschäfte und Infrastrukturen sollen nun mit weiteren Maßnahmen geschützt werden. Das Finanzsystem werde aber auch zur „hybriden Kriegsführung“ genutzt. Deshalb soll die Polizeiagentur Europol nun mit ihren Strukturen zum Aufspüren von Terrorismusfinanzierung und Geldwäsche eingebunden werden. Europol solle auch bei der Bekämpfung von gewalttätigem Extremismus und Radikalisierung unterstützen. Diese seien zwar nicht per se „hybrider Natur“, würden jedoch von Tätern genutzt, um „verletzbare“ Teile der Gesellschaft durch moderne Kommunikationsmittel und Propaganda zu radikalisieren. Im Sommer hatte Europol eine „Meldestelle für Internetinhalte“ eröffnet, die zunächst auf „terroristisch/extremistische“ Postings beschränkt war. Kurz darauf folgte die Ausweitung der Zuständigkeit auf „Migranten-schmuggel“, nun soll die Meldestelle auch bei „hybriden Bedrohungen“ tätig werden und Inhalte durch die Internetanbieter entfernen lassen.*

*Im September 2015 hat der Europäische Auswärtige Dienst ein Team für „Strategische Kommunikation“ (EU East StratCom Task Force) ins Leben gerufen, um damit die politischen EU-Ziele in der östlichen Nachbarschaft „voranzutreiben“ (Bundestagsdrucksache 18/6486). Die Arbeitsgruppe soll „Russlands andauernden Desinformationskampagnen über den Ukraine Konflikt“ kontern. Die EU East StratCom Task Force will keine Gegenpropaganda lancieren, entwickelt aber „positive Narrative und Kommunikationsprodukte“ in russischer Sprache.*

*Schließlich wird in der Mitteilung vom 6. April 2016 auch die Abwehr eines „großangelegten, schweren hybriden Angriffs“ vorbereitet. Mit der Solidaritätsklausel nach Artikel 222 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) verfügt die Europäische Union über Möglichkeiten zur Krisenreaktion. Die Mitteilung vom 6. April 2016 schlägt vor, die mögliche Nutzung des Artikels 222 AEUV im Falle „hybrider Angriffe“ zu diskutieren. Entsprechende Maßnahmen könnten dann in einer Ausführungsbestimmung festgelegt werden. In Artikel 42 des Vertrags über die Europäische Union (EUV) hat sich die EU mit der Beistandsklausel zudem die Möglichkeit einer gemeinsamen militärischen Antwort auf Bedrohungen geschaffen. Die erstmals von Frankreich nach den Paris-Anschlägen im November 2015 ausgerufene Beistandspflicht soll nun ebenfalls für „hybride Angriffe“ ausgebaut werden.*

### **Vorbemerkung der Bundesregierung**

Auch wenn die Begriffe „hybride Kriegsführung“, „hybride Konflikte“ und „hybride Bedrohungen“ seit mehreren Jahren Teil des sicherheitspolitischen Diskurses geworden sind, entziehen sich diese Begriffe einfachen und abschließenden Definitionen.

Wie Konflikte in der jüngeren Vergangenheit gezeigt haben, kann ein hybrides Vorgehen aufeinander abgestimmte Aktivitäten beinhalten, wie beispielsweise die para-militärische, politische und logistische Unterstützung nichtstaatlicher Akteure und den Einsatz verdeckt operierender oder nicht gekennzeichnete Spezialkräfte bei einem gleichzeitigen Aufbau einer konventionellen militärischen Drohkulisse. Der Einsatz hybrider Mittel erfolgt dabei vorzugsweise unterhalb der Schwelle eines bewaffneten Konflikts und unter Verschleierung der eigenen Rolle als Konfliktpartei.

Varianten „hybrider Bedrohungen“ werden von Kampagnen im Informationsraum begleitet. Dabei erweisen sich neben den klassischen Medien die sozialen Netzwerke als wirkungsvolle Instrumente für Propaganda oder Desinformation.

Ziele hybrider Aktionen im Informationsraum können beispielsweise die Destabilisierung der Gesellschaft durch die Manipulation der öffentlichen Meinung sein, sodass die Voraussetzungen für die Anwendung politischer, wirtschaftlicher und militärischer Mittel oder für weitere hybride Aktionen geschaffen werden.

Überdies versuchen hybride Angreifer, die Möglichkeit der Feststellung von Verstößen gegen das völkerrechtliche Gewalt- und Interventionsverbot sowie die Ausübung des Rechts auf Selbstverteidigung zu erschweren und damit im Kern das bisherige Verständnis von Kriegen und Konflikten von Grund auf zu verändern.

In der jüngsten Vergangenheit lieferte vornehmlich das russische Vorgehen auf der Krim und in der Ost-Ukraine Beispiele hybrider Eskalationsdynamik. Diese Fälle haben das Bewusstsein der Bundesregierung dafür geschärft, dass zur Abwehr „hybrider Bedrohungen“ neben der Stärkung nationalstaatlicher Resilienz eine Kooperation zwischen der NATO und der EU sowie ggf. die Einbindung weiterer Organisationen zielführend sind.

Wesentliche weitere Elemente der Abwehr „hybrider Bedrohungen“ sind die Krisenfrüherkennung, die Aufklärung mit militärischen und zivilen Mitteln, der Aufbau und die Stärkung der eigenen Analysefähigkeiten, die Strategieentwicklung und vor allem eine glaubhafte Abschreckung.

Dabei ist es im konkreten Fall wesentlich, einem Herausforderer eindeutig und glaubwürdig zu vermitteln, dass „hybride Bedrohungen“ erkannt wurden und sowohl der Wille als auch die Fähigkeiten vorhanden sind, ihnen entschlossen entgegenzutreten. Es muss deutlich zu Ausdruck kommen, dass die potentiellen Gegenmaßnahmen und damit die zu erwartenden Kosten die möglichen Gewinne für einen hybriden Angreifer bei weitem übersteigen.

Mit der Verabschiedung des Readiness Action Plan (RAP) auf dem Gipfel in Wales hat die NATO einen ersten wichtigen Schritt unternommen, um u.a. dem Phänomen der hybriden Konfliktaustragung in seinen militärischen Aspekten auch im Bündnisrahmen mit dem gesamten Spektrum an Instrumenten begegnen zu können.

1. *Wie definiert die Bundesregierung den Begriff „hybride Bedrohungen“?*

- a) *Wodurch grenzen sich „hybride Bedrohungen“ aus Sicht der Bundesregierung von „terroristischen“ oder „kriminellen“ Angriffen oder Praxen ab?*
- b) *Inwiefern können „hybride Bedrohungen“ aus Sicht der Bundesregierung als Praxen von staatlichen oder nichtstaatlichen Akteuren differenziert werden?*
- c) *Unter welchen Umständen sind aus Sicht der Bundesregierung auch „gewalttätiger Extremismus“ und „Radikalisierung“ als Angriffe „hybrider Natur“ einzustufen?*

Die Fragen 1 sowie 1a) bis 1c) werden im Zusammenhang beantwortet.

Bei „hybriden Bedrohungen“ handelt es sich um ein Phänomen, das sich nur schwer eindeutig von anderen Konfliktformen abgrenzen lässt, da eines seiner Hauptmerkmale gerade darin besteht, unterschiedliche Formen und Methoden der Konfliktaustragung und der Kriegführung miteinander zu kombinieren. „Hybride Bedrohungen“ oder „hybride Kriegführung“ können sich auf verschiedene Weise manifestieren: die Verbindung staatlicher und nicht-staatlicher Akteure, militäri-

scher und nicht-militärischer Mittel, asymmetrische Einsatzformen, die Nutzung des Informationsraums zur Verbreitung von Propaganda und Desinformation oder auch Cyberattacken und -sabotage, um nur einige mögliche Elemente eines „hybriden Szenarios“ zu nennen. In diesem Zusammenhang wird auch auf die Antwort der Bundesregierung auf Bundestagsdrucksache 18/6989 verwiesen.

Hybride Angriffe richten sich gezielt gegen die erkannten Verwundbarkeiten eines Bündnisses, eines Staates oder einer Gesellschaft, beispielsweise entlang staatlich getrennter Verantwortungsbereiche und Ressortgrenzen oder entlang ethnischer und sozialer Spannungen. Dies betrifft u.a. die Schnittstellen von innerer und äußerer Sicherheit, innerstaatlichem oder zwischenstaatlichem Konflikt sowie zivilem oder militärischem Handeln. Kritische Infrastrukturen, die Werteorientierung und kulturelle Pluralität sowie der Staat und die Gesellschaft insgesamt können so zu potenziellen Angriffszielen werden.

Eine wesentliche Begleiterscheinung „hybrider Bedrohungen“ ist das zumindest versuchte Verschleiern von den Verantwortlichkeiten und der Urheberschaft.

2. *Was ist der Bundesregierung aus ihrer Teilnahme an Ratsarbeitsgruppen über gemeinsame Treffen mit Russland bekannt, die nach Kenntnis der Fragesteller im Februar 2016 in Brüssel stattfanden und die Themenfelder „gewalttätigen Extremismus“ und „Terrorismusbekämpfung“ thematisierten?*
  - a) *Auf wessen Initiative fanden die Treffen statt, und wer nahm daran teil?*
  - b) *Welche Ergebnisse der Treffen sind der Bundesregierung bekannt?*

Die Fragen 2 sowie 2a) und 2b) werden im Zusammenhang beantwortet.

Nach Kenntnis der Bundesregierung fand ein informelles Treffen von Vertretern des Europäischen Auswärtigen Dienstes (EAD) und Russlands am 1. April 2016 in Brüssel statt, das auf russische Initiative zustande kam und konstruktiv verlief. Das Treffen hat den Ansatz der Europäischen Union bestätigt, Gesprächskanäle mit Russland offen zu halten und dabei sowohl über Differenzen als auch über gemeinsame Interessen den Dialog zu führen.

3. *Inwiefern hält es die Bundesregierung für erforderlich oder nicht erforderlich, sich auf einen „großangelegten, schweren hybriden Angriff“ vorzubereiten?*

Der Schutz Deutschlands und seiner Bürgerinnen und Bürger ist die originäre Aufgabe der Bundesregierung. Die zu dessen Gewährleistung erforderlichen Anstrengungen und Vorbereitungen orientieren sich sowohl an der aktuellen als auch an einer zukünftig möglichen Bedrohungslage. Im Rahmen deutscher Bündnisverpflichtungen ist hierzu auch die Bedrohungslage unserer Verbündeten und Partner zu berücksichtigen. Ein „großangelegter, schwerer hybrider Angriff“ kann dabei nicht grundsätzlich ausgeschlossen werden.

Im Übrigen wird auf die Antwort auf die Frage 1 verwiesen.

4. *Inwiefern ist der Einsatz „hybrider Bedrohungen“ aus Sicht der Bundesregierung auch bei Mitgliedstaaten der NATO zu beobachten?*

Die in der Antwort auf die Frage 6 getroffenen Aussagen sind grundsätzlich auch auf andere NATO-Mitgliedstaaten übertragbar.

5. *Was ist der Bundesregierung darüber bekannt, inwiefern auch das internationale Finanzsystem zur „hybriden Kriegsführung“ genutzt wird oder werden könnte?*

Der Bundesregierung liegen hierzu keine Erkenntnisse vor.

6. *In welchem Maß sieht sich die Bundesregierung „hybriden Bedrohungen“ ausgesetzt, und welchen Einfluss haben diese demnach auf ihr Sicherheitsumfeld?*

„Hybride Bedrohungen“ zielen auf die von einem möglichen Angreifer wahrgenommenen Verwundbarkeiten eines Staates und seiner Gesellschaft. In offenen Gesellschaften wie der Bundesrepublik Deutschland wird beispielsweise versucht, im Rahmen von Desinformations- und Propagandamaßnahmen die plurale Medien- und Meinungslandschaft sowie die hohe Vernetzung innerhalb der Gesellschaft auszunutzen, um strategische Ziele durchzusetzen. Weitere denkbare Mittel hybrider Konfliktaustragung gegen die Bundesrepublik Deutschland sind Cyberangriffe.

- a) *In welchen geografischen Bereichen treten diese „hybriden Bedrohungen“ besonders häufig auf?*

„Hybride Bedrohungen“ haben oft einen transnationalen Charakter und können grundsätzlich von staatlichen Akteuren – auch unter Einbindung nichtstaatlicher Akteure – aus allen Regionen der Welt ausgehen und in allen Regionen durchgeführt werden.

- b) *Welcher konkrete Schaden wurde dabei bereits angerichtet?*

„Hybride Bedrohungen“ umfassen eine Vielzahl von Formen und Methoden, bei denen es um den Effekt ihres Zusammenwirkens geht einschließlich des Aufbaus einer möglichen militärischen Drohkulisse. Es kann konkreter materieller, finanzieller und personeller Schaden entstehen. Im Falle eines Hackerangriffs oder der Sabotage kritischer Infrastruktur können Schäden entstehen, die mit den Auswirkungen bewaffneter Angriffe vergleichbar sind. Propaganda- und Desinformationsmaßnahmen können negative (massen-)psychologische Auswirkungen nach sich ziehen, deren Schadensumfang im Vorhinein nicht exakt zu beziffern ist.

7. *Inwiefern ist auch die Bundesregierung wie die Europäische Kommission und der Europäische Auswärtige Dienst der Ansicht, „hybride Bedrohungen“ seien geeignet, Gesellschaften zu destabilisieren und „durch Verschleierungstaktik“ die Entscheidungsfindung zu einer gemeinsamen Antwort zu behindern?*

Die Bundesregierung ist der Ansicht, dass Propaganda- und Desinformationsmaßnahmen durch (massen-)psychologische Beeinflussung destabilisierend wirken können. Sie ist zudem der Ansicht, dass es häufig Ziel „hybrider Bedrohungen“ ist, die Verantwortlichkeit und die Urheberschaft gezielt zu verschleiern, um die Entscheidungsfindung nationaler Regierungen und internationaler Gremien und Organisationen zu verzögern oder zu verhindern. In diesem Zusammenhang wird auch auf die Antwort der Bundesregierung auf Bundestagsdrucksache 18/6989 verwiesen.

Die Bundesregierung teilt die Ansicht der Europäischen Kommission und der Hohen Vertreterin der Union für Außen- und Sicherheitspolitik, die in ihrer Gemeinsamen Mitteilung vom 6. April 2016 eine verstärkte Kooperation zwischen der EU und der NATO sowie zwischen EU-Mitgliedstaaten und EU-Institutionen in diesem Bereich unterstützen. Der Rat hat in seinen Schlussfolgerungen vom 19. April 2016 die Gemeinsame Mitteilung begrüßt.

8. *In welchen herausragenden Fällen ist dies in der jüngeren Vergangenheit bereits zu beobachten gewesen?*

In der jüngeren Zeit war die gezielte Verschleierung der Verantwortlichkeit insbesondere im Zuge der völkerrechtswidrigen Annexion der Krim durch Russland zu beobachten.

9. *Inwiefern teilt die Bundesregierung die von dem durch das Bundesministerium der Verteidigung als Experte der Deutschen Gesellschaft für Auswärtige Politik e. V. (DGAP) vorgestellten Stefan Meister im März 2016 vor Vertretern von Europäischer Union, NATO und des Auswärtigen Amts vorgetragene Behauptung, wonach „eines der wichtigsten Instrumente“ zur Verbreitung der „Propaganda-Nachrichten des Kreml“ das Online-Medienportal „Sputnik“ sei, bei dem „Kreml-Trolle“ zur Verbreitung falscher oder erfundener Informationen beschäftigt seien (bmvg.de vom 4. April 2016, Autor: Tilman Engel)?*

Die zitierte Einschätzung von Herrn Dr. Stefan Meister gibt dessen persönliche Auffassung wieder. Es ist aber unbestritten, dass Online-Medienportale über eine mitunter große internationale Reichweite verfügen können und damit über entsprechende Möglichkeiten der Information und gegebenenfalls gezielten Beeinflussung. Insbesondere staatlich gelenkte Online-Portale können im Einzelfall als ein mögliches und wesentliches Instrument hybriden Vorgehens im Informationsraum angesehen werden.

10. *Welche Einteilung von Kategorien digitaler Angriffe hält die Bundesregierung für sinnvoll, und inwiefern macht sie sich die Einschätzung des NATO Strategic Communications Centre of Excellence (NATO StratCom COE) in Riga zu eigen, das in „Verschwörungs-Trolle“, „Wut-Trolle“, „Anhang-Trolle“, „Wikipedia-Trolle“ und „Bikini-Trolle“ unterscheidet (bmvg.de vom 4. April 2016, Autor: Tilman Engel)?*

Die Bundesregierung nimmt die Arbeit des NATO Strategic Communications Centre of Excellence aufmerksam zur Kenntnis, ohne sich einzelne Diskussionsbeiträge automatisch zu eigen zu machen. Sie misst der offenen wissenschaftlichen Auseinandersetzung mit den vielfältigen Aspekten „hybrider Bedrohungen“ große Bedeutung zur Schaffung eines besseren Verständnisses des Gegenstandes und zur Ableitung möglicher politischer Handlungsempfehlungen zu und begrüßt diese ausdrücklich.

11. *Wann haben der Präsident des Bundesnachrichtendienstes (BND) und der Präsident des Bundesamtes für Verfassungsschutz (BfV) erstmals belastbare Kenntnisse davon erlangt, dass der Whistleblower Edward Snowden „Teil russischer Geheimdienstoperationen gegen Deutschland und Westeuropa“ gewesen sei (FOCUS vom 15. April 2016)?*

- a) *Aus welchem Grund hält es die Bundesregierung für „sehr auffällig“, dass Edward Snowden „ausgerechnet Unterlagen über die Zusammenarbeit der National Security Agency (NSA) mit dem BND oder dem englischen Geheimdienst Government Communications Headquarters (GCHQ) veröffentlicht hat“?*
- b) *Über welche belastbaren Erkenntnisse verfügen der Präsident des BND und der Präsident des BfV, dass Edward Snowden auch über Dokumente zu Ländern wie China oder Russland verfügt, diese aber zurückhält, um durch den „Verrat“ lediglich eines Teils der Dokumente „einen Keil zwischen Westeuropa und die USA zu treiben“?*

Die Fragen 11 sowie 11a) und 11b) werden im Zusammenhang beantwortet.

Entgegen der Formulierung der Fragesteller hat der Präsident des Bundesamtes für Verfassungsschutz (BfV) in dem bezeichneten Interview (erschieden im FOCUS vom 16. April 2016) nicht von belastbaren Erkenntnissen gesprochen. Über die genauen Motive des Handelns von Herrn Snowden verfügt die Bundesregierung über keine belastbaren Informationen.

Die weitere Beantwortung der Frage ist als „VS-VERTRAULICH“ eingestuft und wird zur Einsichtnahme in der Geheimschutzstelle des Deutschen Bundestages hinterlegt.

Die Bundesregierung ist nach sorgfältiger Abwägung zu der Auffassung gelangt, dass eine Beantwortung nicht offen erfolgen kann. Die erbetenen Auskünfte sind geheimhaltungsbedürftig, weil sie Informationen enthalten, die Rückschlüsse auf die Führung nachrichtendienstlicher Quellen erlauben könnten. Der Quellenschutz stellt für die Aufgabenerfüllung der Nachrichtendienste einen überragend wichtigen Grundsatz dar.



Die öffentliche Bekanntgabe von Informationen, die Unbefugten Rückschlüsse auf die Identität von Quellen ermöglichen könnten, würde zum einen die staatliche Fürsorgepflicht gegenüber den Betroffenen verletzen. Zum anderen würde die künftige Anwerbung von Quellen schon durch die bloße Möglichkeit des Bekanntwerdens der Identität von Quellen insgesamt nachhaltig beeinträchtigt. Dieses würde wiederum zu einer erheblichen Schwächung der den Nachrichtendiensten zur Verfügung stehenden Möglichkeiten zur Informationsgewinnung führen. Eine Kenntnisnahme durch Unbefugte würde daher für die Auftragserfüllung des Bundesnachrichtendienstes erhebliche Nachteile zur Folge haben. Sie kann für die Interessen der Bundesrepublik Deutschland schädlich sein.

12. *Welche „psychologischen Operationen“ unter Zuhilfenahme von „Desinformation, Infiltration, Einflussnahme, Propaganda und Zersetzung“ haben „die Russen“ nach Kenntnis des Präsidenten des BND bereits in Deutschland durchgeführt (FOCUS vom 15. April 2016)?*
13. *Inwiefern sind mit dem Begriff „die Russen“ auch nicht-staatliche Kräfte gemeint?*

Die Antworten auf die Fragen 12 und 13 sind als „VS-VERTRAULICH“ eingestuft und zur Einsichtnahme in der Geheimschutzstelle des Deutschen Bundestages hinterlegt.

Die Bundesregierung ist nach sorgfältiger Abwägung zu der Auffassung gelangt, dass eine Beantwortung aus Gründen des Staatswohls nicht offen erfolgen kann. Arbeitsmethoden und Vorgehensweisen der Nachrichtendienste des Bundes sind im Hinblick auf die künftige Erfüllung des gesetzlichen Auftrags aus § 1 Abs. 2 des Gesetzes über den Bundesnachrichtendienst besonders schutzwürdig. Ebenso schutzbedürftig sind Einzelheiten zu der nachrichtendienstlichen Erkenntnislage. Eine Veröffentlichung von Einzelheiten betreffend solche Erkenntnisse würde zu einer wesentlichen Schwächung der dem Bundesnachrichtendienst (BND) zur Verfügung stehenden Möglichkeiten zur Informationsgewinnung führen. Dies würde für die Auftragserfüllung des BND erhebliche Nachteile zur Folge haben. Sie kann für die Interessen der Bundesrepublik Deutschland schädlich sein.

14. *Wie viele Referenten und Referatsleiter des BfV sind derzeit mit der Aufarbeitung der Akten für Untersuchungsausschüsse beschäftigt, und wie viele Referenten und Referatsleiter befassen sich derzeit mit dem „Bereich islamistischer Terrorismus“ (FOCUS vom 15. April 2016)?*

Mit der Aufarbeitung der Akten für Untersuchungsausschüsse sind derzeit 20 Referentinnen bzw. Referenten und Referatsleiterinnen bzw. Referatsleiter im BfV befasst. Für die Beantwortung fachlicher Detailfragen werden darüber hinaus anlassbezogen weitere Referentinnen bzw. Referenten und Referatsleiterinnen bzw. Referatsleiter aus den Arbeitseinheiten der Abteilungen hinzugezogen, die inhaltlich im besonderen Maße von den Beweisbeschlüssen und Anfragen betroffen sind, so dass zeitweise - d.h. beweisbeschlussabhängig - eine weitaus höhere Anzahl mit Untersuchungsausschuss-Angelegenheiten befasst waren bzw. sind und Arbeits- und Personalkapazitäten in erheblichem Maße und abteilungsübergreifend gebunden werden.

Mit Stand 28. April 2016 sind im BfV 13 Referentinnen bzw. Referenten und Referatsleiterinnen bzw. Referatsleiter mit dem „Bereich islamistischer Terrorismus“ befasst.

15. *Welche Cyberbedrohungen sind aus Sicht der Bundesregierung nicht von der EU-Strategie zur Cybersicherheit erfasst, und welche weiteren Maßnahmen sind demnach erforderlich?*

Die von der Europäischen Kommission und der Hohen Vertreterin der Union für Außen- und Sicherheitspolitik am 7. Februar 2013 vorgelegte Mitteilung „Cybersicherheitsstrategie der Europäischen Union“ ist ähnlich der deutschen Cybersicherheitsstrategie vom Februar 2011 inhaltlich breit ausgelegt und spricht für den Bereich der Cyber-Sicherheit umfassend übergreifende strategische Prioritäten an.

Die strategische Bündelung der Cyber-Sicherheitsaktivitäten auf EU-Ebene trägt dazu bei, die Gesamtsicherheit in der EU erhöhen. Die Notwendigkeit für eine Neuauflage der EU-Cybersicherheitsstrategie wird seitens der Bundesregierung derzeit nicht gesehen.

16. *Inwiefern sollten „hybride Bedrohungen“ aus Sicht der Bundesregierung auch durch mehr Beobachtung und Kontrolle des Internets bekämpft werden?*

Im Rahmen der Vorsorge gegen „hybride Bedrohungen“ nehmen die Behörden des Bundes ihre gesetzlichen Befugnisse auch in Bezug auf das Internet wahr.

- a) *Welche Haltung vertritt die Bundesregierung zur Frage, welche Aufgabe die zunächst für „terroristisch/extremistische“ Postings und schließlich auf „Migrantenschmuggel“ erweiterte, bei Europol eingerichtete „Meldestelle für Internetinhalte“ hierzu übernehmen könnte?*

Aus Sicht der Bundesregierung besteht auch angesichts der Unbestimmtheit der Begrifflichkeit kein Bedarf, die Zuständigkeit der bei Europol eingerichteten „Meldestelle für Internetinhalte“ auf „hybride Bedrohung“ zu erweitern.

- b) *Was ist der Bundesregierung darüber bekannt, welche weiteren internationalen Strafverfolgungsbehörden sowie Internetunternehmen an der von Europol unterstützten Operation der britischen „Counter Terrorism Internet Referral Unit“ (CTIRU) teilnahmen, um unerwünschte Internetinhalte aufzuspüren und zu entfernen (Pressemitteilung „International operation against online terrorism and extremism“ vom 21. April 2016)?*

Der Bundesregierung ist nicht bekannt, welche weiteren internationalen Strafverfolgungsbehörden sowie Internetfirmen an der von Europol unterstützten Operation der britischen „Counter Terrorism Internet Referral Unit“ teilgenommen haben.

- c) *Inhalte welcher „internationaler terroristischer Organisationen“ außer dem „Islamischen Staat im Irak und in Syrien“ (ISIS) und „Boko Haram“ sowie welcher „extrem rechter Gruppierungen“ wurden dabei gefunden und entfernt?*

Soweit das Bundeskriminalamt im Rahmen der vorgenannten Operation durch Europol beteiligt worden ist, waren neben dem sog. Islamischen Staat Inhalte der Gruppierungen Taliban und Al-Shabab betroffen.

17. *Was ist der Bundesregierung über Pläne zur Einrichtung einer „Hybrid Fusion Cell“ im Lagezentrum INTCEN in Brüssel bekannt, und wer soll ihr angehören?*

- a) *Inwiefern soll die neue „Hybrid Fusion Cell“ auch Internetbeobachtung betreiben?*

Die Fragen 17 und 17a) werden im Zusammenhang beantwortet.

Die EU Hybrid Fusion Cell wird vom Europäischen Auswärtigen Dienst eingerichtet werden. Details hierzu sind noch nicht bekannt.

- b) *Auf welche Weise könnte die „Hybrid Fusion Cell“ aus Sicht der Bundesregierung mit der Polizeibehörde Europol und der Grenzschutzagentur FRONTEX kooperieren?*

Die Bundesregierung ist der Auffassung, dass eine zu schaffende EU Hybrid Fusion Cell als zentrale Anlaufstelle für einen Informationsaustausch zu Fragen „hybrider Bedrohungen“ den Kontakt zu allen diesbezüglich relevanten EU-Gremien und -Agenturen pflegen sollte.

- c) *Inwiefern wird auch die Bundesregierung eine nationale Kontaktstelle für die „Hybrid Fusion Cell“ einrichten, und welche Aufgaben werden dort von welchen Behörden übernommen?*

Die Bundesregierung greift die Anregung zur möglichen Einrichtung einer nationalen Kontaktstelle für hybride Bedrohungen auf. Einzelheiten hierzu stehen jedoch noch nicht fest.

18. *Auf welche Weise soll nach Kenntnis der Bundesregierung die EU East StratCom Task Force ihre Anstrengungen zur Erstellung und Verteilung „positiver Narrative und Kommunikationsprodukte“ verstärken?*

Eine der Aufgaben der EU EAST STRATCOM Task Force ist die Erarbeitung von Kommunikationsstrategien und -produkten. Dazu werden in Zusammenarbeit mit den EU-Delegationen und den Botschaften der EU-Mitgliedstaaten in den Ländern der Östlichen Partnerschaft länderspezifische Kommunikationsstrategien entwickelt, die eine einheitliche Außendarstellung befördern sollen.

Von der EU EAST STRATCOM Task Force wird die Umsetzung dieser Strategien durch die Bereitstellung spezifischer Kommunikationsprodukte unterstützt, etwa durch Videos, Artikel, Infographiken, etc.

19. *Welche weiteren Schritte bzw. Initiativen zur Umsetzung des „Aktionsplans über strategische Kommunikation“ wurden nach Kenntnis der Bundesregierung zu den Aktivitätsfeldern „Verbesserung der Kommunikationsfähigkeit der EU, Zusammenarbeit mit Partnern, Unterstützung für Presse- und Meinungsfreiheit, public diplomacy in den Nachbarländern der EU, Training für Journalisten, Unterstützung für Pluralismus in russischsprachigen Medien und Zusammenarbeit mit der Zivilgesellschaft“ entfaltet (Bundestagsdrucksache 18/6486)?*

Auf die Antwort auf die Frage 18 wird verwiesen.

Zur Unterstützung von Presse- und Medienfreiheit und zur Ausbildung von Journalisten hat die Europäische Kommission das sog. OPEN-Programm aufgelegt. Mit einem Budget von 20 Mio. Euro sollen zwischen den Jahren 2015 und 2019 Journalisten aus- und fortgebildet und Kommunikationskampagnen unterstützt werden.

EU-Mitgliedstaaten unterstützen diese Maßnahmen. Die Bundesregierung hat im Rahmen des Programms „Ausbau der Zusammenarbeit mit der Zivilgesellschaft in den Ländern der Östlichen Partnerschaft und Russland“ seit dem Jahr 2014 mit dem Förderschwerpunkt „Pluralismus stärken“ Projekte unterstützt, die sich den Auf- und Ausbau von Informations-, Meinungs- und Medienvielfalt zum Ziel gesetzt haben. Hierzu gehören Maßnahmen zur Aus- und Fortbildung von Journalisten und Bloggern, Hospitationsprogramme in Deutschland sowie geeignete Projekte an Schulen und Universitäten ebenso wie der Umbau des ukrainischen Staatsfernsehens in eine öffentlich-rechtliche Medienanstalt, den die Deutsche Welle-Akademie beratend begleitet. Insgesamt wurden so seit dem Jahr 2014 für insgesamt 119 Projekte mit diesem Schwerpunkt 11,2 Mio. Euro vergeben. Zudem werden im Jahr 2016 2,3 Mio. Euro für die Förderung von Medienprojekten mit einem Bezug zu Russland vergeben.

Mit dem gleichen Ziel wurden für die baltischen Staaten Maßnahmenpakete geschnürt. So wurde im Jahr 2015 neben der Förderung von Journalistentrainings diverser zivilgesellschaftlicher Akteure mit Themen wie Recherchekompetenz und konfliktsensitiver Berichterstattung auch die Intensivierung der Zusammenarbeit der Deutschen Welle mit ihren baltischen Partnern und andere mit den baltischen Staaten vereinbarte Projekte finanziert.

20. *Auf welche Weise wird die Bundesregierung die „Schlussfolgerungen des Rates zur Bewältigung hybrider Bedrohungen“ vom 19. April 2016 (Ratsdokument 7928/16) berücksichtigen und/oder umsetzen, der ein „rasches und angemessenes Handeln zur Prävention und Bewältigung von hybriden Bedrohungen für die Union und ihre Mitgliedstaaten sowie für ihre Partner“ anmahnt?*

Die ressortübergreifende Ableitung der Bundesregierung zu den in den „Schlussfolgerungen des Rates zur Bewältigung hybrider Bedrohungen“ angeregten Maßnahmen ist angelaufen. Details zur Umsetzung liegen daher noch nicht vor.

- a) *Was ist der Bundesregierung über Pläne einer noch einzurichtenden „Hybrid Fusion Cell“ bekannt, mit einer NATO-Abteilung gegen „hybride Bedrohungen“ gemeinsame Übungen „auf politischer und technischer Ebene“ durchzuführen, und worum handelt es sich dabei?*

Die Bundesregierung ist der Auffassung, dass zur Bewältigung hybrider Bedrohungen eine enge Koordination und Kooperation zwischen der NATO und der EU anzustreben ist, die auch Übungen einschließen soll.

- b) *Sofern diese Übungen „auf politischer und technischer Ebene“ noch nicht ausformuliert sind, welche Anstrengungen hält die Bundesregierung hierzu für notwendig?*

Die Stäbe der EU und der NATO sind zur Ausformulierung von parallelen oder gemeinsamen Übungen in engem Kontakt. Die Bundesregierung unterstützt dieses Vorhaben.

21. *Inwiefern und mit welchen Einschränkungen könnte aus Sicht der Bundesregierung die Solidaritätsklausel nach Artikel 222 AEUV und die Beistandsklausel nach Artikel 42 EUV zur Vorbeugung und Reaktion auf „hybride Bedrohungen“ angewandt werden, und welche Änderungen zur Ausführung oder Umsetzung wären hierfür erforderlich?*

Der Bundesregierung sind hierzu keine konkreten Überlegungen bekannt.